UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

NATHAN LOPES DOS SANTOS

APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO DE ANÁLISE COMBINATÓRIA E SEGURANÇA DIGITAL NO ENSINO MÉDIO

VITÓRIA DA CONQUISTA-BA

2024

UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
MESTRADO PROFISSIONAL EM MATEMATICA EM REDE NACIONAL – PROFMAT
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

NATHAN LOPES DOS SANTOS

APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO DE ANÁLISE COMBINATÓRIA E SEGURANÇA DIGITAL NO ENSINO MÉDIO

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, oferecido pela Universidade Estadual do Sudoeste da Bahia – UESB, como requisito necessário para obtenção do grau de Mestre em Matemática. Orientador: Prof. Dr. Flaulles Boone Bergamaschi.

VITÓRIA DA CONQUISTA

2024

S233a Santos, Nathan Lopes dos.
Aplicação da criptografia no ensino de análise combinatória e segurança digital no ensino médio. / Nathan Lopes dos Santos, 2024.
100f. il.
Orientador (a): Dr. Flaulles Boone Bergamaschi.
Dissertação (mestrado) – Universidade Estadual do Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista - BA, 2024.
Inclui referências. 93 - 94.
1.Análise Combinatória - Ensino de matemática. 2. Criptografia - Segurança digital. 3. Princípio Fundamental da Contagem. 4. Tabela Geradora de Senhas. 5. Aritmética Modular - Semiótica, I. Bergamaschi, Flaulles Boone. II. Universidade Estadual Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista - Ba. III. T.

CDD: 511.6

Catalogação na fonte: Juliana Teixeira de Assunção - CRB 5/1890
UESB – Campus Vitória da Conquista – BA

Nathan Lopes dos Santos

Aplicação da criptografia no ensino de análise combinatória e segurança digital no ensino médio

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Estadual do Sudoeste da Bahia - UESB, como requisito necessário para obtenção do grau de Mestre em Matemática.

BANCA EXAMINADORA:

Prof. Dr. Flaulles Boone Bergamaschi - UESB

Prof. Dr. André Nagamine - UESB

Prof. Dr. Claudio Andrés Callejas Olguín - UFERSA

Vitória da Conquista - Ba

Aprovada em 05 de agosto de 2024

Documento assinado digitalmente
gov.br
CLAUDIO ANDRES CALLEJAS OLGUIN
Data: 07/08/2024 16:46:32-0300
Verifique em https://validar.iti.gov.br

Claudio Andrés Callejas Olguín - UFERSA

Documento assinado eletronicamente por **Flaulles Boone Bergamaschi**, **Professor Titular**, em 06/08/2024, às 10:44, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **André Nagamine**, **Professor Titular**, em 06/08/2024, às 11:09, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00095377414** e o código CRC **54DC1C9C**.

Resumo

Este trabalho tem como objetivo principal, apresentar a aplicabilidade da análise combinatória no ensino de matemática para estudantes do ensino médio, usando-a na mensuração de espaços amostrais dentro do contexto da segurança digital com foco na criptografia. Por meio do princípio fundamental da contagem e com inspiração na teoria dos registros de representação semiótica, busca-se gerar aprendizado expondo o estudante às diferentes formas de representação e tratamento de um objeto matemático.

Palavras-Chave: Criptografia; Análise Combinatória, Princípio Fundamental da Contagem, Aritmética Modular, Semiótica, Segurança Digital, Tabela Geradora de Senhas

Abstract

This work's main objective is to present the applicability of combinatorial analysis in teaching mathematics to high school students, using it to measure sample spaces within the context of digital security with a focus on cryptography. Through the fundamental principle of counting, inspired by the theory of semiotic representation records, in the search to generate learning by exposing the student to different forms of representation and treatment of a mathematical object.

Keywords: Cryptography; Combinatorial Analysis, Fundamental Counting Principle, Modular Arithmetic, Semiotics, Digital Security, Password Generator Table

LISTA DE TABELAS

LISTA DE QUADROS

Sumário

1 INTRODUÇÃO

A Matemática permeia os mais diversos setores do conhecimento humano, e num contexto de *sociedade digital*, onde a conectividade promovida pelos avanços tecnológicos, vem transformando a forma como o homem moderno vive, trabalha e se relaciona, não raro ocorre de o estudante de ensino médio ainda desconhecer como funcionam os princípios básicos das tecnologias que o cerca, não estando capacitado a lidar de modo coerente e seguro com elas.

Numa busca de coadunar os objetivos educacionais do ensino médio no que afirma a Base Nacional Comum Curricular (BNCC):

> (...) no Ensino Médio o foco é a construção de uma visão integrada da Matemática, aplicada à realidade (...). Nesse contexto, quando a realidade é a referência, é preciso levar em conta as vivências cotidianas dos estudantes do Ensino Médio, envolvidos, em diferentes graus dados por suas condições socioeconômicas, pelos avanços tecnológicos, pelas exigências do mercado de trabalho, pela potencialidade das mídias sociais, entre outros. (Brasil, 2017, p. 518)

Neste trabalho propõe-se uma forma de apresentação da *criptografia*, área na qual matemática e informática estão aplicadas, de modo levemente conceitual e experimental, aos alunos do ensino médio, considerando a sua relevância, por ser onde está fundamentada toda a segurança digital atual. Também abordar-se-á tipos de senha mais comumente usados e melhores escolhas de segurança para os dispositivos eletrônicos afim de proteger melhor os dados do estudante.

Abordando a questão do uso da tecnologia, uma das perguntas centrais do presente estudo é: “O que torna uma senha segura?”. Se fosse pedido a alguém que tente acertar um número de um caractere, este teria 10 possibilidades de acertar (números de 0 e 9), ou seja, cada uma das tentativas de descobrir o número (quebrar o código) teria 10% de probabilidade. Contudo, aumentando esse número para dois caracteres, qual seria a nova probabilidade de acerto? Qual o aumento da segurança de uma senha quando são inseridos letras e símbolos em conjunto com números? Análises como essas serão feitas nos capítulos posteriores com contribuições da Análise Combinatória, Probabilidade e Estatística, da Criptografia e aplicações da Aritmética Modular diversas a serem explanadas nesse trabalho.

Mais do que o desvendar de um quebra-cabeça, ou uma maneira jocosa de esconder alguma informação a criptografia pode ser um fator determinante para o sucesso de um empreendimento, justamente por permitir o sigilo de uma comunicação de eventuais curiosos. Pode também manter uma invenção em segredo dos concorrentes até a aprovação de sua

Patente, criptografando os dados cruciais da descoberta. Pois como afirma Sun T-zu, autor de A Arte da Guerra, quando trata a respeito da espionagem: *"*(...) *ninguém, em todo o exército, deve ser tratado com tanta familiaridade quanto os espiões, ninguém deve ser mais regiamente compensado do que eles, e nenhuma outra atividade deve ter os segredos mais bem preservados do que os espiões.*" (Sun T-zu, 2015, p. 152-153)

A importância da proteção de dados confidenciais tem vários marcos históricos como em 1918 a criação da cifra ADFGVX que garantiu, na Primeira Guerra Mundial, ao exército alemão a dianteira e o elemento surpresa, por conta de uma comunicação eficiente e sigilosa, fato esse que se converteu em desvantagem quando o francês Georges Painwin, no mesmo ano, quebra o código e dá vantagem aos Franceses. (conforme Singh, 2022. Pg 123-124.). Portanto a *quebra de sigilo* de uma informação observando apenas o fato isolado acima, determinou o rumo de um dos maiores conflitos da história da humanidade, sem a qual possivelmente as bandeiras poderiam ser diferentes das atuais.

Assim, essa teoria poderia se aplicar a um estudante de ensino médio? No atual contexto da revolução tecnológica do Século XXI, os "smartphones" vem ocupando a dianteira entre os meios de comunicação e operações sigilosas, com os aplicativos bancários como um dos principais meios de operações. Por exemplo temos as transações de transferência instantâneas PIX (pagamento ou transferências instantâneos), registradas no Sistema de Pagamentos Instantâneos (SPI), que vem numa crescente desde seu lançamento em 2020, como afirma o Banco Central Brasileiro: *"Após dois anos de lançamento, as transações via Pix ultrapassam a marca de mais de 30 bilhões de transações, com mais de 141 milhões de usuários."* (Brasil, 2022, p. 2). Sobre essas transações e comunicações existem diversos modos de criptografia.

Com a democratização crescente do acesso à tecnologia, não raro, adultos e adolescentes tem em seus aparelhos: contas de e-mail, aplicativos bancários, aplicativos de mensagens, redes sociais (costumeiramente usados para fins de trabalho e pessoais), bem como fotos e conversas que precisam ser protegidos. Como afirma Stein & Silva: *"À medida que a oferta de serviços online, tais como online bankings ou comércio eletrônico, cresce exponencialmente, a demanda por proteção de informações críticas vem aumentando na mesma proporção.*" (Silva; Stein, 2007, p. 48)

Mesmo com o uso de métodos de segurança como impressões digitais, reconhecimento facial, reconhecimento de voz, entre outros, as senhas alfa-numérico-simbólicas ainda se fazem necessárias, como afirma Silva & Stein:

> Apesar de suas falhas básicas e de causar problemas de memorabilidade para os usuários, sistemas de senhas ainda constituem a abordagem mais utilizada para autenticação. Em sistemas desse tipo, em primeiro lugar, a pessoa declara sua identidade, por exemplo, com um nome de usuário, e então revela ao sistema um código secreto ou palavra-chave, que somente o usuário deveria conhecer. As vantagens de sistemas de autenticação por senhas decorrem do fato de que estes não requerem equipamento especial, como leitores de impressões digitais. Ainda, se comprometidos por uma invasão, os objetos de identificação, isto é, nome de usuário e senha, podem ser alterados facilmente, e a um custo muito baixo. (Silva; Stein, 2007, p. 48)

Todavia, por conta da multiplicidade de dados, ter todas as senhas armazenadas apenas na memória é um risco. Contudo deixa-las anotadas em único lugar, também se torna um risco, especialmente para pessoas que viajam muito e precisam ter as senhas ao seu alcance. Vazamentos não autorizados de dados pessoais, em larga escala, são chamados nos sistemas de informação de *Data Breaches*. Um dos primeiros foi invasão a uma loja americana chamada DSW Shoe Warehouse, no ano de 2005, que resultou no vazamento de 1,4 milhões de números de cartões de crédito, e de modo mais recente a invasão do base de dados(do inglês *datasets*) do portal Yahoo, expondo dados pessoais de cerca 1 bilhão de usuários (conforme Roccia, 2021, p. 7). Para também ilustrar os riscos e prejuízos de vazamento de senhas Silva & Stein, citando o Jornal globo trazem:

> Em 29 de Novembro de 2005, em São Paulo, um estagiário do INSS de 18 anos foi preso e acusado de inserir dados falsos nos sistemas da previdência usando senhas de colegas. Em dois anos o jovem acumulou três milhões de reais. Ele adquiriu seis carros de luxo, equipamentos eletrônicos de alto custo e mobiliou sua casa com móveis de alta qualidade. (Silva; Stein, 2007, p. 49).

O que fazer então para acrescentar mais uma camada de segurança nesse processo? A sugestão neste trabalho é que se faça o uso da criptografia para a geração e codificação de senhas de aplicativos e contas pessoais, de modo que um leitor leigo ao observar o papel ou tabela onde estão as senhas, não saiba usá-las de imediato, contudo seu usuário possa usá-la sem a necessidade de se lembrar de tantas senhas, pois todas estarão codificadas por uma única palavra-geradora facilitando a vida do usuário, pois como afirmam Silva e Stein (2007) citando Norman:

> "Da mesma forma, quando o número de códigos secretos que uma pessoa precisa armazenar e ser capaz de lembrar aumenta muito, a memória pode falhar. Quando a memória fica sobrecarregada, pode ser muito difícil lidar com a variedade de dados necessários diariamente. Para as atividades diárias, temos que ter disponíveis em nossa memória desde números de telefone, números de contas bancárias, números de documentos e senhas; sem falar em informações mais pessoais tais como endereços, datas de aniversário, tamanhos de roupas, e assim por diante." (Silva; Stein, 2007, p. 47)

É importante que o estudante seja conscientizado acerca de como a Segurança Digital é gerida, e ser instruído em como proteger seus dados dentro de um ambiente cada vez mais

informatizado, este processo de informação permite que diversos conteúdos matemáticos sejam trabalhados, contextualizados ao tema, potencializando a abstração por parte dos estudantes. Dessa forma neste trabalho buscaremos o entendimento da Análise Combinatória, da Aritmética Modular, o contexto histórico da Criptografia, bem como aspectos mais atuais de recomendações de Segurança Digital que fundamentem a Sequência Didática construída, permitindo a mensuração dos dados ao final pelo professor-pesquisador.

2 REFERENCIAIS TEÓRICOS

Neste capítulo busca-se abordar as principais áreas matemáticas que constituem a fundamentação matemática do trabalho: análise combinatória, funções afins, aritmética modular e criptografia. Bem como, a teorias de ensino principia da aplicação do trabalho, semiótica e uso de sequências didáticas

2.1 Teoria da Análise Combinatória

A Análise combinatória é a área matemática responsável pelos métodos de contagem de elementos de um determinada lista ou conjunto, com uma característica própria, sendo uma "lista" um agrupamento onde a ordem de seus componentes influencia na contagem, de modo que se dois elementos são trocados de posição isso representa um novo agrupamento que deve ser contado. Sobre os conjuntos tomando a definição de conjunto Scheinerman aponta: *'Um conjunto é uma coleção de objetos, sem repetição e não ordenada. Determinado objeto é, ou não é, elemento de um conjunto - um objeto não pode figurar em um conjunto "mais de uma vez". Não há ordem para os elementos de um conjunto.'* (Scheinerman, 2011, p. 55, grifos do autor)

O estudo da Análise Combinatória depende de três ideias fundamentais: a relação biunívoca que associa cada um dos elementos contados a um número natural; a propriedade aditiva (Princípio Aditivo), dados dois conjuntos A e B, sem elementos em comum, a união deles ($A \cup B$) será a soma entre eles; a propriedade multiplicativa (princípio multiplicativo), havendo n conjuntos, sendo n um natural, sendo a intersecção entre quaisquer dois deles vazia, sendo que cada um deles associado a {1,2, ..., m}, a quantidade de elementos da reunião dos n conjuntos é o produto nm. (Vasques, 2011, p. 38)

Dentro das formas de contagem da análise combinatória uma das estruturas centrais de onde derivam seus ramos diversos é o Princípio Fundamental da Contagem (P.F.C.) que está relacionado a um número de decisões possíveis. Por exemplo sejam $D_1, D_2, \dots D_n$, com $n \in N$, as decisões possíveis para a formação de um determinado conjunto, tais que $D_1 = x_1, D_2 = x_2, \dots, D_n = x_n$, o número de elementos deste conjunto será o produto $x_1 x_2 \dots x_n$.

Existe uma estratégia de resolução de problemas próprias ao PFC que se explicita por: postura, divisão e não adiamento de dificuldades. Deste modo diante de um problema com essas especificidades é incentivada uma *postura participante*, para se colocar no lugar do personagem do problema refletindo as decisões a serem tomadas. Diante disso as possíveis decisões

precisam de uma subdivisão, em pequenos questionamentos com maior simplicidade, facilitando a resolução. Por fim, as decisões mais difíceis devem ser tomadas (contadas) em primeiro sempre que possível. (Morgado; Carvalho, 2015)

Entre as aplicações do Princípio Fundamental da Contagem temos a Permutação Simples (com ou sem repetição), Permutação Circular, Combinação Simples, Combinação Completa, sendo que a permutação circular não será abordada neste trabalho, enquanto que as demais serão vistas na sequência didática. Cabe ressaltar a notória diferença entre Permutações (também chamadas de Arranjos) e Combinações. A primeira, leva em consideração a ordem de um grupo de elementos, enquanto nas Combinações, a ordem dos elementos é suprimida, contam-se possíveis conjuntos, onde a ordem dos elementos é irrelevante.

Comumente nesses métodos de contagem surge a notação n!, leia-se "n fatorial" e , também a notação $\prod_{k=1}^{n} k$, que representa a multiplicação de números consecutivos em ordem de crescente $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1, \forall n \in \mathbb{Z}^{+}$. Scheinerman ressalta alguns casos específicos da notação:

> Merecem atenção dois casos especiais da função fatorial. Consideremos, em primeiro lugar, 1!. É o resultado da multiplicação de todos os inteiros a partir de 1 e até 1. A resposta é 1. Se isso não é bastante claro, voltemos à aplicação da contagem de listas. De quantas maneiras podemos fazer uma lista de comprimento 1, em que há apenas um elemento possível para preencher a primeira (e única!) posição? Obviamente, há apenas uma lista possível. Assim, 1! = 1. (Scheinerman, 2011, p. 51).

Outro caso explanado pelo autor é $0! = 1$, pois só existe um único modo de se dispor uma lista com zero elementos (Scheinerman, 2011, p. 51)

Um caso particular de permutação é o Arranjo Simples, de notação $A_{n,p} = \frac{n!}{(n-p)!}$, leia-se arranjo de *n* elementos tomados em *p* quantidades por vez, escolhendo então p elementos, do 1º ao elemento de ordem p, portanto a ordem em que os elementos são escolhidos, influencia na quantidade de conjuntos, o $(n-p)!$, garante que a contagem será encerrada após escolher a quantidade de elementos desejada. As Combinações, outra forma de permutação, levam em consideração o conjunto formado pela escolha de elementos, independente de ordem, sua notação é $C_{n,p} = \frac{n!}{p!(n-p)!}$, sua fórmula tem o *p!* no denominador, para desfazer a contagem de diferentes ordens de uma mesma quantidade de elementos escolhida. (Scheinermann, 2011).

Exemplificando as diferenças entre arranjos e combinações, por exemplo: Para a permutação de um conjunto com 3 elementos contamos que $(x_1; x_2; x_3) \neq (x_2; x_1; x_3)$, portanto são dois elementos distintos, contudo para a combinação esta diferença não existe, em

seu cálculo então, a quantidade de trocas entre os mesmos elementos será desfeita, seu uso depende da intencionalidade da contagem. Como na notação do Arranjo de um grupo de 3 elementos retirados de um grupo de 8 elementos temos $A_{8,3} = \frac{8!}{(8-3)!} = \frac{8!}{5!}$, já na combinação $C_8^3 = \frac{8!}{3!5!}$ a única diferença, para além de uma absorção de algoritmos, é a de que as permutações entre os 3 elementos (3!) será dividida da combinação.

Deste modo a permutação é mais utilizada para situações onde a mudança de ordem gera um produto diferente, como letras, números, disposição de cores, ordem de pessoas, etc., sendo a contagem das representações diversas dos elementos de um mesmo conjunto. A versatilidade destes métodos de contagem será útil posteriormente ao determinar o espaço amostral de cada tipo de senha.

Vejamos um exemplo de permutação simples sem repetição: Quantos são os modos de dispor 4 letras diferentes entre si, formando palavras com ou sem significado? Para esta contagem temos 26 decisões de primeira letra, 25 decisões de segunda letra, 24 de terceira letra e 23 de quarta letra, um arranjo de $n.(n-1).(n-2).(n-3)$ com $n = 26$ então o total A de permutações é:

$A = 26.25.24.23 = 358.800$ modos distintos. Se for eliminada a restrição das letras serem diferentes entre si, a quantidade de modos será $A = n^4 = 26^4 = 456.976$ modos distintos.

Nas combinações, a expressão $\frac{n!}{p!(n-p)!}$ para determinar o número de combinações de n (C_n^p) objetos tomados r de cada vez foi usada por Blaise Pascal primeiramente em 1653, no livro Traité du Triangle Arithmétique. (Eves, 2011) Tratando da abordagem de senhas e criptografia deste trabalho, em que a alteração da disposição dos elementos gera uma nova senha ou cifra, dentro do Princípio Fundamental da Contagem, as permutações simples ocuparão maior destaque para a determinação de espaços amostrais.

2.1.1 Combinação Completa

A combinação completa surge quando desejamos formar um conjunto com uma determinada quantidade de elementos, tomando esses elementos de mais de um grupo de origem distinto, sem delimitar qual a quantidade de elementos será tomada de cada grupo. Sua

abordagem vem da contagem de multiconjuntos de modo que $\binom{n}{k}$ que é a listagem de quantos subconjuntos de k elementos podem ser constituídos com os inteiros de 1 a n é tal que $CR_{n,k} = \binom{n+k-1}{k}$, sendo CR= combinação com repetição. Conforme Scheinerman salienta:

> Note que, dada uma sequência arbitrária de k *s e n-1|, podemos recuperar um multiconjunto único de cardinalidade k cujos elementos são escolhidos entre os inteiros l a n. Assim, há uma correspondência um a um entre multiconjuntos de k elementos escolhidos em {1,2, ..., n} e listas de estrelas e barras com k *s e n - 1|. A boa notícia é que não é difícil contar o número de tais listas de estrelas e barras. [...] Cada lista de estrelas e barras contém exatamente $n + k - 1$ símbolos, dos quais exatamente k são *s. O número de tais listas é $\binom{n+k-1}{k}$ porque podemos escolher exatamente k posições na lista de tamanho (n + k - 1) para serem *s. Em outras palavras, $n + k - 1$ posições nessa lista. Queremos selecionar, de todas as maneiras possíveis, um subconjunto de k elementos entre essas $n + k - 1$ posições. Podemos fazê-lo de $\binom{n+k-1}{k}$ maneiras. Portanto, $\binom{n}{k} = \binom{n+k-1}{k}$. (Scheinerman, 2011. Pg. 137-138)

Conforme explanado acima, com essa abordagem é utilizado um esquema de símbolos *(estrela) e |(barra) em que * representa os elementos do conjunto universo e '|' representa os (n-1) separadores usados para ter n subconjuntos, a isto é denominado **Codificação Estrelas-e-barras**. Por exemplo, dado o conjunto A={a,b,c,d} de quantos modos podemos escolher um subconjunto de 6 elementos (logicamente repetições serão permitidas}. Para esta contagem utilizando a Codificação Estrelas-e-Barras, podemos observar que:

Uma configuração possível é o subconjunto $\{a, a, a, a, a, a\} = ******|||$, outra seria $\{aaaccd\} = ***||**|*$. Portanto o total de subconjuntos possíveis (T) serão todas as configurações entre os seis símbolos '*' e os três símbolos '|', perfazendo $T = \binom{9}{6} = \frac{9!}{3!6!} = 84$ subconjuntos, salientando que $\binom{9}{6} = \binom{4+6-1}{6}$.

2.2 Funções

Funções ocupam um espaço considerável na literatura matemática, por ser um de seus pilares, também pela aplicabilidade em diversas situações. Uma função é definida como uma relação de associação entre os elementos de dois conjuntos. Embora seja comum sua apresentação nos livros didáticos como sendo uma "função real", ou seja uma função com domínio pertencente ao conjunto dos números reais, e seja explicitada apenas por sua lei de associação, geralmente uma fórmula algébrica, esta abordagem não abarca todas as condições necessárias de uma Função, como coaduna Elon Lages:

> A preocupação com domínio e contradomínio na definição de uma função é abandonada e a ênfase passa a se concentrar apenas nas fórmulas algébricas. Os dois contextos anteriores são então deixados de lado e esta passa a ser a abordagem predominante no restante dos livros. Geralmente, poucas relações são estabelecidas entre esses três contextos. Em alguns casos, a separação é tão estrita, que pode causar a impressão de que o termo "função" é empregado para noções matemáticas inteiramente distintas, que por acaso recebem o mesmo nome. (Lima, 2012, p. 138)

Sobre as relações entre domínio, imagem e contradomínio de uma função. Elon Lages define as regras dessa relação para seja uma função:

> (i) Os conjuntos X e Y são chamados **domínio** e **contradomínio** de f, respectivamente; (ii) O Conjunto $f(X) = \{y \in Y\ ;\ \exists x \in X, f(x) = y\} \subset Y$ é chamado **imagem** de f; (iii) Dado $x \in X$, o (único) elemento $y = f(x) \in Y$, correspondente é chamado **imagem** de x. (Lima, 2012, p. 44)

Uma função pode ser considerada Injetora, Sobrejetora ou Bijetora (também denominadas Injetiva, Sobrejetiva e Bijetiva). A primeira dessas é uma função $f: X \to Y$, sendo $x, y \in R$, tal que tomando x_1, x_2 tais que $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, assim dois ou mais elementos do domínio não têm jamais, na função injetora, a mesma imagem, também é válido para a igualdade $f(x_1) = f(x_2) \to x_1 = x_2$. Na segunda função, também de domínio e imagem reais, com o conjunto Contradomínio {C(f)} Y tal que, $\forall y \in Y;\ \exists x \in X$ assim sendo $f(x) = y$, nessa tipo de função a imagem é igual ao contradomínio, nenhum dos elementos do contradomínios estão fora da imagem da função.

Dizemos que uma função é bijetoras se é simultaneamente injetora e sobrejetora, a bijeção é uma característica mister para a inversibilidade de uma função, se a função não for bijetiva, não será invertível. Antes de demonstrar a prova da Bijeção é necessário definir que duas funções $f: \mathbb{R} \to \mathbb{R}$, são iguais quando tomando $x = x'$, sendo $f: X \to Y$ e $g: X' \to Y'$ tais que $f(x) = g(x')$.

2.2.1 Funções Afim

A lei de associação de uma função afim tem forma base: $f(x) = ax + b$, onde 'a' é denominado coeficiente angular, e *'b'* é denominado constante (ou coeficiente linear). A coordenada (0,b) é o ponto onde o gráfico da função intersecta o eixo OY, e a coordenada $\left(-\frac{b}{a}, 0\right)$ é o ponto onde gráfico da função intersecta o eixo OX, o que não ocorre para o caso de função afim constante. De modo geral para determinar o valor da constante basta determinar tomar $x = 0$, logo $f(0) = b$.

A função afim propriamente dita, acontece quando se têm constantes reais *a,b* de modo que exista $f(x) = ax + b$, para todo $x \in R$. (Lima, 2012). Dentre suas modalidades, considerando domínio e contradomínio dentro dos reais, tende-se as funções: identidade, translações, lineares e constantes, sendo a primeira delas com domínio e imagens iguais, $f(x) = x$, a segunda tem coeficiente $a = 1$, assumindo a forma $f(x) = x + b$, nas lineares temos coeficiente $b = 0$, assim $f(x) = ax$, esse tipo de função está notoriamente ligada a aspectos de proporcionalidade.

Nas Funções Constantes temos o coeficiente $a = 0$, dessa forma $f(x) = b$, portanto nesta a variável x não influencia o valor de y. A função constante e a linear são consideradas casos particulares. De modo geral os gráficos das funções afins são representado por reta, que pode ser ascendente para $a > 0$, descendente quando $a < 0$ ou constante quando $a = 0$.

Nas aplicações da sequência didática para a criptografia, foram usadas de modo mais proeminente as funções afim do tipo translação. Para não esbarrar em possíveis carências de aprendizado dos estudantes quanto a operações com racionais, assim permanecendo domínio e imagem ao conjunto dos inteiros, todavia nada impede que as aplicações passam ser feitas usando funções com $a \neq 1 \; ou \; a \neq -1$, pois considerando que funções afim são bijetoras, usando o domínio dos números inteiros, como é próprio da aritmética modular, a imagem da função inversa também pertencerá ao conjunto dos inteiros.

2.3 Aritmética Modular

A aritmética modular é definida como a aritmética que estuda fenômenos cíclicos, vinda das relações de equivalência. As relações de equivalência R, que acontece no conjunto A, de modo que os elementos deste conjunto se relacionam entre si, assim: $R \subset AxA$. O símbolo $\sim$ (til) é usado como símbolo representativo dessa relação, tomando $a, b, c \in A$, as condições de existência deste tipo de relação estão nela cumprir as 3 propriedades a seguir:

I) Propriedade Reflexiva, assim $a \sim a$;

II) Simétrica, se $a \sim b$ então $b \sim a$;

III) Transitivas, de modo que se $a \sim b \; e \; b \sim c$ então $a \sim c$.

Na aritmética modular essa relação de equivalência é denominada *congruência*, ou *classe de congruência*, e está aplicada aos números Inteiros. Ela é uma relação de equivalência

nos inteiros, onde o resto é o objeto de estudo, de modo que dois números $a, b \in \mathbb{Z}$, são chamados *congruentes módulo n*, com $n \in \mathbb{Z}^+$. Se $a - b = kn$, cuja notação fica $a \equiv b\ (mod\ n)$, leia-se 'a' é congruente 'b' módulo n. Nesse caso $a = b + kn$ e $b = a + qn$, para algum $k, q \in N$. (Carneiro, 2017).

Comumente é usada na forma $a \equiv r\ (mod\ n)$, sendo r o resto da divisão de n por a, de modo que $n|(a - r)\ e\ a = kn + r$ para $k \in Z$, e para n|a (n divide a) temos que $r = 0$. Assim por exemplo $30 \equiv 2(mod\ 7)$, pois $30 = 4.7 + 2$, ou $30 \equiv 0(mod\ 6)$ pois $6|30$. Dessa forma podemos afirmar que {30; 23; 16; 9; 2} são representantes dos números pertencentes a classe de equivalência $2(mod\ 7)$, sendo formalmente representada como $\overline{2} = \{2 + 7k, k \in \mathbb{Z}\}$. (Coutinho, 2014)

Portanto a Aritmética Normal é diferente da Modular, por exemplo, na aritmética comum, tomando em comparação a função $f(x) = 5^x\ e\ g(x) = 5^x(mod\ 7)$, observando a tabela abaixo que o a função na aritmética modular terá caráter cíclico, considerando que no exemplo dado o conjunto imagem de $g(x)$ tem somente 7 classes de equivalência possíveis $(\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$:

X	1	2	3	4	5	6	7	...
$f(x) = 5^x$	5	25	125	625	3125	15625	78125	...
$g(x) = 5^x(mod\ 7)$	5	4	6	2	3	1	5	...

Na tabela dada que a função é constituída por potências de 5, em nenhum momento a classe $\overline{0}$ aparecerá, por não existir um inteiro de base 5 divisível por 7.

O cálculo de um resto de divisão, utilizando a aritmética modular se torna relativamente simples. Por exemplo para encontrar o resto do produto $246 \cdot 348$ numa divisão por 7 temos:

$246 \cdot 348 \equiv (6 \cdot 41)(6 \cdot 2 \cdot 29) \equiv (6 \cdot 6)(12 \cdot 1) \equiv (36)(12) \equiv (1)(5) \equiv 5(mod\ 7)$

onde em vez de efetuar o produto, para depois a divisão por 7, vamos decompondo cada parcela em fatores menores, substituindo cada fator maior do que 6 pelo seu resto correspondente na divisão por 7, como acontece com 41, 29, 36 e 12, pois $(41 = 5 \cdot 7 + 6); (29 = 4 \cdot 7 + 1); (36 = 5 \cdot 7 + 1)$ e $(12 = 1 \cdot 7 + 5)$

Ainda que monótono, é simples encontrar os resultados de uma função modular, quando lidamos com números relativamente pequenos, todavia quando se observa a realidade dos números primos, especialmente os primos de maior quantidade de casas decimais determinar o resultado de uma função torna-se uma tarefa muito mais complexa, essa dinâmica de números

primos grandes que fez da aritmética modular, um forte campo de estudo para a Criptografia como se detalhará posteriormente.

2.4 Código e Criptografia

Os estudos de criptografia trazem alguns termos bem distintos dos usuais das outras áreas matemáticas, a saber: código é substituição de palavras ou frases; cifra é a substituição de letras; codificar é esconder usando um código; decodificar é a tradução de uma mensagem cifrada (ou codificada).

A palavra criptografia, vem de kryptos, do grego, significa secreto, oculto. Unida a *grafia*, significa escrita oculta. Sobre seus estudos, Coutinho define: *"A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la"* (COUTINHO, 2014). Para que isso ocorra, emissor e destinatário da mensagem precisam conhecer o modo como a comunicação foi encriptada, qual o processo de embaralhamento da mensagem utilizado, já que a encriptação errada, bem como, a desencriptação errada geram falhas sensíveis na comunicação.

Os modos de codificação são diversos, e visam garantir o sigilo do conteúdo de uma comunicação, seja ela analógica ou digital, o método de cifragem é também conhecido como *algoritmo*, assim como o método de codificação de uma mensagem em específico é denominado *chave.* Singh citando Kerckhoff detalha a usabilidade desses termos que resultam no Princípio de Kerckhoff: *"A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave"* (Singh apud Kerckhoff, 2022, p. 28)

Contudo ao longo da história da humanidade houveram personagens que viram alguma vantagem na interceptação de mensagens secretas, para tanto, era necessário a quebra do código, essa necessidade tornou-se uma área de estudo a parte, denominada criptoanálise, a qual evoluiu quase que paralelamente a criptografia pois a cada nova cifra criada, um novo método de quebra de código era criado. E de modo análogo para cada código quebrado pelos criptoanalistas, uma nova forma de criptografia busca de reestabelecer o sigilo e segurança de suas comunicações.

Para que um sistema criptográfico funcione é necessário que ele atenda a três propriedades:

I. Seja reversível, do contrário a mensagem não poderá ser decodificada jamais
II. O receptor detenha a chave de desencriptação
III. Não gere interpretações dúbias

Existem dois ramos principais da criptografia: transposição e substituição. Seu uso não necessariamente é feito separadamente, podendo ser combinadas em alguns tipos de cifras. Na transposição existe um embaralhamento da mensagem, formando anagramas, como por exemplo a palavra "agora" pode ser criptografada como "garoa". Este tipo de cifra apresenta fraquezas para mensagens curtas pois com uma criptoanálise relativamente simples pode-se estudar todos os anagramas possíveis, neste caso $\frac{5!}{2!} = 60$ palavras possíveis. Segundo Singh, à medida que o número de letras de uma mensagem aumenta, aumenta também a força deste tipo de cifra:

> "Entretanto, à medida que o número de letras aumenta, o número de arranjos possíveis rapidamente explode, tornando impossível obter-se a mensagem original, a menos que o processo exato da mistura das letras seja conhecido. **Como exemplo vamos considerar essa frase.** (grifo do autor) Ela contém apenas 35 letras, e no entanto existem mais de 50.000.000.000.000.000.000.000.000.000.000 de arranjos distintos. Se uma pessoa pudesse verificar uma disposição por segundo, e se todas as pessoas no mundo trabalhassem dia e noite, ainda assim levaria mais de mil vezes o tempo de existência do universo para checar todos os arranjos possíveis. (SINGH, 2022, p. 23)

Uma criptografia de transposição com embaralhamento ao acaso, tornaria então praticamente impossível o processo de leitura da mensagem por terceiros, contudo o fator de acaso impossibilitaria a leitura da mensagem pelo destinatário, já que deixaria um anagrama de difícil compreensão. Dessa forma é necessário que a cifragem de transposição seja feita por um sistema lógico, para que o destinatário possa fazer sem grande dificuldade a reversão do processo de cifragem.

2.5 Teoria dos Registros de Representação Semiótica

Na semiótica a relação entre símbolos e significados influenciam fortemente o aprendizado matemático, pois esta que é fortemente abstrata, é beneficiada com símbolos que representem esses dados abstratos, por exemplo os conjuntos numéricos e suas representações $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ que simbolizam respectivamente os conjuntos naturais, inteiros, racionais e reais.

Considerando a capacidade de transformação de informações inerente a criptografia, especificamente os critérios matemáticos com os quais cada tipo de criptografia realiza a transformação e o tratamento dos seus dados, tais aspectos fazem da teoria dos registros de

representação semiótica, de Raymond Duval, um sustentáculo necessário e adequado ao pensar a criptografia aplicada num contexto de educação matemática.

A teoria é baseada entre *objeto* e *representação*, para que o conhecimento seja bem definido ao estudante, segundo a semiótica, o objeto deverá estar bem definido, não sendo confundido com suas *representações*, além disso, em cada uma de suas representações deverá o estudante ser capaz de reconhecer o objeto. As representações são todas as formas de se representar um objeto matemático, sejam elas textuais, simbólicas, imagéticas (constituídas por figuras não geométricas), formas geométricas, entre outras, não contendo o objeto em si, já que este pode ter mais de uma representação.

Enquanto abordada dentro da teoria dos registros de representação xemiótica, a palavra "Objeto" se refere também a conhecimento ou conteúdo matemático. Registros de Representação, são espécies de categorias de representações, organizadas conforme os próprios fatores cognitivos de cada uma. (Duval, 2023). A formação desses diferentes Registros é algo comum à história da humanidade, pois as ciências tendem a criar Sistemas de Registro de Representação Semióticas independentes da língua natural, como os símbolos químicos da Tabela Periódica, o Sistema Internacional de Medidas (S.I.), a escrita algébrica, o cálculo numérico, entre outros, para que não seja necessário a *conversão* entre idiomas antes da compreensão do exposto.

Na teoria as representações são articuladas e constituídas por meio de *signos* que são próprios a cada uma delas, os signos recebem a definição de Duval: "Unidades elementares de sentido, que são apenas caracteres para codificar: letras, siglas, algarismos, às vezes palavras-chave, ou os gestos de mão. O que equivale a considerar os signos como as "coisas" pelas quais é preciso começar para dar um sentido" (Duval, 2011. P. 38). Sendo, portanto, o alicerce onde todos os sistemas de registro são construídos.

A teoria é balizada entre dois distintos aprendizados, um podendo ser considerado o meio e o outro o fim (objetivo final), que é a dialógica entre *semiose* e *noesis*, os dois processos referentes ao aprendizado, onde a Semiose é ligada aos processos envolvendo uma representação semiótica e a noesis está ligada ao processo envolvendo o *objeto matemático*. Como afirma Duval:

> "O funcionamento cognitivo do pensamento humano se revela inseparável da existência de uma diversidade de registros semióticos de representação. Se é chamada "semiose" a apreensão ou a produção de uma representação semiótica, e "noesis" a apreensão conceitual de um objeto, é preciso afirmar que a noesis é inseparável da semiose." (Duval, 2023, p. 5)

Assim a forma como cada objeto pode ser apresentada, consiste em um aprendizado em si mesma, por exemplo ao se abordar análise combinatória (objeto), é necessário que estudante esteja familiarizado com fatoriais, produtos e quocientes racionais, que consistem em uma de suas representações, outra representação são os problemas e estudos de caso, (representações textuais) onde a análise combinatória é também expressa. Quanto a justificativa de uso de representações semióticas, Duval afirma:

> "Não obstante, as diversas representações semióticas de um objeto matemático são absolutamente necessárias. De fato, os objetos matemáticos não estão diretamente acessíveis à percepção ou à experiência intuitiva imediata, como são os objetos comumente ditos "reais" ou "físicos". É preciso, portanto, dar representantes." (Duval, 2023, p. 3)

Ademais, segundo a teoria, o processo de aprendizado se consolida quando o estudante consegue identificar um objeto em suas diversas representações, conseguindo realizar a interpretação e cálculo (tratamento) em cada uma delas, bem como, fazer as transformações (conversões) entre uma representação e outra quando houver a necessidade, esse processo tem para a teoria um fator afirmativo no desenvolvimento das habilidades cognitivas.

Como afirma Duval (2023) "No entanto, é essencial, na atividade matemática, poder mobilizar muitos registros de representação semiótica (figuras, gráficos, escrituras simbólicas, língua natural etc...) no decorrer de um mesmo passo, poder escolher um registro no lugar de outro." (Duval, 2023, p. 6). Nessa necessidade intrínseca que a aprendizagem dos objetos tem dos registros de representações que o autor define como: Paradoxo Cognitivo do Pensamento Matemático, onde é possível o sujeito confundir o objeto com representação, pois o processo de aprendizado de ambas é circular, quanto melhor se entende a representação, melhor é o aprendizado do Objeto, contudo o aprendizado deste reforça a representação. (Duval, 2023)

Dentre os processos da Semiótica tem-se: *formação*, *tratamento* e *conversão*. Conceituados a seguir.

I) Formação

É a seleção de signos que comporão as representações de um Sistema de Registro, seleção essa feita em função da Categoria de Representação que se deseja. Deverá ser identificável facilmente, para que ao observar uma determinada formação o sujeito reconhece de qual representação ela se trata, e de qual objeto. Cada formação deve ter seu conjunto de regras internas, suas unidades. Sobre essas regras de formação Duval afirma:

> Esta formação deve respeitar regras (gramaticais para as línguas naturais, regras de formação num sistema formal, entraves de construção para as figuras...). A função

> destas regras é de assegurar, em primeiro lugar, as condições de identificação e de reconhecimento da representação e, em segundo lugar, a possibilidade de sua utilização para tratamentos. São regras de conformidade, não são regras de produção efetiva por um sujeito. Isto quer dizer que o conhecimento de regras de conformidade não está relacionado a competência para formar representações, mas somente para reconhecê-las. (Duval, 2023, p. 7)

Conceituaremos tratamento a seguir, contudo as regras de formação são extremamente necessárias para seus processos pois determinam suas leis internas, suas possibilidades. Ademais as regras sendo bem definidas permitem ao sujeito identificar o tipo de registro cognitivo que se deseja criar uma representação a partir delas.

II) Tratamento

Tratamento são os processos de transformação interna de uma representação, que ocorrem dentro de seu mesmo sistema de registro. Os tipos de tratamentos são vários, variando para cada categoria, e havendo vários dentro de uma mesma categoria, que vão ser usados conforme a necessidade para aprendizado do objeto. Também dispõe de regras internas, que não devem contradizer as regras de formação da representação e são diversos como afirma Duval:

> Há, naturalmente, regras de tratamento próprio a cada registro. Sua natureza e seu número variam consideravelmente de um registro a outro: regras de derivação, de coerência temática, associativas de contiguidade e de similitude. No registro da língua natural há, paradoxalmente, um número elevado de regras de conformidade, e poucas regras de tratamento para a expansão discursiva de um enunciado completo. (Duval, 2023, p. 7)

Um exemplo de tratamento é a codificação, usada na criptografia, quando ela substitui caracteres por outros caracteres dentro da mesma representação, temos também secção dentro das figuras geométricas, paráfrase dentro da linguagem textual, funções afim dentro do *registro algébrico* que entregam um *y* dentro da mesma representação para cada *x* dado.

III) Conversão

A conversão de registros é a transição entre diferentes registros de sistema de tratamento semiótico, para que ocorra, deverá haver uma conservação de parte ou da totalidade da representação inicial. É uma atividade cognitiva bem diferente do Tratamento, daí a importância de utilizar ambos para um maior estímulo do aprendizado.

Exemplificando a conversão: se há uma tabela representando um conjunto de 6 pontos distintos de uma função afim e se quer convertê-la em um gráfico no plano cartesiano, este

gráfico ao ser feito representará a mesma função (objeto/conceito), contudo disporá de infinitos pontos pertencentes a função.

Por outro ângulo, na conversão do gráfico para a tabela deverão ser selecionados alguns pontos representantes da função, pois como esta dispõe de infinitos pontos, não é viável transcrever todos na Tabela pois perderia o caráter resumido desse tipo de registro de representação. É notável que na conversão da tabela para gráfico, toda a informação do sistema de partida, estava contida no sistema de chegada, o recíproco não é verdadeiro, pois na conversão de gráfico para tabela apenas parte do conteúdo foi conservado.

Aprofundando o conhecimento sobre conversão, Duval afirma:

> Para a expressão de um número é preciso, de fato, distinguir a significação operatória ligada ao significante, em virtude das regras do sistema de expressão escrita (esta significação operatória não é a mesma para $0{,}25$, ¼ e 25.10^{-2}: não são os mesmos tratamentos que devem ser considerados para efetuar as adições $0{,}25 + 0{,}25 = 0{,}5$; $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ *e* $25 \times 10^{-2} \times 25.10^{-2} = 50 \times 10^{-2}$ e o **número representado que não é o significante 0,25, nem o significante $\frac{1}{4}$ e nem o significante 25×10^{-2}. Cada uma destas três expressões tem uma significação operatória própria, mas representa o mesmo número.** (Duval, 2023, p 8, grifos do autor)

O exemplo citado acima, consiste em um exemplo elementar das dificuldades operatórias matemáticas dos estudantes do ensino médio, pois ao terem no ensino os conteúdos de frações, decimais e potências ensinados de modo isolado, ou se esperando que a conversão entre eles fosse um processo espontâneo ao estudante, faz com que estes não reconheçam os 3 resultados das operações citadas como o mesmo número.

Outros exemplos de conversão são:

Ilustração: Linguístico → Figural

Tradução: Idioma 1 → Idioma 2

Descrição: Não Verbal → Linguístico

A transição entre dois diferentes sistemas de registro, segue dois casos particulares: caso de congruência e caso de não-congruência. No primeiro, quando existe uma correspondência clara entre os elementos dos dois sistemas, a conversão é quase que intuitiva. Já no segundo caso o processo não é tão natural, pois não há um método geral para todos os casos de conversão entre as diversas representações de *partida* e as de *chegada*. Essa coordenação para as conversões entre os diferentes registros não surge de modo espontâneo nos sujeitos, embora o ensino esteja estruturado como se essa espontaneidade fosse natural. (Duval, 2023)

Aspectos cognitivos da Teoria

Para a teoria de Durval a importância cognitiva do processo de transferências de registros, reside em que cada na oportunidade dos tipos de tratamentos próprios que cada registro em si oferece, assim um conceito ou objeto cognitivo serão analisados sobre diferentes aspectos, muitas vezes com um substancial grau de independência entre si, porém inter-relacionados por meio da conversão.

Portanto o ensino do conteúdo por meio de conversões permite que formas de abordagens deste, muitas vezes vistas como isoladas durante o ensino, possam ser integralizadas como afirma Duval:

> Pode-se observar, em todos os níveis de ensino, na grande maioria dos alunos, um enclausuramento de registros de representação. Estes não reconhecem o mesmo objeto nas representações que são dadas em sistemas semióticos diferentes: a expressão algébrica de uma relação e sua representação gráfica [...]; a expressão numérica de uma relação e sua representação geométrica sobre uma reta ou no plano; o enunciado de uma fórmula em francês e a expressão desta fórmula na forma literal; a descrição de uma situação e a sua equação matemática correspondente; etc. Este isolamento subsiste, mesmo após um ensino de conteúdos matemáticos que tenha tido estes diferentes registros amplamente utilizados. (Duval, 2023, p. 18)

Essa ausência percebida, nos sistema de ensino, de processos que favoreçam a conversão sistemas de registro semióticos, não tem caráter impeditivo quanto ao aprendizado, todavia, não atuam como facilitadoras para o estudante, promovem o isolacionismo dos objetos de aprendizado, não promovendo a habilidade de bem utilizar os conhecimentos em situações completamente distintas (situações de outros sistemas semióticos) por não terem aprendido a interrelacioná-los, o que é denominado por Duval como Compreensão Mono Registro.

Ainda que a conversão seja de grande importância, Duval não incentiva exercícios focados na conversão entre diferentes registros, afirmando que a Coordenação entre os diferentes registros deve ser favorecida por conscientização, buscando propostas mais Globais, dada a infinidade de Registros, não se pode apresentar todo tipo de conversão particular, mas, conscientizar que os Objetos de Ensino podem aparecem nas mais distintas formas e que para cada um é necessário a compreensão de seus diferentes Registos. (Duval, 2023)

A Teoria sugere então três modos de se trabalhar atividades na perspectiva de formar corretas relações de Noesis e Semiose:

I) Apreensão das Representações Semióticas: Onde é necessário tomar conhecimento do comportamento das variações, internas do registro, tanto do registro de partida quanto do conjunto de chegada, desta forma é possível sugerir uma situação de Variação Sistemática. Por exemplo a conversão de temperatura de escala Célcius para Fahrenheit, onde é necessário conhecer a forma de variação de cada escala para sugerir uma conversão entre elas.

II) Aprendizagem de um Tratamento Próprio de uma certa Categoria de Registros, como os exemplificados inicialmente, Algébricos, Geométricos, Figurais, entre outros. Existindo um certo domínio nos tratamentos de uma categoria torna-se mais promissor o desenvolvimento de conversões entre Registros dentro dessas categorias.

III) Produção de Representações Complexas

Quando a organização das representações apresenta características lineares, será necessária uma organização anterior em um outro registro não-linear, Duval detalha: "*Chama-se representação complexa toda representação que "expõe um procedimento": um texto, um cálculo com diversas etapas, um raciocínio."*(Duval, 2023, p. 28)

3. ASPECTOS METODOLÓGICOS

Aplicações matemáticas envoltas a esfera da informática e segurança digital oferecem uma oportunidade salutar para que o estudante do ensino médio vislumbre como a matemática e suas diversas vertentes contribuem com o funcionamento da sociedade, e estão mais próximas de seu contexto, indo para além do carácter abstrato que lhe é próprio a ela em muitas de suas vertentes.

Na criptografia são aplicadas desde as operações aritméticas mais básicas, além de amplificar a divisão pelo uso do Algoritmo de Euclides, dando ênfase ao Resto da Divisão, ela também admite aplicações nas áreas de funções, podendo elas comporem os algoritmos que codificam as informações, dentre essas funções ocupa destaque a de Aritmética Modular que apesar de sua versatilidade comumente está fora do escopo curricular do Ensino Médio, contudo oferece oportunidade para aplicações das operações essenciais aritméticas.

Permeando noção de "força" de uma criptografia, são comumente usados como parâmetros avaliativos desta como a quantidade de resultados possíveis (quantidade de senhas possíveis) de um algoritmo, sendo a cifra mais forte aquela que gera um espaço amostral maior, gerando menor probabilidade de ser "quebrada" por criptoanalistas. O resultado dessas análises pode ser exposto em forma de porcentagens com o auxílio de gráficos, tabelas, imagens, etc. Assim o estudo da criptografia pode proporcionar o aprofundamento dos conhecimentos da análise combinatória e probabilidade, trabalhando também a habilidade do tratamento da informação. Como aponta a BNCC para o ensino médio:

> Para o desenvolvimento de habilidades relativas à Estatística, os estudantes têm oportunidades não apenas de interpretar estatísticas divulgadas pela mídia, mas, sobretudo, de planejar e executar pesquisa amostral, interpretando as medidas de tendência central, e de comunicar os resultados obtidos por meio de relatórios, incluindo representações gráficas adequadas. (BRASIL, 2017, p. 518)

O conteúdo de segurança digital oferece várias problemáticas a serem levantadas pelo estudante, de modo que sob uma orientação investigativa docente, estes sejam instigados a se preocupar com a segurança de suas mídias sociais, contas bancárias e aparelhos eletrônicos, avaliando quais têm sido as fraquezas de suas senhas, bem como saber criar senhas mais fortes, o que sob a intencionalidade didática deverá ser feito com argumentação matemática bem fundamentada, permitindo a aplicação e revisão de conteúdos diversos desta área, buscando fortalecimento do aprendizado e fomentação de competências como afirma a BNCC:

> Assim, para o desenvolvimento de competências que envolvem o raciocinar, é necessário que os estudantes possam, em interação com seus colegas e professores, investigar, explicar e justificar os problemas resolvidos, com ênfase nos processos de argumentação matemática. Embora todas as habilidades pressuponham a mobilização do raciocínio, nem todas se restringem ao seu desenvolvimento. Assim, por exemplo, a identificação de regularidades e padrões exige, além de raciocínio, a representação e a comunicação para expressar as generalizações, bem como a construção de uma argumentação consistente para justificar o raciocínio utilizado. (Brasil, 2022, p. 519)

Salienta-se a importância do supracitado de que o desenvolvimento do pensamento do estudante não deve ser posto numa perspectiva individualista, acontecendo em grande parte pelo trabalho coletivo, pela interação e trocas não só com os professores, mas, também com seus colegas.

Os processos metodológicos atribuídos na aplicação prática deste trabalho, detalhados posteriormente, visam voltar o aluno ao desenvolvimento de habilidades e competências como relacionadas na BNCC. As temáticas abordadas com os alunos tendem a trabalhar habilidades das cinco competências de Matemática e suas tecnologias: 1) Interpretação Matemática em diversos contextos através de estratégias, conceitos e procedimentos; 2) Investigação de desafios diversos do Mundo Contemporâneo amparados na articulação de conhecimentos matemáticos; 3) Interpretar, construir modelos e resolver problemas com o uso de estratégias, conceitos e procedimentos matemático aplicados aos suas subáreas: Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística; 4) Compreensão e uso de diferentes formas de representação de registros matemáticos em vista de solucionar problemas e comunicar essas resoluções; 5) Uso de recursos e estratégias, seja tecnológicas, seja observações de padrões ou experimentações para investigação e conjecturação sobre diferentes conceitos matemáticos. (Brasil, 2018)

Entre as habilidades divididas entre as competências supramencionadas, as que estão em torno da proposta de abordagem da Segurança Digital na Criação de Senhas, bem como, os seus subtemas, são:

> (...) (EM13MAT102) Analisar gráficos e métodos de amostragem de pesquisas estatísticas apresentadas em relatórios divulgados por diferentes meios de comunicação, identificando, quando for o caso, inadequações que possam induzir a erros de interpretação, como escalas e amostras não apropriadas. (...) (EM13MAT202) Planejar e executar pesquisa amostral usando dados coletados ou de diferentes fontes sobre questões relevantes atuais, incluindo ou não, apoio de recursos tecnológicos, e comunicar os resultados por meio de relatório contendo gráficos e interpretação das medidas de tendência central e das de dispersão. (EM13MAT203) Planejar e executar ações envolvendo a criação e a utilização de aplicativos, jogos (digitais ou não), planilhas para o controle de orçamento familiar, simuladores de cálculos de juros compostos, dentre outros, para aplicar conceitos matemáticos e tomar decisões. (...) (EM13MAT302) Resolver e elaborar problemas cujos modelos são as funções polinomiais de 1º e 2º graus, em contextos diversos, incluindo ou não tecnologias digitais. (EM13MAT303) Resolver e elaborar problemas envolvendo porcentagens

> em diversos contextos e sobre juros compostos, destacando o crescimento exponencial. (...) (EM13MAT310) Resolver e elaborar problemas de contagem envolvendo diferentes tipos de agrupamento de elementos, por meio dos princípios multiplicativo e aditivo, recorrendo a estratégias diversas como o diagrama de árvore. (EM13MAT311) Resolver e elaborar problemas que envolvem o cálculo da probabilidade de eventos aleatórios, identificando e descrevendo o espaço amostral e realizando contagem das possibilidades. (...) (EM13MAT315) Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma. (...) (EM13MAT408) Construir e interpretar tabelas e gráficos de frequências, com base em dados obtidos em pesquisas por amostras estatísticas, incluindo ou não o uso de softwares que inter-relacionem estatística, geometria e álgebra. (EM13MAT409) Interpretar e comparar conjuntos de dados estatísticos por meio de diferentes diagramas e gráficos, como o histograma, o de caixa (box-plot), o de ramos e folhas, reconhecendo os mais eficientes para sua análise. (...) (EM13MAT508) Identificar e associar sequências numéricas (PG) a funções exponenciais de domínios discretos para análise de propriedades, incluindo dedução de algumas fórmulas e resolução de problemas. (Brasil, 2018, p. 525-534)

Em suma as habilidades trabalhadas devem focar o estudante no pensamento estratégico matemático, inter-relacionando conhecimentos de funções, análise combinatória, probabilidade, de modo a contribuir com o desenvolvimento do raciocínio matemático mediante subsídios para tomada de decisão sobre segurança digital, contribuir também para a argumentação e tratamento de dados através das diversas representações, gráficas ou não, dos resultados dos estudos.

3.1 Sequência Didática

Ao fim deste trabalho será proposta uma sequência com o objetivo de associar a criptografia a outros objetos matemáticos, as sequências didáticas são a forma que se pretende abordar esses conteúdos com os estudantes, são definidas como um conjunto ordenado de atividades, com articulação entre elas que formam unidades didáticas. (Zabala, 2014)

O modo como essas Sequências são escolhidas, dentre seus diversos tipos, dará a tonalidade das relações entre professores e alunos, bem como seus papéis em cada atividade, em vista da construção do conhecimento ou da aprendizagem, pois são fatores importantes para formar o vínculo afetivo que atua como favorecedor, quando positivo, da prática educacional, como afirma Zabala:

> A forma de estruturar os diferentes alunos e a dinâmica grupal que se estabelece configuram uma determinada organização social da aula em que os meninos e meninas convivem, trabalham e se relacionam segundo modelos nos quais o grande grupo ou os grupos fixos e variáveis permitem e contribuem de uma forma determinada para o trabalho coletivo e pessoal e sua formação. (Zabala, 2014, p. 26-27)

Pois como metodologia de ensino, a sequência deve ser pensada e usada com um planejamento pedagógico, uma intencionalidade de contribuir na formação do discente em um ou mais determinados objetos de ensino, matemáticos no caso, não devendo ser confundida com um conjunto de atividades se essas não tiverem conectadas e visando um avanço escalonado do objeto de estudo, acrescendo a complexidade da aplicação do objeto ao longo da sequência. A aplicação deve se atentar ao público ao qual é destinada, levando em conta as peculiaridades da trajetória da educação dos estudantes, também as especificidades do objeto de ensino.

Como coadunam Peretti & Costa ao discorrerem sobre o planejamento de uma Sequência Didática:

> (...)planejadas para ensinar um conteúdo, etapa por etapa, organizadas de acordo com os objetivos que o professor quer alcançar para aprendizagem de seus alunos e envolvendo atividades de avaliação que pode levar dias, semanas ou durante o ano. É uma maneira de encaixar os conteúdos a um tema e por sua vez a outro tornando o conhecimento lógico ao trabalho pedagógico desenvolvido. (Peretti; Costa, 2013, p. 06)

Na sequência didática, o processo inicial é o levantamento prévio de conhecimentos dos estudantes sobre o objeto didático, também chamado de sondagem. As atividades de uma sequência têm 3 caráteres principais, podendo ser: conceituais, procedimentais e/ou atitudinais.

Ao se referir a conteúdos conceituais, esses de seu caráter abstrato, o autor sobre uma perspectivo construtivista explana a importância de se analisar conhecimentos prévios, para que que o princípio abordado na aula não seja tão distante do que o aluno sabe a ponto de dificultar o aprendizado. Assim a significância do objeto, seus fundamentos serão assegurados através de uma atividade mental estimulada de modo adequado pela sequência didática.

Para os conteúdos procedimentais, estes se referem ao desenvolver no sujeito as capacidades de aplicação dos conceitos, para tanto deve ser desenvolvido neles o valor de significância ao objeto ensinado, sendo ensinada sua utilidade e finalidade, sendo preferível fugir de repetições exaustivas de um mesmo tipo de exercício, assim a Sequência Didática, onde busca o desenvolvimento desses conteúdos deve ser guiadas por modelos, onde a utilidade e finalidade do objeto possa ser destrinchada. (Zabala, 2014)

Dentro do chamado modelo “tradicional” de ensino, poderia uma sequência didática ser dividida em quatro fases: exposição da lição; estudo individual (podendo-se usar o livro didático ou outro material de apoio); fixação do conteúdo (através da repetição) e Avaliação do Aprendizado (Zabala, 2014). Todavia, o autor aponta que o modelo com essas fases é apenas

um ponto de partida, pois a necessidade do ensino acrescenta novas fases em outras abordagens, ou mesmo na abordagem tradicional.

Os conteúdos atitudinais trazem com eles uma complexidade de planejamento, por focarem numa formação de atitudes com relações afetivas, o que é algo de certa forma particular do sujeito, portanto subjetivo. Os valores, normas e atitudes com relação ao objeto que se pretendem ensinar podem ser feitos de modo conceitual, todavia é necessário um esforço que una a intenção com a ação, para que de fato haja a aplicação atitudinal. Sobre esse conteúdo Zabala acrescenta:

> Agora, para que este conhecimento se transforme em referência de atuação é preciso mobilizar todos os recursos relacionados com o componente afetivo. O papel e o sentido que pode ter o valor solidariedade, ou o respeito às minorias, não se aprende apenas com o conhecimento do que cada uma destas ideias representa. As atividades de ensino necessárias têm que abarcar, junto com os campos cognitivos, os afetivos e condutuais, dado que os pensamentos, os sentimentos e o comportamento de uma pessoa não dependem só do socialmente estabelecido, como, sobretudo, das relações pessoais que cada um estabelece com o objeto da atitude ou do valor. (Zabala, 2014, p. 109)

Dessa forma, os afetos e relações com que o estudante relaciona a si com o Objeto de aprendizado, pra isso vários fatores são preponderantes como a relação estudante/professor, relação aluno/aluno, o ambiente criado, as preconcepções sobre o Objeto (por exemplo: criptografia é coisa de hacker), as impressões do estudante sobre cada atividade dentro da sequência que podem incentivá-lo ou não na continuidade de seu envolvimento, entre outros, o sentido visto em relação as atitudes sugeridas. Dessa forma o trabalho com Conteúdos Atitudinais, pode não ser tão frequente quanto os outros pelo maior esforço necessitado e pelo carácter subjetivo necessita fomentar protagonismo nos discentes.

A maior ressalva que se pode fazer ao modelo tradicional, analisando o trabalho de Zabala, é que suas unidades não trazem o desenvolvimento de procedimentos Atitudinais, quando muito envolvem os procedimentais, mas, estão fixadas nos conceituais, o que não é bom ou ruim, apenas uma limitação. (Zabala, 2014). O autor não traz nomenclatura para os modelos de Sequência, contudo existem aquelas com um Problema como tema central visando construção de soluções, para concluir com a generalização do Objeto, outras com caráter mais Investigativo, exploratório ou de Pesquisa, em geral o aspecto de Pesquisa, Discussões em Grupo, Criação de Modelo surgem nas outras Sequências “Não-Tradicionais” elencadas pelo autor, o protagonismo estudantil segue como foco dessas.

3.2 Uso das Tecnologias Digitais na Educação

A tecnologia tornou-se após a promulgação da BNCC e reformulação das disciplinas, especialmente da Matemática, que tornou-se a área do conhecimento Matemática e suas Tecnologias, enfatizando a importância das tecnologias no ensino. No contexto tecnológico ao qual os estudantes estão inseridos é importante que essas ferramentas sejam utilizadas no ensino, especialmente no contexto desse trabalho, pois a Criptografia está profundamente ligada ao atual mundo digital.

Para que a palavra tecnologia não fique restrita a dispositivos eletrônicos, se usa o termo Tecnologias Digitais, pois a palavra tecnologia em si se refere a toda ferramenta construída para facilitar um propósito. Seguindo esta linha, as tecnologias estão presentes desde o início da humanidade, para cada época eram considerados inovadores o conjuntos de itens tecnológicos que melhor facilitaram um determinado aspecto da vida humana, então é natural que no atual contexto do século XXI ao se referir a Tecnologia, venha primeiramente a mente Computadores, Smartphones, Tv's Smart, e congêneres. (Almeida, 2015)

O conceito de tecnologia é de grande abrangência, pois como afirma Almeida citando Kenski: "o conjunto de conhecimentos e princípios científicos que se aplicam ao planejamento, à construção e à utilização de um equipamento em um determinado tipo de atividade" (ALMEIDA, 2015, Pg. 226 apud KENSKI, 2013). Portanto as tecnologias permeiam não só as atividades aplicadas em sala de aula, como o processo de preparação do professor, bem como a avaliação posterior da atividade.

As Tecnologias Digitais da Educação são então esse esforço de subsidiar o aprendizado por meio das mais diversas tecnologias presentes na humanidade, da calculadora, até os softwares com diversos fins, conectados ou não a internet. Sobre as potencialidades de seu uso Almeida corrobora: "podem também contribuir na estimulação do raciocínio lógico e, consequentemente, da autonomia, à medida que os alunos podem levantar hipóteses, fazer inferências e tirar conclusões, a partir dos resultados apresentados" (Almeida, 2015, Pg. 234, conforme Bona, 2009)

A *intencionalidade didática* dentro do uso das tecnologias digitais da educação é o fator que dará a maior ou menor eficiência de suas aplicações, de modo que o planejamento do uso adequado da tecnologia, desde a capacitação do professor, instrução do uso correto para os

alunos, quanto a clareza dos objetivos da atividade são fatores importantes para uma atividade que gere sentido ao estudante.

3.3 Metodologias Matemáticas

Dentre as metodologias de ensino com enfoque específico em matemática, foram abordadas na aplicação da sequência didática: Resolução de Problemas, investigação e modelagem matemática.

3.3.1 Resolução de Problemas

Sob esse aspecto, uma tendência metodológica matemática que potencializa as discussões, auxiliando no processo investigativo, quando aplicada corretamente é a Resolução de Problemas, já que para além da pergunta central, outras perguntas podem sugestionar o estudante à pesquisa e ao enfrentamento de suas dúvidas, ao questionar: os aspectos históricos da Criptografia, seu papel na história da sociedade, especialmente nos períodos Medievos e das Guerras Mundiais, os enfrentamentos entre Criptógrafos e Criptoanalistas, a formação da Criptografia que é usada em seus aparelhos telefones (Criptografia RSA). Sobre essa abordagem metodológica afirmam Silveira e Miola:

> A resolução de problemas como ação didática, como provocadora do movimento de aquisição de saberes, requer a seleção de problemas que realmente exijam dos alunos alguma habilidade na busca de estratégias de resolução. As operações matemáticas ocorrerão por necessidade da busca pela solução apropriada. (Silveira; Miola, 2013, p. 50-51)

Em vista de chegar ao objeto de conhecimento pretendido, além da clara definição do problema central, os passos do processo devem ser deixados claros ao estudante, que são: Compreender o problema, buscando as informações necessárias sobre a pergunta chave, aumentando o escopo do estudante; estabelecer um plano, selecionando entre os conhecimentos adquiridos em pesquisa, quais serão usados, quais serão os prioritários e em qual ordem; executar o plano estabelecido; verificar o resultado pretendido, validando-o ou não.

Todo este processo não pode surgir apenas como um modelo pré-concebido pelo professor, de modo que seu objetivo seja que os estudantes cheguem exatamente na proposta que pré-concebeu correndo o risco de perder toda a dinamicidade proposta pela Resolução de Problemas. Como afirma Lamonato & Passos citando D'Ambrósio:

> Dificilmente o aluno de Matemática testemunha a ação do verdadeiro matemático no processo de identificação e solução de problemas. O professor faz questão de preparar todos os problemas a serem apresentados com antecedência; consequentemente, o legítimo ato de pensar matematicamente é escondido do aluno, e o único a conhecer a dinâmica desse processo continua sendo o professor. O professor, com isso, guarda para si a emoção da descoberta de uma solução fascinante, da descoberta de um caminho produtivo, das frustrações inerentes ao problema considerado e de como um matemático toma decisões que facilitam a solução do problema proposto. (Lamonato; Passos, 2011, p. 53 apud D'Ambrósio, 1993)

Seguindo esta forma equivocada apontada pelas autoras supracitadas, o aluno pode ter uma equivocada visão de que resolveu o problema, quando de fato foi apenas conduzido, portanto em uma outra situação-problema que envolva o mesmo conteúdo matemático trabalho poderá se ver perdido sem o auxílio do professor, não produzindo então a aprendizagem efetiva.

3.3.2 Investigação Matemática

Com intuito de desenvolver no estudante a atitude de pesquisador, a investigação matemática convida o estudante a observar problemas e teoriza-los, "redescobrindo" o pensamento científico que compõe a solução dos problemas

Lamonato & Passos (2011), conceitual a Investigação Matemática como:

> (...) entendida como um meio pelo qual pode ocorrer a aprendizagem da Matemática em um processo que busca possibilitar ao estudante momentos de produção/criação de seus conhecimentos matemáticos, respeitando o nível de desenvolvimento em que ele se encontra. Investigar é procurar o que ainda não se conhece; investigar é questionar e procurar responder. Para investigar, é necessário querer saber; para investigar, é preciso estar curioso. (Lamonato; Passos, 2011, p. 62)

Proposta através de problemas com questões mais abertas (comparando com o Método de Resolução de Problemas), onde observações, testes, erros, reformulações fazem parte do processo de aprendizagem. O estudante não deve ser coagido a se preocupar excessivamente com o não conseguir atingir os resultados imediatamente, mas, incentivado a analisar a trajetória percorrida e ressignificá-la por meio de alterações, em vista de sair convencido e convencer os colegas, ao fim do estudo, que as conclusões/produtos finais estejam corretas. Sobre aplicação Investigação Matemática, Lamonato & Passos trazem:

> (...) possibilita ao aluno pensar a partir de uma dinâmica que prevê observações, descobertas, erros, acertos e, fundamentalmente, decisões. Essa, em síntese, é a essência da exploração-investigação matemática que entendemos para a Educação Básica (...), uma vez que, por tratar-se de questões ou situações abertas, cabe, a quem está interessado em investigar, a tomada de decisões sobre o percurso a seguir. (Lamonato; Passos, 2011, p. 53)

A perspectiva das autoras aponta para a construção de um conhecimento matemático ligado a superação das dúvidas e incertezas como promotoras do aprendizado alcançado pelo

esforço intencional de questionamentos e busca de propostas de resoluções. O docente envolvido no processo deve auxiliar os estudantes respondendo seus questionamentos as tarefas propostas, incentivando-os e instigando-os, contudo evitando conduzi-los a uma resposta, mas, visando ajuda-los a formular melhor suas perguntas.

Este método de estudo apresenta uma matemática investigativa, aberta a contribuições, não uma ciência fechada onde nada mais pode ser descoberto, o ensino deixa de ser por Transmissão e Memorização, passando a um maior protagonismo do estudante com atitude pesquisadora.

3.3.3 Modelagem Matemática

Muito semelhante a abordagem de Resolução de Problemas, é a Modelagem Matemática, pois a primeira pode ser mesclada na aplicação da segunda. A Modelagem é uma abordagem que busca realizar a simbiose entre a matemática cotidiana (ou da matemática aplicada a situações reais) com a matemática escolar, gerando modelos matemáticos aplicáveis a situações específicas buscando construir uma aprendizagem significativa ao aluno, como afirma Silveira & Miola sobre o fator de aprendizagem:

> "Ao lidar com situações comuns ao seu dia a dia, espera-se que o aluno faça algumas ligações entre a Matemática dos programas escolares e a matemática que existe imersa no seu mundo. Uma vez que essa relação é feita, é provável que o aluno não se esqueça tão facilmente do conteúdo que foi desenvolvido, uma vez que esse conteúdo passou a ter significado para ele." (Silveira; Miola, 2013, p. 50-51)

Os passos metodológicos da modelagem matemática são bem semelhantes aos da resolução de problemas, contudo para a primeira é necessário gerar um modelo, um produto final, deverá haver uma construção concreta: como gráficos, fórmulas, diagramas, tabelas, etc, que tornem a aplicação do conhecimento matemático mais simples. um exemplo concreto de seu uso que será aplicado no trabalho é uma forma rápida de gerar senhas, para uma pessoa que por questões de segurança precisa semanalmente mudar as senhas de suas contas e aplicativos (este exemplo será abordado no capítulo de aplicações).

4. REVISÃO LITERÁRIA

Neste capítulo são expostos os principais levantamentos feitos sobre o a segurança digital e criptografia, que fundamentam o contexto ao qual as teorias matemáticas serão aplicadas.

4.1 Evolução Histórica da Criptografia

Ao abordar um tema relativamente pouco abordado na educação básica, especificamente no ensino médio, é importante para contextualização histórica da ciência, assim o estudante poderá ver a criptografia como uma construção científica-histórica, que influenciou momentos emblemáticos da história da humanidade e sempre esteve em constante evolução.

4.1.1 A Cifra de César

O Império Romano é considerado a maior e mais longeva potência militar da antiguidade. Espalhando-se por grande parte da Europa, além de conquistar a parte ocidental do Oriente Médio e parte do norte da África. A este império atribuímos um dos pioneiros e mais simples códigos, a Cifra de Substituição Monoalfabética denominada Cifra de César, em referência ao cônsul, militar e político romano, Caio Júlio César (nascido em 100 a.c), sua cifra foi uma das primeiras de que se tem registro a ser empregada com intencionalidade militar, pois na época as comunicações eram feitas através de mensageiros a pé ou a cavalo, e o risco de interceptação desses mensageiros e apreensão das mensagens por um exército inimigo era alto, a cifra poderia não proteger o mensageiro, mas, certamente impediria o adversário de saber dos planos romanos. Sobre essa a cifra de substituição Coutinho afirma:

> "O mais simples dos códigos consiste em substituir uma letra pela seguinte; isto é transladar o alfabeto uma casa para diante. Um código semelhante foi usado por César para comunicar-se com as legiões em combate pela Europa. Este parece ter sido o primeiro exemplo de um código secreto de que se tem notícia" (COUTINHO, 2014, p. 1)

Singh detalha o uso feito por César: "Ele simplesmente substituía cada letra na mensagem por outra que estivesse três casas à frente no alfabeto. Os criptógrafos geralmente pensam em termos do *alfabeto original*, usado para escrever a mensagem, e o *alfabeto cifrado*,

formado pelas letras usadas na substituição.” (Singh, 2022. Pg.. 26, grifos do autor). Para fins demonstrativos, usando o alfabeto atual, tomemos como exemplo a palavra “Tucano”, utilizando a cifra de César, teremos a palavra: “WXFDQR”

Portanto cada letra foi substituída pela letra três casas a frente: T → W; U → X; C → F; A → D; N → Q; O → R. O funcionamento da Cifra de César é semelhante ao de uma Função Afim no formado: $f(x) = x + 3$. Posteriormente abordaremos essa funcionalidade. Ainda que o autor do século II, Suetônio, no livro *As vidas dos Césares* só especifique esse única forma de uso da Cifra de César, ela pode ser aplicada para qualquer deslocamento de letras, substituindo-se o 3 de césar por qualquer número entre 1 e 25. (Singh, 2022). Utilizando os termos abordados anteriormente, o algoritmo da cifra é o deslocamento de letras para frente, e a chave utilizada por César é 3 letras para frente.

Fraquezas da Cifra de César

Enquanto permaneceu sem sigilo a Cifra de César constituiu em uma boa vantagem bélica, contudo não é constituído por um algoritmo forte, pois só existe 26 chaves possíveis. Em palavras soltas apresenta um certo grau de dificuldade para decodificação da mensagem. Contudo, para textos maiores a cifra é facilmente quebrada através da Criptoanálise por meio de um Ataque de Frequência, como detalha Coutinho:

> “Códigos como o de César padecem de um grande mal, são muito fáceis de decifrar. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto se deve ao fato de que a frequência média com que cada letra é usada em uma língua é mais ou menos constante.” (Coutinho 2014, p. 01)

Tomando a Língua portuguesa como exemplo, temos uma predominância maior das vogais A (13,52%), E (12,25%), O (10,36%) e as consoantes S (7,92%) e R (6,74%), as porcentagens foram aproximadas (Quaresma, 2006). Portanto na análise de frequência de um texto em português haverá uma predominância da letra que substitui o A, no caso, a letra D, seguida pelas letras H, R, V e U correspondentes a E, O, S e R.

Outro aspecto deste tipo de análise, é a observação de palavras com uma, duas ou três letras, que têm uma previsibilidade maior, as vogais (não acentuadas) A, E e O representam aproximadamente 87,79% das palavras com uma única letra, sendo A mais frequente entre elas, portanto por onde começaria as tentativas de quebra do código. De modo análogo, palavras com duas letras tem a primazia do monossilábico DE (22,28%), SE (9,35%), DO (7,44%) e DA

(7,02%), portanto se começaria o processo de análise por correspondentes ao DE. Com três letras a predominância é de QUE (20,23%), NÃO (7,76%) e COM (6,80%), onde no texto cifrado, deveria se observar a palavra de 3 letras mais frequentes e analisar sua correspondência com ‘que’. (QUARESMA, 2006)

Abordando um estudo sobre o idioma inglês num texto onde as letras mais frequentes foram O, X, e P, Singh apresenta outro aspecto sobre a análise de frequência de um texto, se referendo a justaposição das letras:

> “(...) devemos contar com que frequência elas aparecem do lado de outras letras. Por exemplo, será que a letra **O** aparece antes ou depois de várias letras ou teria ela a tendência a ficar ao lado de algumas letras em especial? A resposta a esta pergunta nos dará uma boa indicação de se **O** representa uma vogal ou uma consoante” (SINGH, 2022, p. 38)

O que o autor supracitado aborda é válido para análise de qualquer outro idioma, de posse do conhecimento da análise de frequência dele, bem como com um bom conhecimento de suas estruturas linguísticas, é possível avançar em termos criptográficos na Análise de Frequência.

Dependendo do tipo do texto, algumas variações podem surgir, como quando são usadas muitas palavras de outros idiomas, ou aspectos técnicos de uma determinada área, o que gera um vício num texto para outras letras que podem diferir da Análise de Frequência padrão da Língua. Ainda assim essa Análise Padrão oferece um chão sólido para um ataque da criptoanálise, identificando as letras/palavras com maior frequência no texto cifrado é possível ir estabelecendo correspondências das outras letras.

4.1.2 O Quadrado de Blaise de Vigenère

A criptografia perpassa os períodos da antiguidade, chegando a Idade Média europeia onde a multiplicidade de reinos, crises diplomáticas e ocasionais ameaças de invasões vindas do Oriente Médio demandaram novas formas de criptografia. Dentre elas a *cifra polialfabética*, onde mais de um alfabeto seria usado para fazer o algoritmo, de modo que a análise de frequência ficaria desabilitada nos moldes usados em cifras monoalfabética. Leon Battista Alberti, um polímata florentino, nascido em 1404, começa a pesquisar esta nova forma de criptografia, conforme relata Singh:

> “Naquela época todas as cifras de substituição exigiam um único alfabeto cifrado para codificar cada mensagem. Alberti propôs o uso de dois ou mais alfabetos cifrados,

> usados alternadamente, de modo a confundir os criptoanalistas em potencial" (Singh, 2022, p. 64)

Os estudos de Alberti não o levaram a um algoritmo aplicável, sendo seguido pelos estudos de Johannes Trithemius e Giovanni Porta que desenvolveram a tese de Alberti. Contudo quem conseguiu aplica-la foi o diplomata Blaise de Vigenère, nascido em 1523, que ao conhecer os trabalhos dos três autores supracitados, motivado pela natureza de seu trabalho criou o que se tornou conhecido como O Quadrado de Vigenère, representado no quadro abaixo:

Quadro 1 - Quadrado de Vigenère

0	a	b	c	d	e	f	g	H	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	Y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Adaptado de Singh, 2022.

Esta cifra utiliza 26 alfabetos cifrados simultaneamente, pode ser visto como 26 cifras de César, onde cada número de linha representa a quantidade de casas para frente que o alfabeto foi deslocado, neste algoritmo cada letra do alfabeto original é cifrada com uma letra de uma das linhas do Quadrado de Vigenère. Para o exemplo vamos cifrar a frase de J.R.R. Tolkien: "Ações não valerão menos porque não foram elogiadas". O uso da cifra de Vigenère procede do seguinte modo: Se escolhe uma palavra-chave, para este exemplo será usada a palavra BLAISE, em maiúsculo. Em seguida a palavra-chave será repetida acima da mensagem, de modo que cada letra, em minúsculo da mensagem seja relacionada a uma letra da palavra-chave, como mostra a tabela abaixo:

Quadro 2 - Uso da Cifra de Vigenere

B	L	A	I	S	E	B	L	A	I	S	E	B	L	A	I	S	E	B	L	A	
a	c	o	e	s	n	a	O	v	a	l	e	r	a	o	m	e	n	o	s	P	
I	S	E	B	L	A	I	S	E	B	L	A	I	S	E	B	L	A	I	S	E	B
o	r	q	u	e	N	a	O	f	o	r	a	m	e	l	O	g	i	a	d	A	S

Fonte: Elaborada pelo autor

A primeira correspondência será a letra A, que está ligada a letra B da Palavra-Chave, portanto olharemos a linha no Quadrado de Vigenère que começa por B, linha 1, onde encontraremos o substituto para A, que será a letra que pertence a Coluna A e linha 1, neste caso o próprio B. Em seguida vamos cifrar o C, que será o encontro da coluna C com a linha 11, sendo cifrado como N. Prosseguindo dessa forma a primeira palavra do texto cifrado terá a forma ‘bnomh’, representada no quadro abaixo:

Contudo, se pensarmos matematicamente, sabemos que cada uma das letras da palavra-chave, representará, em suma, um deslocamento isolado da cifra de César, então é possível fazer esse processo de modo matemático. Atribuindo números as letras do alfabeto de 0 a 25 (. Portanto a chave BLAISE serão os números 1-11-0-8-18-4, aqui os elementos da linha 26 são iguais aos da linha 0, recomeçando o ciclo. Para cada letra *a* ser cifrada, somaremos seu número correspondente com o número da letra correspondente a chave, aplicando o algoritmo da *divisão de euclides,* tendo 26 como divisor, o resto será o número correspondente a cifra. Por exemplo para cifrar a letra L em “valerão”, que tem como correspondente na palavra chave a letra S teremos: $11 + 18 = 29 = 26 \,.\, 1 + 3$. O resto 3 é equivalente a D. Portanto L nessa palavra será cifrado como D. Abaixo está a tabela com a cifragem das três primeiras palavras, ignorando acentuações e espaços:

Tabela 1 - Conversão da Cifra de César em formato Numérico

Palavra-Chave	B	L	A	I	S	E	B	L	A	I	S	E	B	L	A
N°	1	11	0	8	18	4	1	11	0	8	18	4	1	11	0
Texto Original	a	c	o	e	s	n	a	o	v	a	l	e	R	a	o
N°	0	2	14	4	18	13	0	14	21	0	11	4	17	0	14
RESTO	1	13	14	12	10	17	1	25	21	8	3	8	18	11	14
CIFRA	**B**	**N**	**O**	**M**	**K**	**R**	**B**	**Z**	**V**	**I**	**D**	**I**	**S**	**L**	**O**

Fonte: Elaborado pelo autor

O processo de cifragem acima demonstrado, também poderia ser feito com uma função da aritmética modular, tema que será abordado mais a frente neste texto. O interessante deste processo de cifragem é que a Análise de Frequência não funcionária com ele. Se observarmos a frase: AÇÕES NÃO VALERÃO MENOS PORQUE NÃO FORAM ELOGIADAS e também sua versão cifrada BNOMK RBZ VIDISLO VWRPD PWJUVP NIG KPCAU WPP RIIVET,

a conversão pela análise de frequência fica impossível já que letras diferentes foram cifradas igualmente diversas vezes. Como mostrado na tabela abaixo:

AÇÕES NÃO VALERÃO MENOS PORQUE NÃO FORAM ELOGIADAS

BNOMK RBZ VIDISLO VWRPD PWJUVP NIG KPCAU WPPRIIVET

Tabela 2 - Comparação da Análise de Frequência de texto criptografado

Texto Original			Texto Criptografado		
Letra	Ocorrência	Frequência	Letra	Ocorrência	Frequência
A	8	19%	A	1	2%
B	0	0%	B	2	5%
C	1	2%	C	1	2%
D	1	2%	D	2	5%
E	5	12%	E	1	2%
F	1	2%	F	0	0%
G	1	2%	G	1	2%
H	0	0%	H	0	0%
I	1	2%	I	5	12%
J	0	0%	J	1	2%
K	0	0%	K	2	5%
L	2	5%	L	1	2%
M	2	5%	M	1	2%
N	3	7%	N	2	5%
O	8	19%	O	2	5%
P	1	2%	P	6	14%
Q	1	2%	Q	0	0%
R	3	7%	R	3	7%
S	3	7%	S	1	2%
T	0	0%	T	1	2%
U	1	2%	U	2	5%
V	1	2%	V	4	9%
X	0	0%	X	0	7%
Y	0	0%	Y	0	0%
W	0	0%	W	3	0%
Z	0	0%	Z	1	2%

Fonte: Elaborado pelo autor

Através desse algoritmo, a frequência não se repete. Se na mensagem original temos 9 letras que não aparecem, na mensagem cifrada este número é de apenas 5 letras, além de as letras mais frequentes são, cada uma por vez, cifra de diferentes letras.

> “Além de ser invulnerável à análise de frequência, a cifra de Vigenère tem um número enorme de chaves. O remetente e o destinatário podem escolher qualquer palavra no dicionário, ou qualquer combinação de palavras, ou até mesmo criar palavras novas. Um criptoanalista não conseguiria decifrar a mensagem procurando todas as chaves possíveis, porque o número de opções é simplesmente grande demais” (Singh, 2022, p. 68.)

Com Blaise Vigenère se tem a evolução da cifra monoalfabética para a cifra Polialfabética, esta imune a análise de frequência. Porém seu uso exigia maior tempo e esforço, o que para alguns usos da criptografia não a tornavam primeira opção pois em situações bélicas

ou diplomáticas, a velocidade da encriptação e desencriptação garantia a utilidade da informação, ainda que com o sigilo conservado pela criptografia. (Singh, 2022)

Mesmo com todo o poder criptográfico, que beneficiaria muito a comunicação diplomática dos países europeus, a Cifra de Vigenère ficou esquecida pelos dois séculos que se seguiam, quando a Criptoanálise deixa de ser um esforço de pequenos entusiastas individuais e passa a ser industrializada, com esforços coletivos nas chamadas Câmaras Negras, que eram unidades de criptografias governamentais de países europeus, responsáveis pela interceptação, cópia e reenvio de correspondências, como aponta Singh:

> As Câmaras Negras Efetivamente tornaram todas as formas de cifras monoalfabética inseguras. Enfrentando uma oposição tão profissional dos criptoanalistas, os criptógrafos foram afinal forçados a adotas a cifra de Vigenère, mais complexa, porém mais segura. E gradualmente os secretários de cifras passaram a usar as cifras polialfabéticas. Além de uma criptoanálise mais eficiente, havia outra pressão encorajando a mudança para as formas mais seguras de cifragem: o desenvolvimento do telégrafo e a necessidade de proteger os telegramas de serem interceptados e decifrados. (SINGH 2022, p. 78)

Com o surgimento do Telégrafo no século XIX, as comunicações começam a ser feitas através do código Morse, ainda que tenha essa nomenclatura, ele não era um código criptografado, portanto a Cifra de Vigenère auxilia que as comunicações em Morse fossem criptografadas, sua efetividade premiou esta cifra com a alcunha francesa *le chiffre indéchiffrable* (traduzido como O Dígito Indecifrável)

A Quebra da Cifra de Vigenère foi feita pelo britânico Charlles Babagge, com uma forma inédita à época de análise de frequência bem mais elaborada do que as usadas anteriormente, ele observa que num texto mais longo, palavras frequentes em determinado idioma seriam cifradas de diferentes modos. Portanto seu ataque criptográfico consistia em: Observar sequências de letras que se repetiam. Sobre isso Singh aponta:

> “Existem dois meios pelos quais tais repetições poderiam surgir. O mais provável é que a mesma sequência de letras no texto original tenham sido cifradas usando-se a mesma parte da chave. Como alternativa, existe uma ligeira possibilidade de duas sequências diferentes de letras no texto original tenham sido cifradas usando-se partes diferentes da chave, o que coincidentemente, teria levado a uma sequência idêntica no texto cifrado” (SINGH, 2012, p. 87)

Dando primazia as sequências mais longas e observando o primeiro caso, eram analisados os espaçamentos entre cada repetição. Por exemplo, se duas sequências idênticas de letras distam-se de 30 caracteres, e sendo os divisores inteiros e positivos de 30: 1, 2, 3, 5, 6, 10, 15 e 30. Então existem 8 possibilidades: A chave tem 1 letra de comprimento e é repetida 30 vezes durante a cifragem; a chave tem 2 letras de comprimento e é repetida 15 vezes durante

a cifragem; a chave tem 3 letra de comprimento e é repetida 10 vezes durante a cifragem; assim por diante chegando a possibilidade da chave ter 30 letras e ser repetida uma única vez.

Se o primeiro caso fosse provado, a Cifra seria monoalfabética, o que na época de Babbage estava em desuso para comunicações sensíveis. Para confirmar a extensão da palavra-chave, buscavam-se outros padrões de repetição de sequências de letras diferentes. Como mostra Singh num estudo de um texto onde ouve repetições das sequências EFIQ, PSDLP, WCXYM e ETRL.

Tabela 3 - Análise de possíveis tamanhos de chaves codificadoras

Sequência repetida	Espaços Repetidos	Tamanhos possíveis de chave (ou fatores)										
		2	3	4	5	6	8	10	12	15	19	20
E-F-I-Q	95				✓						✓	
P-S-D-L-P	5				✓							
W-C-X-Y-M	20	✓		✓	✓			✓				
E-T-R-L	120	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

Fonte: Adaptada de SINGH, 2022. Pg 89

Pela análise da tabela os dados apontam para uma palavra chave de 5 letras. Pelo que foi mostrado na Cifra de Vigenère, uma chave de 5 letras define que 5 alfabetos foram utilizados na codificação do texto. Portanto a Análise de Frequência comum pode ser aplicada, observando as letras do texto no intervalo de 5 em 5, para compreender qual alfabeto foi usado para cada uma dessas sequências, por conseguinte descobre-se a palavra-chave, daí a desencriptação torna-se simples como se a mensagem tivesse sido destinada ao próprio criptoanalista.

Os feitos de Babbage não foram publicados, sendo descobertos para fins históricos apenas de modo póstumo, quando suas anotações foram analisadas por estudiosos, contudo, a quebra da Cifra de Vigenère foi descoberta de modo independente por Friedrich Wilhelm Kasiski, oficial militar prussiano da reserva, tal que a quebra da cifra é conhecida como Teste de Kasiski. (Singh, 2022)

4.1.3 Cifra de Substituição Homofônica

Uma alternativa eficaz para a Guerra entre Criptógrafos Profissionais contra Criptoanalistas tender para o lado dos Criptógrafos com um tipo de Cifra de maior agilidade, portanto mais útil que a Cifra de Vigenère, isso considerando a época, é a Cifra de Substituição Homofônica. Assim como o método de Vigenère, esta cifra também é eficaz contra a análise de frequência.

Seu uso consiste numa espécie de tecnologia reversa contra a análise de frequência, ao transformar uma letra, que por exemplo, tenha 5% de Frequência em uma cifra com 5 símbolos diferentes, desse modo quando num texto essa letra com 5% de frequência aparecer, será substituída por um dos cinco símbolos com os quais esta foi relacionada, isso de modo alternado de modo que cada um dos oito símbolos corresponda a um por certo do texto. (Singh, 2022)

Esses símbolos comumente eram números de dois dígitos. E uso deles tinha por objetivo equilibrar a frequência das letras mais populares oferecendo substituições alternadas para elas, de modo a quebrar a análise de frequência pois o texto carecerá de números de maior incidência, ainda que o texto contenha algumas outras pistas que podem ser objeto de análise. Um exemplo disso é a análise posicional dos números, pois considerando o idioma existem padrões de comportamento das vogais, letras que dificilmente aparecem depois e/ou antes de outras, ainda assim a Cifra Homofônica aumentou o nível de eficiência e segurança comparada ao uso de suas antecessoras.

Portanto nesses casos a análise será focada nas relações linguísticas entre as letras, todavia um criptógrafo pode alternar continuamente o alfabeto cifrado usado, tornando mais difícil o trabalho do criptoanalista.

> "Podemos pensar nos números de dois dígitos que correspondem à letra **a** como efetivamente representando o mesmo som no texto cifrato, ou seja, o som da letra **a**. Daí a origem do termo substituição homofônica, *homos* significado "mesmo" e *phone* significando "som" em grego." (Singh, 2022. Pg. 71)

As Câmaras Negras

O sucesso da Cifra Homofônica perdura até os anos 1700, época em que a função dos criptoanalistas foi expandida, industrializada, não mais feita por sujeitos isolados considerados "gênios" de seus tempos, ou por pares isolados de pessoas. Os governos europeus, em especial reuniam equipes que trabalhavam conjuntamente na criptoanálise, os locais onde essas equipes se reuniam eram denominados Câmaras Negras, onde até medos dos século XIX as informações eram interceptadas e traduzidas (Singh, 2022)

A criação dessas Câmaras que iam desde a interceptação de documentos, até sua cópia, desencriptação, e envio ao destinatário lacrado novamente tornou qualquer cifra monoalfabética inútil, obrigando o mundo da criptografia a voltar os olhos para as Cifras de Vigenère, polialfabéticas. O método de interceptação de mensagens mudaria de forma com a invenção do

telégrafo, inaugurado em 1844, que se difundiria gradualmente, até ser o principal meio de comunicação nas vésperas da primeira guerra mundial. (Singh, 2022)

4.1.4 Criptografia durante a Primeira Guerra Mundial

De modo ilustrativo em 1917, uma mensagem alemã interceptada pelos Ingleses e Americanos impõe uma vitória emblemática do confronto. Pois antes dela os Estados Unidos da América apresentavam neutralidade no confronto. Conforme aponta Singh: *"O presidente Woodrow Wilson passara os primeiros dois anos da guerra recusando-se a enviar tropas americanas para apoiar os soldados. (...) Wilson achava que podia servir melhor o ao mundo se permanecesse neutro e atuasse como mediador"* (Singh, 2022, p. 125). Essa intenção do então presidente Americano era reforçada pela nomeação de um novo ministro alemão de Relações Exteriores, Arthur Zimmermann, que foi aclamado pela mídia como um potencial pacificador do lado alemão do confronto, o que era o oposto da real intenção do novo Ministro.

Zimmermann pretendia lançar uma guerra naval irrestrita com seus submarinos, além de recrutar o México para a Guerra (Singh, 2022, p. 128-132). Essa comunicação, com o México foi feita por intermédio do embaixador alemão nos Estados Unidos, todavia como a Inglaterra havia sabotado os cabos transatlânticos da Alemanha, Zimmermann enviou um telegrama criptografado a o embaixador alemão em Washington, telegrama este que foi interceptado e encaminhado para a "Sala 40", unidade de cifras da Inglaterra, onde o código foi quebrado pelo Reverendo Montgomery e Nigel de Grey.

Houve ainda um engenhoso artifício do Sir. William Hall, almirante inglês, para que nem Alemães nem Americanos soubessem que a mensagem foi desencriptada na Inglaterra. De uma parte para que a Quebra da Cifra permanecesse em Sigilo, de modo que a Cifra Alemã continuasse sendo usada, a segunda motivação é que os Americanos não achassem que a revelação da mensagem fosse uma armação dos ingleses para que abandonassem a neutralidade na guerra.

Deste modo, com o uso da espionagem britânica e com alguns cortes, a mensagem desencriptada chegou para o presidente Americano, com a informação de que havia sido interceptado na forma de telegrama enviado do embaixador alemão em Washington para o embaixador alemão no México, o que de fato aconteceu, porém muito depois do conteúdo da

mensagem encriptada já ser conhecido antes de se tornar “O telegrama Zimmermann”, como viria a ser notavelmente conhecido (Singh, 2022)

Singh citando a historiadora americana Bárbara Tuchman:

> “Se o telegrama não tivesse sido interceptado nem publicado, inevitavelmente os alemães teriam feito alguma outra coisa que nos levaria para a guerra. Mas o tempo já estava se esgotando, e se tivéssemos nos atrasado um pouco mais os aliados teriam sido obrigados a negociar. Nesse ponto o telegrama Zimmerman mudou o curso da história(...) Em si mesmo era apenas um cascalho da longa estrada que matou a ilusão americana de que podíamos continuar nossas vidas separados dos outros países. Para os negócios do mundo era apenas uma pequena trama do ministro alemão. Mas para as vidas do povo americano significava o fim da inocência” (Singh, 2022, p. 133-134, apud Tuchman, 1994)

A autenticidade do telegrama sofreu um período de dúvida curto, pois após sua veiculação na mídia o próprio Zimmermann confirmou a autoria alemã do documento. Portanto uma única desencriptação, unida a inteligência militar propiciou a entrada de mais um país na primeira Guerra mundial, o que 3 anos de diplomacia entre os aliados da Inglaterra com os Estados Unidos não havia feito, isso livrou os americanos de outros ataques, impediu a entrada do México no conflito e contribuiu decisivamente para definir o lado vencedor do conflito. (Singh, 2022)

4.1.5 Criptografia na Era da Computação

Ao fim da Primeira Guerra Mundial, a Cifra de Vigenère é reinventada, com os codificadores buscando mitigar os riscos de sua maior fraqueza: A Palavra-Chave, que poderia também ser um conjunto de palavras ou uma frase. Por conta da natureza cíclica da cifra era possível identificar o comprimento da palavra-chave, com isso se dividia os textos em blocos e se buscava por padrões de palavras mais comuns no idioma do texto original.

Este ataque cripto-analítico era de dificuldade moderada quando a palavra-chave era curta, se fosse longa aumentava-se muito o processo, começou-se a usar chaves tão longas quanto a própria mensagem. Isso porém ainda permitia uma desencriptação ainda que mais lenta, pois as palavras-chave eram reconhecíveis e dedutíveis.

Em 1918, porém, passou-se usar chaves desprovidas de estrutura, com letras embaralhadas sem sentido gramatical relevante ao idioma, de modo que a palavra-chave não era mais dedutível (Singh pg. 138). O resultado disso foi algo indecifrável, este método de

produção de chaves foi conduzido por Joseph Mauborgne, militar Americano que foi chefe da divisão de Engenharia e Pesquisa do Signal Corps após a Primeira Guerra Mundial.

Posteriormente foram desenvolvidos blocos feitos com calhamaços de folhas com várias chaves encriptadas cada, que eram feitos sempre em duas cópias, ficando uma com quem enviava a mensagem e outra com quem a decodificaria. O que garantia segredo absoluto da mensagem contra qualquer interceptador, seja da mensagem física, via rádio, telégrafo entre outros. A cada comunicação feita, emissor e receptor descartavam a folha de códigos utilizada.

Embora extremamente segura esse método trazia algumas dificuldades bem sensíveis e não foi amplamente usado. Pois: 1) A produção de chaves aleatórias, num contexto ainda de datilografia, era trabalhosa e custosa, 2) Ocorriam vícios do datilógrafo que faziam que os dígitos se alternassem com uma frequência previsível entre os datilografados pela mão direita e os datilografados pela mão esquerda, o que acabava gerando padrões ocasionalmente, falhando nos termos de segredo absoluto ao qual o método propunha. 3) Os blocos não poderiam ser reutilizados, pois resultaria num erro criptográfico. Todavia esse método de cifragem foi o propulsor do Desenvolvimento das Máquinas de Cifragem, sendo o último marco da Criptografia “Papel e Lápis”.

4.1.6 As Primeiras Máquinas de Criptografia

No sentido mais básico da palavra máquina, diríamos que a primeira máquina de Cifragem foi o Disco de Cifras, criado pelo arquiteto italiano Leon Albert, este relacionado a criação da cifra polialfabéticas.

> “Ele pegou dois discos de cobre, um ligeiramente maior do que o outro, e gravou um alfabeto ao longo da borda de cada disco. Colocando o disco menor em cima do maior e fixando-os com um pino para agir como eixo, ele construiu algo semelhante ao disco de cifras [...]. Os dois discos podem ser girados independentemente, de modo que os dois alfabetos possam mudar suas posições relativas” (Singh, 2022, p. 143)

Com este engenho relativamente simples, ele automatizava a cifra de César, pois o uso feito no império romano dependia de tubos pré-moldados, Albert moderniza o uso da cifra, o que seria um subsídio para os inventos posteriores. O Disco de Cifras foi reinventado no século XX, em 1918, por Arthur Scherbius e Richard Ritter, fundadores da Sherbius & Ritter, uma empresa que desenvolvia engenharia inovadora diversas. Entre um de seus empreendimentos existe a Máquina Enigma, uma versão elétrica do disco de Alberti.

> "A forma básica da invenção de Scherbius consiste em três elementos conectados por fios: um teclado para a entrada de cada letra do texto original, uma unidade misturadora, que cifra cada letra, transformando-a na letra correspondente da mensagem cifrada, e um mostrador consistindo em várias lâmpadas para indicar as letras do texto cifrado" (Singh, 2022, p. 146)

O disco misturador era de borracha e cheios de fios que eram misturados na rotação, embaralhando as referências de letras, trocando as letras da mensagem originais, os fios entram no misturador por 26 pontos, gerando 26 trocas de letras, todavia um único disco gera uma fraqueza na máquina para misturas repetidas. Após estudo dos criptógrafos ao longo do uso da Enigma foram introduzindo outros discos misturadores, cada um fazendo sua rotação de mistura dos caracteres após a rotação do disco anterior aumentando assim o Espaço Amostral, de 26 possibilidades de troca para 26^n com n sendo o número total de discos misturadores. A máquina era considera mais eficiente por seus misturadores de movimento automático, e a velocidade que o sistema eletrizado dava ao processo.

A Enigma idealizada por Scherbius tinha três discos misturadores, portando $26^3 = 17576$ formas de ajustes da máquina, o que a tornava uma criptografia muito mais forte e eficiente que boa parte dos métodos demonstrados anteriormente. A Enigma de Scherbius funcionava do seguinte modo:

> "Um operador deseja enviar uma mensagem secreta. Antes da cifragem começar, ele deve primeiro girar os misturadores para uma determinada posição inicial. Existem 17.576 ajustes possíveis, e portanto 17.576 posições iniciais possíveis. A disposição inicial dos misturadores vai determinar como a mensagem será cifrada" (Singh, 2022, p. 152)

É notável que para que uma pessoa decifre a mensagem, ainda que ela disponha de uma Máquina Enigma de mesmo modelo, sem a posição inicial da mensagem será muito difícil decifrar a mensagem, e um "ataque de força bruta" será demorado devido ao grande número de ajustes possíveis.

Esses ajustes iniciais eram definidos num livro, com os ajustes iniciais dos misturadores para cada dia específico. Portanto apenas se alguém descobrisse o livro de ajuste iniciais, na época, seria possível desencriptar a mensagem, do contrário a mensagem em si poderia ser transmitida por qualquer meio, na época o rádio, sem grandes preocupações. Em resumo: A Mensagem Original é digitada na Enigma do emissor, é gerada uma Mensagem Criptografada e transmitida ao destinatário, este de posse de outra máquina Enigma sabendo das configurações de ajuste do dia, digita nesta a Mensagem Criptografada e no Mostrador aparecerá a Mensagem Original.

Um criptoanalista poderia gastar até duas semanas para determinar o conteúdo da mensagem, testando todas as combinações e verificando se a mensagem para cada uma delas é coerente, então a segurança da mensagem era considerada moderada. Porém se for destacada uma equipe maior de pessoas para o trabalho, esse tempo poderia ser reduzido substancialmente.

Diante de mais uma batalha entre Criptógrafos e Criptoanalistas, Scherbius introduziu duas novas características a Enigma: A primeira foi reprojeta-la de modo que os três discos misturadores pudessem ser trocados entre si, portanto gerando seis modos de se organizá-los; o segundo engenho foi introduzir cabos e tomadas entre teclados de cada letra e fios conectando-os ao primeiro misturador, acrescentou ali outra característica interessante que foi seis cabos com pinos que conectavam duas letras do teclado, permutando-as durante a digitação.(Singh, 2022)

As máquinas Enigma e semelhantes ficaram no ostracismo por um período longo, foram consideradas desnecessárias. Porém a Enigma de Scherbius encontraria mercado entre os Alemães após a ampla divulgação das derrotas destes no campo da criptografia durante a Primeira Guerra Mundial.

> "Os militares alemães organizaram uma investigação para determinar como seria possível evitar os fiascos criptográficos da Primeira Guerra Mundial e concluíram que a máquina Enigma oferecia a melhor solução possível. Em 1925, Scherbius começou a produção em massa de máquinas Enigma, que passaram a ser usadas pelos militares no ano seguinte. [...]Nas duas décadas seguintes os militares alemães compraram 30 mil máquinas Enigma. E a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo. Com ele, no início da Segunda Guerra Mundial as comunicações estavam protegidas por um nível sem igual de cifragem. Naquela época parecia que a máquina Enigma desempenharia um papel vital na vitória nazista, mas ela acabou ajudando na queda de Hitler." (Singh, 2022, p. 161)

É notável o papel que as novas tecnologias de criptografia marcaram o curso de eventos históricos tão emblemáticos na humanidade. A Enigma porém, não permaneceria inquebrável por muito tempo, embora tenha gerado tremendo desconforto as equipes de "Câmaras Negras" de diversos países, durante o interstício entre as duas guerras mundiais. A Enigma era comercializada em uma versão comercial de fácil acesso para o estudo, porém, a versão militar, exclusiva do exército alemão não era conhecida ainda.

As Unidades de Criptografia dos países vencedores da Primeira Guerra arrefeceram seu empenho por ocasião da aparente paz conquistada, todavia a Polônia se encontrava em uma posição menos confortável por fazer fronteira com a Alemanha, mantendo então os esforços de interceptação de desencriptação de mensagens. Graças a um ressentido ex-militar alemão,

Hans-Thilo Schimidt, documentos confidenciais sobre a Enigma Militar Alemã foram obtidos dele pelo governo francês.

> "Em 8 de novembro de 1931, Shmidt chegou ao Grande Hotel em Verviers, na Bélgica, para um encontro com um agente secreto francês, cujo codinome era Rex. Em troca de 10 mil marcos (o equivalente a 20 mil libras na cotação atual), ele permite que Rex fotografasse dois documentos: "Gebrauchsanweisung für die Chiffriermaschine Enigma" e "Schlüsselanleitung für die Chiffriermaschine Enigma". Esses documentos eram basicamente, instruções para o uso da fiação da máquina Enigma, e embora não apresentassem descrições explícitas da fiação dentro de cada misturador, continham informações necessárias para que a disposição dessa fiação fosse deduzida" (Singh, 2022, p. 166)

A falta de interesse do Governo Francês em estudar a máquina permitiu, que por um tratado de cooperação militar, os poloneses tivessem acesso aos documentos, que inclusive dava detalhes sobre o uso dos livros-código. O Biuro Szyfróm, unidade de criptografia polonesa, recrutou aquele que iria decifra à Enigma, o estudante de estatística Marian Rejewski que após um ano de árduas tentativas estabelece as correntes de ligações das letras da Enigma Alemã, com isso ele elabora um catálogo com essas ligações.

Sobre a configuração do Teclado usado, mais uma vez o método de segurança se torna a fraqueza abordada pelos criptoanalistas pois como os alemães repetiam a configuração da Enigma no início da mensagem, a chave de mensagem, o que consistia num padrão a ser explorado:

> A repetição mais óbvia na cifragem da Enigma, era a chave de mensagem, cifrada duas vezes no início de cada mensagem. Se o operador escolher **ULJ** como chave de mensagem, então ele terá que cifrá-la duas vezes, de modo que **ULJULJ** pode se transformar em **PEFNWZ**, que será enviada primeiro, antes da mensagem real. Os alemães exigiam esta repetição de modo a evitar os erros causados por interferências no rádio ou erros dos operadores. (Singh, p. 170)

De posse dessas informações Rejewski mecanizou o método de catalogar as correntes, e projetou as "Bombas", uma adaptação da Máquina Enigma, seis máquinas que simultaneamente rodavam a mensagem criptografada em busca de encontrar a Chave de Mensagem, o processo levava aproximadamente duas horas, sendo seis máquinas por que cada uma rodava em uma das seis possíveis formas de ser alocar 3 discos de cifras. Seriam amplamente conhecidas como Bombas de Rejewski.

Um curioso fato deste invento, é que os esforços de Rejewski eram de certo modo desnecessários, por conta de um objeto guardado no Biuro pelo major Guido Langer, diretor do setor, que detinha posse das chaves Diárias da Enigma Alemã.

> Através dos franceses, Langer ainda recebia informações de Shmidt. As atividades nefastas do espião alemão não terminaram em 1931 com a entrega dos dois documentos sobre a operação da Enigma, mas continuaram durante sete anos. Ele se encontrou com Rex, o agente secreto francês, em vinte ocasiões, frequentemente em chalés alpinos isolados, onde a privacidade era garantida. A cada encontro, Schimidt entregava um ou mais livros-código, cada um contendo um mês de chaves diárias [...]. No total ele forneceu livros-código contendo 38 meses de chaves diárias. (Singh, 2022 p. 177)

Porém o Major não revelou essas informações, pois existia a possibilidade da entrega dos livro-código cessarem, seria muito mais vantajoso taticamente a criação de um método que quebrasse a criptografia da Enigma, como foi conseguido por Rejewski. Pois o objetivo polonês era saber o que os generais alemães tinham em mente e se preparar previamente para um possível ataque, devido a posição vulnerável de seu país.

Em 1938 a Bomba de Rejewski sofre um ataque memorável dos Criptógrafos alemães, a Enigma sofre uma sutil alteração em seu projeto, é alterada de modo que os discos poderiam ser removidos e ter sua ordem alterada, o que aumentava em 6 vezes o número de possíveis arranjos. O ataque de 1938 é que os novos modelos da Enigma contariam com 5 Discos de Cifras distintos, de modo que a máquina usaria 3 deles por vez.

As alterações alemãs não parariam por aí, pois no projeto anterior, a Enigma tinha 6 fios com conectores que permutavam as letras do teclado entre si, novas versões feitas traziam 10 fios conectores, portanto o número de permutações possíveis cresceu notavelmente. Essas alterações impuseram um limite quase intransponível para o Biuro, um limite financeiro, pois seguindo a atual estrutura das Bombas de Rejewski, deveriam ser construídas 10 vezes mais bombas, o que geraria um custo 15 vezes maior do que o Orçamento Anual da instalação Polonesa.

A Polônia então compartilha com os Países Aliados, as descobertas de Rejewski, entregando os projetos e réplicas da Bomba para os Ingleses e Franceses, a cronologia da entrega não poderia ter sido mais precisa, pois duas semanas após a Enigma ser contrabandeada para Londres, os alemães invadem a Polônia.

4.1.7 O Bletchley Park

A descoberta dos avanços poloneses, gerou entre os ingleses um novo furor pela criptografia, já que a criação da Enigma havia frustrado muitos de seus esforços criptoanalíticos. Esse novo movimento provocou o Surgimento das Instalações do Bletchlley

Park, em Buckinghamshire, local onde era sediada a Escola de Cifras e Còdigos do Governo (Singh, 2022). Onde seriam recebidos uma corrente de homens e mulheres, que demonstravam os talentos para ciência e matemática necessários, recrutados principalmente nas Universidades de Oxford, Cambridge, Newnham e Girton.

No Bletchley Park, no ano de 1939, a equipe domina as técnicas de Rejewski e dispondo de maiores recursos estabeleceram uma rotina diária exaustiva capaz de lidar com mesmo com a criptografia da Enigma após o acréscimo de misturadores.

> "À meia-noite, os operadores alemães das Enigmas mudavam para uma nova chave diária e, nesse ponto, quaisquer avanços que a equipe de Bletchley tivesse feito no dia anterior não poderiam ser mais usados para decifrar mensagens. Os decifradores agora tinham que recomeçar o trabalho de identificação da nova chave diária. Isso levava várias horas, mas assim que descobriam os ajustes da Enigma para aquele dia, a equipe de Bletchley poderia começar a decifrar as mensagens alemãs que já tinham se acumulado, revelando informações inestimáveis para o esforço de guerra," (Singh, 2022, p. 183)

Todo esse trabalho deveria permanecer em sigilo, então além de impor sigilo sobre toda a equipe de decifradores, o governo Britânico deveria usar as informações de modo que o Comando Alemão não percebesse que havia interceptação de suas informações, do contrário mudariam o modo da criptografia tornando os esforços do Bletchley Park vãos.

Os ingleses aprimoraram os métodos poloneses e desenvolveram técnicas de criptoanálise, como notar padrões redundantes nas Chaves de Mensagem, como o uso pelos operadores alemães de três letras consecutivas, padrões nas trocas dos misturadores, os quadros de tomadas dos teclados, dificilmente faziam trocas entre letras vizinhas (teoria das trocas óbvias), entre outros, e os testavam antes de lançar mão do modo mais difícil.

Ainda em 1939, a Escola de Cifras e Códigos do Governo, sediada no Bletchley Park faz uma notável aquisição, convida o acadêmico da Universidade de Cambridge, Alan Turing para compor sua equipe de Criptoanalistas. Turing é considerado um dos pais dos computadores ao reinventar o Motor Diferencial, referenciado ao Trabalho de Babbage, "fornecera uma sólida base teórica para a computação, dando ao computador um potencial até então não imaginado. Mas ainda era a década de 1930 e não existia tecnologia para transformar em realidade a máquina Universal de Turing" (Singh pg 190)

Sua busca era encontrar uma alternativa ao trabalhoso método de Rejewski, ele analisou a biblioteca de mensagens decifradas do Bletchley na busca por padrões que subsidiassem uma nova abordagem de criptoanálise das mensagens alemãs. Um dos padrões observados, eram os relatórios meteorológicos diários e uniformidade desse tipo de texto. "(...) a experiência poderia

indicar-lhe que as primeiras seis letras de um texto cifrado em particular correspondiam a **wetter**. E sempre que um pedaço de texto original pode ser associado com um pedaço de texto cifrado, essa combinação é conhecida como *cola*." (Singh, 2022, p. 191, grifo do autor)

De modo semelhante a Rejewski, Turing concentrou-se nas ligações internas de algumas colas em particulares, todavia, diferente de seu antecessor, os elos de Turing não tinha relação com a Chave de Mensagem, pois conectavam o texto original ao texto cifrado através das *colas*.

Turing desenvolve um circuito elétrico com combinações de máquinas enigma, de um modo que ignora as combinações do quadro de tomadas, após vários testes e reformulações do projeto e com um investimento de cem mil libras obtido pelo Bletchley surgem "As Bombas de Turing", que combinavam colas, elos e máquinas conectadas por meio de eletricidade.

> "Cada uma das bombas de Turing consistia em doze conjuntos de misturadores Enigma conectados eletricamente e assim era capaz de lidar com elos muito mais longos de letras. A unidade completa teria dois metros de altura, por dois de comprimento e um metro de largura." (Singh, 2022, p. 197)

Contudo os primeiros protótipos não deram os resultados esperados, e no mesmo ano, os criptoanalistas sofreram um ataque intenso dos criptógrafos alemães, que mudaram o protocolo de troca de chaves, parando de repeti-las ao início das frases. Ataque este que provocou um hiato de informações preocupante num contexto de guerra, mas, que acabaria rápido com a chegada de Agnus Dei, a nova Bomba de Turing, que seria um marco importante para a definição do conflito. Infelizmente muitos criptoanalistas, inclusive o próprio Turing não viveriam para receber o reconhecimento por seu trabalho secreto, pois o sigilo dos esforços no Blenchley Park só seria quebrado três décadas depois.

4.1.8 A Quebra do Axioma de Mão Única

Ao longo de toda a história da criptografia narrada até então, um fato permanece: a necessidade de distribuição de chaves entre emissor e destinatário de uma mensagem. O que era chamado de Axioma da Criptografia ou Axioma de Mão Única. Para que uma mensagem encriptada fosse lida pelo destinatário este precisava saber o tipo de criptografia usado e a chave de desencriptação.

Pudemos observar no caso do telegrama Zimmerman que a necessidade de Distribuição de Chaves na criptografia consistia na maior fraqueza de qualquer método, pois deixava toda

comunicação exposta a espionagem, traições, chantagens e congêneres. Contudo por quase 2000 anos o Axioma da Criptografia permaneceu inalterado.

Sabendo que quem quebrasse o Axioma e encontrasse um modo de estabelecer uma comunicação criptografada sem a distribuição de chaves entraria na história, desponta, na década de 1970, o criptógrafo especialista em segurança William Diffie. O contexto para esse tipo de pesquisa não podia ser mais estimulante, pois estava nos primórdios do surgimento da internet, ou na época ainda ARPANET, criada em 1969, fruto do projeto Americano que criou uma organização chamada Agência de Projetos Avançados de Pesquisa (de onde em Inglês vem a sigla ARPA)

> "Um dos projetos de vanguarda da ARPA era encontrar um meio de conectar os computadores militares através de grandes distâncias. Isso permitiria que um computador danificado transferisse suas responsabilidades para outro computador da rede. O objetivo principal consistia em tornar a infraestrutura da computação do Pentágono mais robusta diante de um ataque nuclear, mas a rede também permitia que os cientistas enviassem mensagens uns para o outro e fizessem cálculos explorando a capacidade ociosa dos computadores remotos." (Singh, 2022, p. 278)

Ao fim daquele ano já haveriam quatro locais, em inglês *sites,* conectados. As pesquisas avançariam até darem origem à Internet no ano de 1982. Seu uso cresceu exponencialmente atingindo o público para além do ambiente universitário e militar.

Nesse contexto William Diffie se antecipa a um problema futuro, a criptografia de comunicações não simultâneas, pois pensava que futuramente as pessoas teriam computadores conectados a Internet pela rede telefônica, e que enviariam mensagens, que posteriormente seriam os e-mails e que deveriam ter o direito a garantir a sua privacidade. Aqui ele esbarra no problema da troca de chaves.

> "Diffie imaginou dois estranhos se encontrando via Internet e se perguntou como eles poderiam trocar uma mensagem cifrada. Ele também considerou o cenário de uma pessoa querendo comprar um produto na Internet. Como esta pessoa poderia mandar um e-mail contendo informações cifradas sobre seu cartão de crédito, de modo que apenas o vendedor da Internet pudesse decifrá-las? Em ambos os casos parecia que as duas partes precisariam trocar uma chave, mas como elas poderiam trocar uma chave em segurança?" (Singh, 2022, p. 279)

Já prevendo a grande quantidade de interações via Internet, sabendo da necessidade de tantas trocas de chave de criptografia e sendo ativista da privacidade digital, Diffie inicia seu processo de pesquisa ao qual, junta-se Martin Hellman, um professor da Universidade de Stanford, que contrata Diffie como estudante graduado, posteriormente Ralph Merkle se junta a eles também, a característica que os unia é justamente serem desacreditados por seus pares sobre a possibilidade da quebra do axioma,

Simon Singh traz uma interessante analogia sobre a necessidade da chave de criptografia, ilustrando com a comunicação entre dois personagens fictícios Alice e Bob, que está sob a tentativa de espionagem de Eva, o terceiro personagem:

> "Alice quer mandar uma mensagem altamente pessoal para Bob. Novamente ela coloca sua carta secreta em uma caixa de ferro com cadeado e envia para Bob. Quando a caixa chega, Bob coloca nela o seu próprio cadeado e a envia de volta para Alice. Quando Alice recebe a caixa, ela agora está trancada com dois cadeados. Ela remove o seu próprio cadeado deixando apenas o cadeado de Bob para impedir a abertura da caixa. Finalmente ela envia a caixa de volta para Bob. E aqui está a diferença crucial: agora Bob pode abrir a caixa porque ela está fechada apenas com o seu cadeado, para o qual só ele tem a chave." (Singh, 2022, p. 283)

Um problema matemático surge nessa situação: Que tipo de Função/Criptografia usar de modo que sobre uma mesma mensagem suas criptografias sejam sobrepostas, de modo que a mensagem original apareça ao fim da desencriptação? A ordem das cifragens e decifragens gera um problema, exemplificando: É como se uma pessoa que durante o inverno usa luvas, quisesse tirar primeiro o anel, sem tirar a luva. Isso funcionava no exemplo dos cadeados, mas, no exemplo da luva e do anel não, pois no caso dos cadeados a ordem não importava.

Diffie e Hellman passaram a procurar uma solução dentro das várias funções matemáticas, especificamente buscavam funções de mão única. Uma função em que a inversão se dá nela mesma, o que vai no sentido oposto da maioria das funções que são da forma $f: x \rightarrow y$, onde é preciso uma função inversa tal que $f^{-1}: y \rightarrow x$.

> "Em outras palavras, as funções de mão dupla são reversíveis, enquanto as funções de mão única são irreversíveis. Novamente, o melhor modo de ilustrar uma função de mão única é pensar nas atividades do dia-a-dia. Misturar tinta amarela com tinta azul para produzir tinta verde é uma função de mão única porque é fácil misturar as tintas, mas impossível desfazer a mistura. Outra função de mão única é quebrar o ovo, mas impossível fazer o ovo voltar a sua condição original" (Singh, 2022, p. 286)

Um campo propício para os intuitos desses matemáticos foi a Aritmética Modular, onde são encontrados diversos exemplos de funções de mão única. Com o auxílio dela, Hellman consegue provar a possibilidade de duas pessoas, Alice e Bob no exemplo mencionado acima, estabelecerem uma chave de encriptação sem se encontrarem. Através da função de mão única $Y^x(modP)$.

Conforme exemplifica Singh: *"Inicialmente Alice e Bob escolhem os valores de Y e P. Quase qualquer valor serve, mas existem algumas restrições tais como Y ser menor do que P"* (Singh, 2022, p. 289). Esses valores Y e P são públicos, em seguida eles escolhem uma chave, normalmente números muito grandes, existe um Padrão de Cifragem de Dados, um conjunto

de 10^{17} chaves feito pela NSA (Agência de Segurança Nacional Americano) e usado até os dias atuais, todavia para fins demonstrativos escolheremos um número menor.

Supondo que Alice e Bob escolham como Y=6 e P=13. Organizando os passos dados por eles na tabela abaixo temos:

Quadro 3 - Exemplo de Alice e Bob, aplicação criptografia RSA

	Alice	Bob
Fase 1	Alice escolhe o número $A = 4$, mantendo-o em sigilo	Bob escolhe o número $B = 5$ e também o mantém em sigilo
Fase 2	Alice calcula $f(A) = 6^4 (mod\ 13)$ Obtendo $6^4 \equiv 1296 \equiv 9(mod 13)$	Bob calcula $f(B) = 6^5 (mod\ 13)$ Obtendo $6^5 \equiv 7776 \equiv 2\ (mod 13)$
Fase 3	Alice denomina $\propto = 9$ e envia essa informação para Bob	Bob denomina $\beta = 2$ e encaminha essa informação para Alice
A troca	No momento do envio de $\propto$ e β, essas informações poderiam ser ouvidas no telefone por EVA. Que apenas saberá das informações $\propto = 9$ e $\beta = 2$	
Fase 4	Através da expressão $\beta^A (mod 13)$, Alice chega a chave: $2^4 \equiv 16 \equiv 3\ (mod 13)$	Com a expressão $\alpha^B (mod 13)$, Bob determina a chave: $9^5 \equiv 59049 \equiv 3\ (mod\ 13)$

Fonte: Adaptada de Singh, 2022, p. 290

Alice e Bob, portanto conseguem compartilhar a chave de modo secreto, pois os números A e B não foram compartilhados via Linha Telefônica, sendo dessa forma, desconhecidos por Eva, e sendo aplicados no mesmo mod13 ao fim temos uma chave igual. Eva poderia tentar fazer a reversão dos cálculos para determinar A ou B, todavia o processo será muito difícil pelo caráter de mão única da função, além de que na criptografia seriam usados números muito maiores. Dificultando o cálculo.

> "O esquema de troca de chaves de Diffie-Hellman-Merkle, como é conhecido permite que Alice e Bob estabeleçam um segredo através de um debate público. Esta é uma das descobertas mais racionais da história da ciência e forçou o estabelecimento criptográfico a reescrever suas regras. Diffie, Hellman e Merkle demonstraram publicamente a sua descoberta na Conferência Nacional de Computação, em junho de 1976, ante um público perplexo de especialistas de criptografia. No ano seguinte eles requereram a patente. Daí em diante Alice e Bob não precisavam mais se encontrar para trocar uma chave. Alice só precisa agora telefonar para Bob e trocar um par de números com ele, estabelecendo uma chave secreta mútua e a partir daí cifrar a mensagem." (Singh, 2022, p. 292)

Embora represente um avanço notável, essa descoberta dá a solução para o compartilhamento secreto de uma chave sem necessidade de encontro, contudo, gera uma nova questão para a Criptografia, trazendo a limitação da comunicação acontecer simultaneamente. De modo que no caso do envio de um email entre nossos personagens fictícios, Alice e Bob, ambos precisariam estar conectados para cifrar e enviar a mensagem, ou então, uma pessoa

enviar sua parte da troca de chaves e aguardar a outra estar online para receber a outra parte e a comunicação de fato acontecer.

Diffie se debruça sobre essa dificuldade criando a Chave Assimétrica, onde a chave de cifragem e a de decifragem não são idênticas, o que novamente foi revolucionário, já que antes da criação de Diffie só havia criptografia de Chaves Simétricas. Nesse tipo de criptografia o Emissor possui a Chave de Cifragem todavia não possui a Chave de Decifragem. Nesse sistema existe uma Chave Pública, que seria amplamente divulgada e uma Chave Particular. Deste modo quando um Emissor deseja enviar uma mensagem um Destinatário, este usará a Chave Pública do Destinatário para cifrar a mensagem, e ao receber o Destinatário usará sua Chave Particular para desencriptá-la.

Embora Teoricamente estaria resolvida a necessidade de comunicação simultânea, Diffie e seus companheiros não conseguiram desenvolver a aplicação prática do conceito, Diffie publicou um resumo de sua ideia em 1975. Contudo essa descoberta teórica serviu de pavimento para a estrada da construção do Método de Criptografia RSA.

4.1.9 Surgimento Da Criptografia Rsa

O trio de Stanford com suas pesquisas inovadoras inspira um outro trio de pesquisadores: Ron Rivest, Leonard Adleman e Adi Shamir, pesquisadores do Laboratório de Ciência de Computação do MIT (sigla inglesa de Instituto de Tecnologia de Massachusetts, nos Estados Unidos), sendo Rivest e Shamir cientistas da computação e Adleman matemático atuando como detector de falhas nas ideias dos dois primeiros, ambos tiveram os estudos motivados pela busca de um método de aplicação da Cifra Assimétrica.

Desta colaboração surgiu o Sistema RSA, sigla dos sobrenomes de seus criadores, sistema de grande relevância para a criptografia moderna. A ideia deles também seria baseada nas Funções de Aritmética Modulares, pelo seu aspecto de mão única, contudo com uma aplicação sobre os números primos. Um dos aspectos que diferem o RSA é o (mod N), onde $N = p.q$, sendo $p\ e\ q$ números primos muito grandes. Novamente recorrendo aos personagens Alice e Bob, temos esse exemplo feito por Singh:

> "Assim Alice pode escolher seus números primos como $p = 17.159$ e $q = 10.247$. Multiplicando esses dois números, o resultado é $N = 17.159 \times 10.247 = 175.828.273$. A escolha de Alice em relação ao N se transforma em sua chave de cifragem pública e ela pode imprimi-la em seu cartão de apresentação, coloca-lo na

> Internet ou publicá-lo num diretório de chaves públicas junto com os valores de N de outras pessoas. Se Bob quiser cifrar uma mensagem para Alice, ele olha o valor do N de Alice (175.828.273) e o insere na forma geral da função de mão única, a qual também será de conhecimento público. Bob agora tem uma função de mão única feita sob medida com a chave pública de Alice (...). Para cifrar uma mensagem para Alice ele pega a função de mão única dela, insere uma mensagem, anota o resultado e envia para Alice." (SINGH, 2022, p. 300)

Por definição a decodificação dessa mensagem é muito difícil, pelo caráter da primalidade de "p" e "q", é fácil calcular que se N = 33, os valores de "p" e "q" serão 3 e 11, não necessariamente nessa ordem, contudo sendo "p" e "q" primos de grande magnitude, ainda que a chave seja pública o processo de descobrir o valor de N por fatoração será muito difícil, por não existirem, ainda, funções que consigam relacionar todos os números primos.

De modo ilustrativo, é relativamente simples com uma calculadora comum, ou mesmo sem ela tomar os números primos 8.387 e 6.949, determinando que seu produto seja 58.281.263, gastando-se poucos segundos. Contudo será um trabalho insalubre e moroso fatorar 58.281.263. No método RSA são usados primos de muito mais casas decimais do que os desse exemplo. (Singh, 2022)

O Sistema RSA é conhecido como Criptografia de Chave Pública, não necessitando de troca de chaves entre Emissor e Remetente, tampouco comunicação simultânea. A seguir será apresentado um modelo de funcionamento do Sistema RSA. Comumente os textos tem os caracteres convertidos em código, um amplamente utilizado é o ASCII estendida (sigla em inglês para American Standard Code for Information Interchange), que tem como base o conjunto de caracteres Windows-1252, com 256 caracteres e símbolos, representados através de 8 bits. Contudo abaixo será usada uma tabela simplificada, para fins demonstrativos, contendo apenas letras do alfabeto.

Uma versão paralela da criação da Criptografia RSA

Uma visão alternativa da RSA é devida ao remanescentes do Bletchley Park, que mesmo após o encerramento das atividades, formaram o GCHQ (sigla inglesa para Quartal-General de Comunicações do Governo), em Cheltenham. E a história da descoberta americana da RSA, se inicia da preocupação de que com a miniaturização dos rádios, fossem encontrado um modo mais econômico para uma criptografia de multiplas comunicações, especificamente buscavam um modo mais econômico para a distribuição de chaves para comunicações secretas.

Neste contexto desponta James Ellis, criptógrafo de renome do governo britânico, conhecido como *Criptoguru* (Singh, 2022), integrante da Estação de Pesquisas dos Correios em Dollis Hill, divisão onde foi inventado o Colossus, o primeiro computador para quebra de código. Esta divisão foi incorporada pelo GCHQ. Através de um relatório da Bell Telephone, Ellis começou a abordar o conceito do ruído numa comunicação secreta, em que o destinatário da mensagem obtivesse uma forma de remover o ruído, desta forma receberia a comunicação, e esta estaria oculta aos interceptores, uma forma de análise semelhante à dos cadeados, explanada anteriormente.

Ele provou que existia a condição possível para a criação de uma chave pública, que solucionaria o problema de distribuição de chaves.

> As ideias de Ellis eram muito semelhantes às de Diffie, Hellman e Merkle, exceto que ele estava vários anos à frente deles. Mas ninguém sabia do seu trabalho, porque ele era um funcionário do governo britânico e tinha jurado segredo. No final de 1969, Ellis parecia ter chegado ao mesmo impasse que o trio de Stanford alcançaria em 1975. (Singh, 2022, p. 309)

Contudo Ellis não era um matemático, e embora tenha tentado alguns tipos de funções matemáticas que chegassem a um modelo de chave pública não obteve sucesso, foi delegado então aos demais cientistas do GCHQ a busca por uma função de mão única. Até que em 1973, Clifford Cocks, matemático recém integrado ao departamento se debruça sobre ideia, no qual ele relata:

> Não havia nada de especial acontecendo, e assim eu achei que podia pensar um pouco na ideia. Como estivera trabalhando com a teoria dos números, era natural pensar em funções de mão única, algo que você pode fazer mas não pode desfazer. Os números primos e a fatoração eram candidatos naturais, e assim eu comecei por eles. (Singh, 2022, p. 310.)

Os alicerces da criação inglesa do que foi conhecido como Sistema RSA estavam lançados, quatro anos antes do trio do MIT, Cocks também concluiu o processo de estruturação lógica com uma rapidez maior. Porém o mesmo que ocorreu com Alan Turing, na quebra do código da Máquina Enigma, ocorre também com Ellis e Cocks por conta do acordo de confidencialidade do Governo Britânico. Houve ainda Malcolm Williamson, do mesmo GCHQ, que na tentativa de encontrar algum erro na função de Cocks, acabou descobrindo a troca de chaves quase que contemporaneamente ao trio de americanos do MIT. Contudo essas descobertas vieram a conhecimento público muito depois que a criptografia RSA já era patenteada, com reconhecimento científico e aplicações comerciais lucrativas.

4.1.10 Um adendo sobre privacidade

As previsões de Diffie se realizaram e na era da informação grande parte das comunicações são feitas via internet, o que colocou o debate sobre a Criptografia para além da segurança, alcançando a esfera dos Direitos Civis no que tange a Privacidade. Debate capitaneado por *instituições de defesa dos direitos humanos*, bem como *grandes corporações* comerciais, de um lado e do outro *governos* juntamente com suas Agências de Segurança.

> "Contudo, o sucesso da Era da Informação depende da capacidade de proteger essas informações enquanto elas fluem ao redor do mundo e isto depende do poder da criptografia; A cifragem pode ser vista como a fonte das chaves e trancas da Era da Informação. Durante dois mil anos ela foi importante apenas para o governo e os militares, mas hoje ela também tem um papel a desempenhar na facilidade dos negócios e, no futuro, pessoas comuns dependerão da criptografia para proteger sua privacidade" (Singh, 2022, p. 319)

Este futuro prescrito por Singh no final do segundo milênio chegou de modo muito rápido a sociedade, com o advento dos Smartphones, democratização dos Computadores Pessoais e Laptops, aplicativos bancários e congêneres. A criptografia RSA passa a ser usada em larga escala, no intento de proteger informações e comunicações, o que apresenta um lado negativo, pois grupos criminosos podem desenvolver suas comunicações protegidas contra a interceptação de agências de segurança.

Esse debate teve como pioneiro Phil Zimmermann, físico e cientista da computação, que atuou como ativista político contra armas nucleares e posteriormente, pela privacidade digital. Outro debate suscitado na época foi o da assinatura digital, que garantisse a autenticidade de um e-mail, por exemplo, essa necessidade gerou um novo dilema para a criptografia RSA, já que esta exigia uma capacidade de computação de dados muito maior do que os computadores comerciais comuns da época. *"Consequentemente, na década de 1980, apenas o governo, os militares e as grandes empresas possuíam computadores suficientemente poderosos para rodar a RSA."* (Singh, 199, p. 324)

Em seu ativismo Zimmermann desejava que a Cifragem RSA pudesse ser usada pela população geral, e desenvolveu o PGP (sigla inglesa de Pretty Good Privacy, traduzida como: Uma Ótima Privacidade), uma interface de uso mais simples para o usuário comum, bem como, com um processo criptográfico menos exigente para computadores pessoais.

> Para acelerar a cifragem e a decifragem, Zimmermann empregou um truque muito hábil que usa a cifragem assimétrica RSA associada com a velha cifragem simétrica. A cifragem simétrica tradicional pode ser tão segura quanto a cifragem assimétrica e é muito mais rápida de ser feita, mas sofre com a necessidade de exigir a distribuição

> de uma chave, que terá que ser transportada em segurança do remetente ao destinatário. É aí que a RSA vem em nossa ajuda, porque ela pode ser usada para cifrar a chave simétrica. (Singh, 2022, p. 324)

Zimmermann usou a cifra IDEA dentro do PGP, de modo que toda a comunicação era cifrada por meio dela, e apenas a chave era cifrada em RSA. Portando ao enviar uma mensagem o destinatário usaria a RSA, uma cifragem de maior exigência de poder computacional, apenas para decifrar a chave, já que a criptografia RSA em si não necessita de compartilhamento de chaves entre as partes da comunicação. Então de posse da chave descriptografada o destinatário conseguiria ter acesso a informação cifrada em IDEA, essa nova aplicação da RSA era mais acessível para computadores pessoais e outra vantagem era a automatização do processo dentro do aplicativo, que beneficiava o usuário com pouco conhecimento matemático.

Uma outra aplicação do PGP para fins de segurança digital é a possibilidade da assinatura digital de um e-mail, onde o Emissor da Mensagem cifra-a inicialmente com a sua própria Chave Particular e em seguida com a Chave Pública do Destinatário, retomando o que foi visto anteriormente, a Chave Particular pode ser decifrada por qualquer usuário da rede, contudo, a Chave Pública de uma Pessoa só pode ser decifrada por ela mesma. Nesse método de cifragem consiste a assinatura digital, pois quando o destinatário utiliza quebra a criptografia pública da mensagem, dentro desta haverá a criptografia pessoal do Emissor, de modo que é confirmada a autenticidade da mensagem. (conforme Singh, 2022. Pg 326-226)

A potência da PGP é atestada por William Crowell, vice-diretor da NSA:

> “Se todos os microcomputadores do mundo – aproximadamente 260 milhões de computadores pessoais – fossem colocados para trabalhar em uma única mensagem PGP, levaríamos, em média, 12 milhões de vezes a idade do universo para decifrar uma única mensagem.” (Singh, 2022, p. 345)

A PGP foi disponibilizada na rede com código aberto, de modo que pudesse ser alterada por novos usuários, ocasionando problemas ao seu emissor, pois o Sistema RSA, que consistia parte importante da criptografia da PGP era patenteado pela RSA Data Security Inc, o que evoluiu para um processo judicial contra Zimmermann. Contudo o que lhe causou maior problema, foi que o compartilhamento em rede, sem autorização do governo Americano, de uma tecnologia criptográfica ia de contra as leis de segurança nacional da época, que classificava a tecnologia criptográfica como uma arma, sendo então o autor acusado de Tráfico Internacional de Armas.

Tal imbróglio se arrastou por anos de processo, ativismo, Phil recebeu apoio de entidades de direitos humanos, grandes corporações comerciais, e por fim o interesse e apoio

da sociedade civil, da comunidade científica incluindo os criadores do RSA, e mesmo da indústria cinematográfica, fazendo o governo retirar as acusações com o tempo. Todo esse embate mostra como a Criptografia divide opiniões e semeia o debate sobre a Privacidade Digital.

5 PADRÕES DE ESCOLHA E RECOMENDAÇÕES DE CRIAÇÃO DE SENHAS

Para cada tipo de uso, um determinado tipo de senha é permitido ou aconselhado, por exemplo, para cartão de crédito/débito usamos apenas senhas numéricas entre 4 a 8 caracteres, para e-mails e aplicativos varia de suas configurações. A medição de força de uma senha é denominada Entropia como detalha Roccia:

> "(...) a entropia na teoria da informação consiste na incerteza dos possíveis valores de uma variável randômica. O grau de incerteza de uma senha pode ser calculado, assumindo a independência e uniformidade de cada caractere, a partir da seguinte fórmula: $H = \log_2 b^l$. Onde b é o número de caracteres possíveis, l é o número de caracteres utilizados e H é a entropia da senha medida em bits" (Roccia, 2021, p. 5)

O Departamento de Defesa Americano, em 1985, lança um conjunto de orientações sobre como os usuários poderiam lidar com as senhas que resultou nas regras abaixo:

1. Cada senha deve ser única, consiste grande erro usar a mesma senha para diversos sistemas, pois dará vantagem a usuários maliciosos que descobrem esta senha em um dos sistemas.

2. A primazia é pela memorização da senha. Caso seja armazenada em Papel, o deverá ser feito em local seguro.

3. As senhas devem ter ao menos seis caracteres, de preferência mais, a depender do conjunto de caracteres usados, quanto menos diversos os conjuntos de caracteres, maior deve ser a senha.

4. Com periodicidade as senhas devem ser substituídas

5. A composição das senhas deve ser feita com: Letras maiúsculas e minúsculas, números e caracteres especiais. (Silva; Stein, 2007)

Acrescenta-se evitar uso de nomes de usuário na senha, bem como informações pessoais de fácil acesso. Ainda que letras maiúsculas e caracteres especiais contribuam substancialmente para o nível de Entropia de uma senha, estes ainda aparecem pouco nas maiorias de senhas analisadas, como mostra Roccia em seu estudo sobre os dados levantados pelo programa zxcvbn de Dan Wheeler que analisou uma base de dados de mais de 200 milhões de senhas, expondo-as a diversos ataques criptográficos que mostra que dos caracteres analisados 63% são letras minúsculas; 33,6% são dígitos(números); 3,1% são letras maiúsculas e apenas 0,3% são caracteres especiais. Dessa forma a despeito das recomendações de segurança o uso de caracteres que melhorem uma senha é negligenciado pelos usuários. (Roccia, 2021)

Para ilustrar o exposto acima sobre a disparidade entre o uso real de caracteres na pesquisa contra o que seria recomendado: Se considerada uma senha de 8 caracteres, padrão costumeiro, com obrigatoriedade de 1 número, 1 letra maiúscula, 1 letra minúscula e 1 caractere especial, a porcentagem de caracteres especiais e letras maiúsculas deveria ser ao menos 12,5% cada.

Contudo, Silva & Stein oferecem um contraponto a esta diretriz do Governo Americano, diante da percepção do usuário dos sistemas:

> Por outro lado, do ponto de vista do usuário, a autenticação é apenas uma tarefa obrigatória para ter acesso aos recursos necessários à realização do trabalho real. Sob essa ótica, uma boa senha deveria ser facilmente disponível, não requerer equipamento especial nem conhecimento técnico, ser conveniente (isto é, não consumir muito tempo) e, acima de tudo, ser fácil de lembrar. Essas motivações, associadas às limitações cognitivas dos seres humanos conflitam diretamente com as recomendações do DoD. (Silva; Stein, 2007, p. 49)

Assim o componente humano deve ser levado em consideração para além da tecnologia de criptografia, pois ainda que os sistemas se atualizem, caracteres sejam adicionados e o número de senhas possíveis aumente exponencialmente ao longo do tempo como demonstrado, a consciência de que se evite padrões repetitivos, como senhas ligadas a informações pessoais, precisa ser formada nos usuários dos sistemas. Os padrões de comportamento dos Usuários dos Sistemas têm se tornado objeto de estudo ao longo das décadas tanto pelos responsáveis por fortalecer os protocolos de segurança, quanto pelos interessados em quebrar esses protocolos para usos privados, institucionais ou criminosos.

Fazendo referência a um estudo Brown (2004) Silva & Stein detalham alguns desses comportamentos recorrentes entre os usuários de sistemas:

> [...] entrevistaram 218 estudantes de graduação para avaliar a geração e o uso de senhas. Com base em um levantamento prévio, 19 itens foram incluídos no questionário, como conta bancária ou e-mail. Para cada item, os participantes deveriam descrever o tipo de informação usada para criar ou lembrar da senha. Os resultados mostraram que dois terços das senhas foram geradas em torno de características pessoais dos usuários e a maioria das senhas restantes se relacionava à família, amigos ou relacionamentos amorosos. Nomes próprios e aniversários compunham aproximadamente metade de todas as senhas levantadas. O estudo ainda encontrou suporte empírico para os maus hábitos mencionados acima. Quase todos os entrevistados reusavam senhas e mais da metade deles mantinha uma cópia escrita de suas senhas. (Silva; Stein, 2007, p. 51)

O estudo de Roccia, baseado num tratamento de dados americano, feito com mais 200 milhões de senhas analisadas de um banco de dados corrobora:

> A tendência dos usuários de inserirem informações pessoais em suas senhas mostrou-se verdadeira nas análises dos padrões de senha. Surpreendentemente, foram encontradas palavras em inglês e nomes em quantidades tão altas quanto a aparição de senhas consideradas comuns. A concentração das datas em anos recentes indica a utilização de datas de nascimento nas senhas. E a diferença dos nomes encontrados de acordo com o país de origem do dataset ficou explícita. (Roccia, 2021, p. 41)

Dessa forma embora existam diretrizes de segurança, elas são comumente ignoradas, mesmo para públicos com grau de instrução, estudantes de graduação, substancialmente maior que o substrato geral da população. Estatisticamente esses "maus hábitos" reduzem muito a gama de senhas possíveis, facilitando em muito a invasão da conta por um dos 3 ataques mais comuns.

Destacando que após uma investigação da vida do usuário, o que está facilitado pelo grau de exposição das pessoas nas redes sociais, informações como: nome de usuário, data de aniversário, cidade de residência, localidade de nascimento, idade, nome e sobrenome de familiares e pessoas próximas, hábitos de trabalho, etc, estão facilmente públicas e acessíveis, reduzindo em muito um Ataque Criptográfico de Força Bruta, relacionando as informações pessoais recolhidas, isso num contexto de usuários com "maus hábitos" na proteção de seus dados.

Pode-se aliar esses dados coletados a outros padrões viciosos de uso, como o de colocar os dígitos da senha apenas no final, padrão encontrado em 11 milhões (5,5%) dentre as mais de 200 milhões de senhas citadas na pesquisa de Roccia, dentre essas senhas, com números ao final, 13,94% tinham o número '1' e 4,75% a sequência numérica '123', ou mesmo referência a filmes como '007', além de sequências numéricas longas como '123456' e '1234' que ocupam respectivamente 1,96% e 1,52% do total de senhas pesquisadas (Roccia, 2021)

Padrões como esses surgem pela falta de criteriosidade do usuário na criação de senha, onde diante, muitas vezes, da exigência da plataforma onde a senha será usada escolhem as combinações que primeiro veem a mente, reduzindo o padrão aleatório de criação de senha. Diante disso, num ataque criptográfico de força bruta, esses padrões viciosos de criação de senha podem ser inseridos no programa utilizado para a quebra da senha, encurtando o tempo de quebra da senha.

O padrão de datas é recorrente como afirma Roccia: *"Usar anos ou datas recentes na senha consiste num padrão bem frequente nas senhas analisadas. Aparecendo isolado ou junto com uma data, os anos encontrados não diferem muito entre os dois padrões."* (Roccia, 2021, p. 33). Um exemplo clássico: uso de datas de aniversário para senhas numéricas de 04

caracteres. Existem apenas 365 (ou 366 para ano bissexto, aqui se ignorará essa possibilidade) dias no ano dividido em 12 meses. Portanto os dois primeiros dígitos, referente ao dia irão de 01 a 31, enquanto os dois últimos, referente aos meses irão de 01 a 12. Uma senha de 4 caracteres comuns terá 10^4 senhas possíveis, contra 365 datas de nascimento possíveis, representando 3,65% do espaço amostral, um “mau hábito” de criação de senha que facilita muito a vida dos usuários.

Dentre as questões cognitivas que envolvem esse processo de acondicionamento de senhas, destacam-se: a) Dificuldade em guardar as informações de modo literal, a ordem de caracteres e detalhes superficiais. b) Informações com significado são mais facilmente memorizadas, em detrimento de senhas aleatórias; c) O fator tempo, tende a fazer esquecer informações como traços literais, e estrutura da senha; d) Informações parecidas tendem a se misturar na mente do usuário interferindo no registro das informações, aqui salienta-se o caso de senhas parecidas. (Silva; Stein, 2007) Em suma o usuário deve optar por senhas grandes, memorizáveis e com caracteres diversos.

Diante do exposto aqui, criptografar a senha em um sistema que facilite a vida do Usuário, gerando senhas através de uma Palavra-Chave de fácil memorização pode consistir em uma vantagem salutar para alinhar as necessidades de segurança recomendadas pelos diversos órgãos especializados juntamente com a dificuldade de memorização comum aos usuários dos sistemas, e a fragilidade em deixar senhas anotadas de forma explícita. Especialmente num contexto de senhas diversas, sabendo que existe dificuldade de memorização de senhas aumentadas para usuários com mais de 8 a 11 senhas (Silva; Stein, 2007), assim falhas de memorização, unidas a estratégias inseguras de criação e proteção de senhas anotadas geram a dificuldade mais sensível de segurança digital ao usuário comum.

6 APLICAÇÕES DAS TEORIAS MATEMÁTICAS PARA A SEGURANÇA DIGITAL

Neste capítulo a segurança digital age como eixo temático por onde circulam as teorias matemáticas e de ensino, metodologias e contribuições da revisão literária para uma aplicação da criptografia e da análise combinatória.

6.1 Codificação Usando a Criptografia Rsa

Será codificada a palavra PROVIDÊNCIA, ignorando o acento.

Passo I) Esta será transformada em um código numérico, chamada **Pré-Codificação**, para em seguida ser criptografada, conforme quadro abaixo:

Quadro 4 - Pré-codificação de letras do alfabeto

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
10	11	12	13	14	15	16	17	18
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
19	20	21	22	23	24	25	26	27
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
28	29	30	31	32	33	34	35	

Fonte: Elaborada pelo autor

Passo II) Para a codificação deverá ser escolhida a Chave Pública de Codificação N, neste exemplo será usado p=7 e q=5, deste modo N=35.

Passo III) O código de PROVIDÊNCIA, obtido substituindo suas letras pelos números respectivos conforme quadro acima, será 252724311813142312 1810 e deverá ser divido em blocos de tamanhos menor do que N. Para o caso serão divididos em blocos de dois números: 25-27-24-31-18-13-14-23-12-18-10.

Passo IV) Para cada bloco ‘b’, tomando um determinado Y, que deve ser ímpar, se determina um valor a, que será o valor criptografado do bloco. A expressão utilizada é $b^Y \equiv X(modN)$. De forma demonstrativa será usado Y=5, a aplicação será feita na tabela abaixo:

4 - Exemplo de aplicação da Criptografia RSA

b	$b^5 \equiv X(\mathrm{mod}35)$	**X**	b	$b^5 \equiv X(\mathrm{mod}35)$	**X**
25	$25^5 \equiv 30(\mathrm{mod}35)$	**30**	13	$13^5 \equiv 13(\mathrm{mod}35)$	**13**
27	$27^5 \equiv 27(\mathrm{mod}35)$	**27**	14	$14^5 \equiv 14(\mathrm{mod}35)$	**14**
24	$24^5 \equiv 19(\mathrm{mod}35)$	**19**	23	$23^5 \equiv 18(\mathrm{mod}35)$	**18**
31	$31^5 \equiv 26(\mathrm{mod}35)$	**26**	12	$12^5 \equiv 17(\mathrm{mod}35)$	**17**
18	$18^5 \equiv 23(\mathrm{mod}35)$	**23**	10	$10^5 \equiv 5(\mathrm{mod}35)$	**5**

Fonte: Elaborada pelo autor

Portanto o código criptografado para a palavra providência ficará 302719262313141817235.

O Processo de Desencriptação se dá pela expressão $X^d \equiv b(mod\ n)$, sendo 'n' o mesmo $n = p.q$, e 'd' é o inverso multiplicativo de $Y(mod[(p-1)(q-1)])$. Vale notar que segundo Abramo Hefez: "A congruência $aX \equiv 1\ mod\ m, com\ (a,m) = 1$, admite uma única solução módulo m. Esta solução será chamada de *inverso multiplicativo módulo m"* (Hefez, 2014, p. 248). Confirmando o caráter de mão única da função, além de não gerar duplicidade.

Portanto $dY \equiv 1\ (mod[(p-1)(q-1)]) \rightarrow 5d \equiv 1(mod[(5-1)(7-1)] \rightarrow 5d \equiv 1(mod\ \ 24)$, conclui-se $d = 5$, pois $5\ .\ 5 - 24 = 1$. Desta forma a expressão de desencriptação será $X^5 \equiv b(mod\ n)$, é importante salientar que nem sempre $Y = d$.

> Sobre a segurança dos dados com um N composto por dois fatores primos: O especialista em segurança Simson Garfinkel estima que um computador Intel Pentium de 100 Mhz, com 8 MB de RAM, levaria aproximadamente 50 anos para fatorar um número tão grande quanto 10^{130}. (...) Assim Garfinkel considerou o que aconteceria se cem milhões de microcomputadores (o número de máquinas vendidas em 1995) fossem interligados. O resultado é que um número tão grande quanto 10^{130} poderia ser fatorado em 15 segundos. Conseqüentemente, agora se aceita, de um modo geral, que para se obter uma segurança genuína é necessário suar números primos ainda maiores. Para importantes transações bancárias, N tende a ser em torno de 10^{308}(…). Os esforços combinados de cem milhões de microcomputadores levariam mais de mil anos para quebrar a cifra. (Singh, 2022, p. 303)

Isso nos mostra que para as situações mais gerais de segurança, para valores de p e q, grandes o suficiente, a RSA torna-se inquebrável, pois o conhecimento de fatoração de primos atual segue limitado. Em um momento futuro, se um método de encontrar e fatorar todos os números primos facilmente for encontrado, a cifra RSA tornar-se-á superada.

6.2 Uso da Análise Combinatória na Mensuração de Espaços Amostrais

I) Como são feitos os Ataques Criptográficos atuais

A criptoanálise segue evoluindo, e ainda que a Cifra RSA ofereça uma segurança ainda inquebrável, outras criptografias continuam sendo usadas, e programas de Criptoanálise são usados para fins diversos, esses programas automatizam os três principais métodos de Ataques Criptográficos: Ataque de Dicionário; Ataque Híbrido e Ataque de Força Bruta.

O Ataque de Dicionário, aplica sobre a senha criptografada uma sequência de palavras consultadas de bases de dados de Dicionários, inclusive com algoritmos voltados para situações

específicas como Dicionários Econômicos, Hospitalares e Educacionais, de modo que sabendo o contexto da pessoa que criptografou a informação ou criou a senha é possível quebrar o código. O sucesso desse ataque se deve aos padrões de comportamento e pouca criteriosidade de seus criadores, como apontam Silva & Steins sobre sua eficácia: “Ataques de dicionário decifram, em média, 25% de todas as senhas e levam apenas alguns segundos.” (Silva ;Stein, 2007, p. 49) Portanto eliminando ¼ do trabalho de modo rápido.

O segundo ataque, o Híbrido, é uma ramificação do ataque de dicionário, trabalhando com as palavras dos dicionários com ligeiras modificações que os usuários poderiam fazer, incluindo substituições de letras por símbolos ou números mais comuns como a troca de ‘a’ por ‘@’, ‘S’ por ‘$’, entre outras. Como detalha Silva & Stein:

> (...) por exemplo, substituindo números por letras visualmente similares, adicionando dígitos ao fim da senha, digitando a palavra de trás para frente, e assim por diante (por exemplo, se a senha escolhida for "salada", a letra "l" minúscula poderia ser substituída pelo número "1" e a letra "S", pelo símbolo "$", gerando então "$a1ada"). (Silva; Stein, 2007, p. 49)

Portanto senhas baseadas em palavras comuns, com sentido, ainda que levemente alteradas, são um alvo fácil para programas que realizem este tipo de ataque, contudo esta alteração em alguns caracteres das palavras leva mais tempo para ser descriptografada, sendo mais vantajosa em relação as palavras sem alteração.

O terceiro ataque, já foi abordado ao longo deste trabalho que é o Ataque de Força Bruta, o método mais lento, onde neste contexto, um programa testa todas as combinações de senha possíveis, para exemplificar Silva & Stein citando Brostoff apontam: “por exemplo, decifrar uma senha de oito caracteres, com ao menos uma letra maiúscula, uma minúscula e um número, levaria em torno de 6354 horas” (Silva; Stein, 2007, p. 50)

II) Analisando Senhas de 8 Dígitos

Analisando somente as combinações possíveis do exemplo da seção anterior, contendo 8 caracteres seguindo as especificações: pelo menos uma letra maiúscula, uma minúscula e um número. Existem 1008 formas de dispor um código nesse formato, resultado obtido pelo produto $3! \times C_8^3 = 336$, que é a disposição dos 3 caracteres obrigatórios, observando-se que ordem entre os obrigatórios deve ser contada. A isso deve ser multiplicado a Combinação Completa $CR_3^5 = C_{3+5-1}^5 = C_7^5 = 21$, que são as possíveis disposições dos demais caracteres

entre os 3 grupos (Letras Maiúsculas, Minúsculas e Dígitos) dados no problema. Isto foi apenas as disposições, tomando apenas um entre os 7056 exemplos, tomando X para representar letras maiúsculas, Y para as minúsculas e Z para os números.

Uma senha com a disposição XYZZZXYZ, dispostos exatamente nessa ordem terá um total de: $26 \times 26 \times 10 \times 10 \times 10 \times 26 \times 26 \times 10 = 456.976.000$ senhas possíveis, retomando ser essa uma de 1008 configurações disponíveis. Portanto a variação de caracteres, uso de números, conjuntos de letras desconexas e algumas maiúsculas torna o trabalho de criptoanálise (ou ataque de hackers) mais difícil e demorado.

Generalizando o Espaço Amostral das Senhas de 8 Dígitos: Considerando que o menor entre esses espaços é a senha numérica ZZZZZZZZ e o maior é a composta apenas por maiúsculas/minúsculas, dada as 1008 configurações possíveis entre os 3 tipos de caracteres, o espaço amostral P (quantidade de senhas possíveis) para uma senha qualquer escolhida entre essas será: $10^8 < P < 26^8 \rightarrow 100.000.000 < P < 26^8$.

Dessa forma é notável como a utilização de diferentes configurações de caracteres amplia o espaço amostral possível, tornando senhas mais seguras a ataques criptográficos. De modo geral existem 94^8 senhas possíveis utilizando os caracteres digitáveis do ASCII.

III) Estudo de caso aplicando Combinação Simples e Completa

Uma determinada senha de 8 caracteres precisa ser constituída com as seguintes configurações: Ter obrigatoriamente 1 dígito, 1 letra minúscula, 1 letra maiúscula, 1 caractere especial, os demais 4 caracteres podem ser escolhidos livremente, todavia, repetições não serão permitidas.

Etapa 01 – Analisando os 4 dígitos exigidos inicialmente

1 Dígito – 10 possibilidades, podendo ocupar qualquer uma das oito posições - $10 \times C_{8,1} = 80$;

1 Letra Minúscula – 26 possibilidades, podendo ocupar qualquer uma das sete posições restantes - $26 \times C_{7,1} = 182$ possibilidades;

1 Letra Maiúscula – 26 possibilidades, podendo ocupar qualquer uma das seis posições restantes - $26 \times C_{6,1} = 156$ possibilidades;

1 Caractere Especial – 32 possibilidades (entre os caracteres digitáveis, excluído o espaço), podendo ocupar uma das cinco posições restantes - $32 \times C_{5,1} = 160$;

Etapa 02 – Aplicação da Combinação Completa

Como as demais posições são de livre escolha, qualquer um dos 90 caracteres digitáveis restantes pode ser usado, inclusive apenas um tipo de caractere, de tal modo que temos:

$$x_1 + x_2 + x_3 + \cdots + x_{90} = 4 \rightarrow C_{4+90-1,\ 4} = C_{93,4} = 2.919.735$$

Como a ordem desses 4 caracteres altera a senha vamos multiplicar o resultado por 4!, desse modo as permutações entre os 4 caracteres serão contadas.

$$2.919.735 \times 4! = 3612280 \times 24 = 70.073.640$$

Etapa 03 – Retirando as repetições das escolhas dos 4 caracteres livres

Caso 01) 4 repetições de um único caractere → $C_{4,4} \times 90 \times 1 \times 1 \times 1 = 90$;

Caso 02) 3 repetições de um algarismo = $C_{4,3} \times 90 \times 1 \times 1 \times C_{1,1} \times 89 = 32.040$;

Caso 03) 2 repetições de um algarismo + 2 repetições de um outro algarismo =

$C_{4,2} \times 90 \times 1 \times C_{2,2} \times 89 \times 1 = 48.060$;

Caso 04) 2 repetições de um algarismo + dois algarismos distintos entre si

$C_{4,2} \times 90 \times 1 \times C_{2,1} \times 89 \times C_{1,1} \times 88 = 8.458.560$;

Tem-se então um total de $90 + 32040 + 48060 + 8458560 = 8.538.750$ exceções

Etapa 04 – Mensuração do Espaço Amostral

De tal modo, com as Regras definidas inicialmente, teremos:

$$80 \times 182 \times 156 \times 160 \times (70.073.640 - 8.538.750) \approx 2{,}2362862 \times 10^{16}$$

combinações possíveis ou 22.362.862.000.000.000.

Este padrão de senha é recorrente em senhas de aplicativos bancários, redes sociais entre outros, e a quantidade de senhas possíveis dele, mostra quão superior é a sua segurança em relação a senhas que usam apenas um tipo ou dois de caracteres.

IV) Senhas Numéricas

São comumente usadas para senhas de cartões Bancários, de Crédito entre outros, perfis de computadores pessoais, além de alguns aplicativos. Cada um digito da senha/código tem 10

possibilidades de acesso, assim cada senha de n algarismos tem um total $P = 10^n$ possíveis senhas. Se o padrão da senha for de *n* algarismos diferentes temos $P = n!$ senhas. Contudo a exigência de algarismos distintos limita a escolha da senha, pois existem apenas 10 algarismos para cada casa de um número de base 10, portanto só é possível gerar senhas de até 10 caracteres com essa restrição.

Estatisticamente uma senha de 10 caracteres distintos representa apenas aproximadamente 3,63% $\left(\frac{10!}{10^{10}}\right)$ das possíveis senhas do que quanto não existe essa restrição de serem apenas números diferentes. Portanto um ataque criptográfico sobre uma senha, sabendo que existe a restrição de algarismos distintos será aproximadamente 33 vezes mais rápido. Sobre o uso de números (chamados pelo autor de dígitos) em senhas, Roccia acrescenta: "*é possível observar a presença de dígitos em senhas de todo tipo de força, mas principalmente nas mais fortes, mesmo sendo o tipo de caractere com menos entropia. Apesar de comum, o uso de dígitos ajuda quando não é feito de forma previsível"* (Roccia, 2021, p. 18)

V) Senhas Alfabéticas e Alfanuméricas

Senhas de e-mails, documentos pessoais, códigos, palavras-chave de acesso podem usar senhas alfabéticas. Seguindo o mesmo parâmetro usado nas senhas numéricas, considerando que o alfabeto é composto por 26 letras existem $P = 26^n$ senhas possíveis para n códigos, se houver restrição das letras serem diferentes a senha fica restrita até 26 caracteres, o que é um número substancial considerando que a quantidade de caracteres que são usados em senhas fica comumente entre 6 a 12 caracteres, considerando a restrição a senha terá $P = 26!$ senhas possíveis para 26 caracteres, representando aproximadamente 0,000000006% $\left(\frac{26!}{26^{26}}\right)$ das senhas possíveis comparado a todas as letras diferentes.

Para o caso da senha admitir letras maiúsculas deverá ser considerado um alfabeto de 52 letras, 26 maiúsculas e 26 minúsculas havendo $P = 52^n$ senhas possíveis, analogamente se a senha for Alfanumérica já considerando as letras maiúsculas teremos o total de $P = 62^n$ senhas distintas. Na tabela abaixo será comparado a quantidade de senhas possível, e por conseguinte a segurança, analisando senhas 4, 6 e 8 caracteres, considerando senhas onde podem haver repetições, os valores em notação científica foram aproximados:

Tabela 5 - Quantidades de senhas possíveis conforme caracteres usados.

	Quantidade de Senhas Possíveis por tipo			
Tamanho da Senha	Numérica $P = 10^n$	Alfabética $P = 26^n$	Alfabética (com maiúsculas) $P = 52^n$	Alfanumérica (com maiúsculas) $P = 62^n$
4 caracteres	1.000	456.976	7.311.616	14.776.336
6 caracteres	100.000	308.915.776	$1{,}977 \times 10^{10}$	$5{,}68 \times 10^{10}$
8 caracteres	10.000.000	$2{,}088 \times 10^{11}$	$5{,}346 \times 10^{13}$	$2{,}183 \times 10^{14}$

Fonte: Elaborada pelo autor

A força da senha contra um ataque criptográfico, como explanado anteriormente, varia positivamente quanto maior o número de senhas possíveis, o que justifica que com o avanço da tecnologia novos caracteres foram sendo acrescentados as senhas, como mostrado na tabela acima. A senha alfanumérica traz aproximadamente 14776 vezes mais resultados possíveis em detrimento da senha numérica, isso para o caso de senha de 4 caracteres, quanto maior a senha, maior será a distância entre o espaço amostral de ambas, considerando que a função de contagem é exponencial.

VI) Senhas Alfanuméricas com Caracteres Especiais

Um dos padrões internacionais de caracteres mais usados É a tabela ASCII (American Standard Code for Information Interchange) usado na maior parte dos computadores. Esta tabela ASCII original possui 120 caracteres, que estão nos códigos de 0 a 127, contudo dentre eles temos somente 95 digitáveis, estes compreendidos entre letras (26 maiúsculas e 26 minúsculas, 10 números e 33 símbolos). Desta forma uma senha de 8 caracteres com critério de segurança que exija ao menos uma letra maiúscula, uma minúscula, um número e um caractere terá: $C_8^4 \times CR_4^4 = C_8^4 \times C_{4+4-1}^4 = C_8^4 \times C_7^4 = 70 \times 35 = 2450$, modos diferentes de usar os tipos de caracteres exigidos. Com um total P de possíveis senhas entre: $(10^8)^{2.450} < P < (26^8)^{2.450} \rightarrow \mathbf{10^{19.600} < P < 26^{19.600}}$, respeitando os critérios dados.

Sobre as senhas de 6 caracteres temos Roccia apresenta:

> Mais amplamente utilizado, a senha ou palavra-chave consiste num identificador composto por uma sequência de caracteres . Levando em conta letras minúsculas, maiúsculas e dígitos, existem 56.800.235.584 possibilidades para uma senha padrão de 6 caracteres. Esse número aumenta para 735.091.890.625 se contar com todos os 95 caracteres imprimíveis ASCII. (Roccia, 2021, p. 3)

Existe também a versão estendida dessa tabela, que acrescenta acentuação em letras e outros símbolos, chamada Tabela ASCII estendida que acrescenta mais 126 caracteres digitáveis, entre letras acentuadas e outros símbolos, contudo a ASCII original é mais usada como padrão para a criação de senhas. (Lima, 2006)

Desta forma com o uso dos Caracteres Mais comuns do teclado do Smartphone temos um total de senhas possíveis $P = 95^n$ para n caracteres para o caso de livre escolha de cada dígito. O Caractere ‘espaço’ (Space em inglês) embora digitavel, não é um caractere válido na criação de senhas, considerando que não é permitido comumente nos sites e aplicativos como senha, portanto as senhas possíveis ficam com $P = 94^n$.

7 APLICAÇÃO EM SALA DE AULA – A SEQUÊNCIA DIDÁTICA

A Sequência Didática, constitui uma oportunidade de ensino, num planejamento de curto/médio prazo, visa um encadeamento dos conteúdos gradual. O que valoriza o ensino de novos conteúdos/habilidades, de modo que antes de apresentar a Aritmética Modular e a Análise Combinatória, será feito um processo de apropriação dos conceitos e procedimentos que tangem a Criptografia de modo que a inserção de novos Objetos seja gradual seguindo dos mais simples aos mais complexos como afirma Zabala:

> Para que a ação educativa resulte no maior benefício possível, é necessário que as atividades de ensino/aprendizagem se ajustem ao máximo a uma seqüência clara com uma ordem de atividades que siga um processo gradual. Esta consideração é visível nos conteúdos mais algorítmicos como, por exemplo, o cálculo, onde o processo de mais simples para mais complexo é uma constante. (Zabala, 2014, p. 108.)

7.1 Sequência Didática – Segurança Digital e Análise Combinatória

Como apontado anteriormente, o processo de memorização de senhas, por parte do usuário é falho, proporcionalmente direto em relação ao quanto maior a quantidade de caracteres das senhas, bem como, a quantidade de senhas utilizadas, e mais diversos os caracteres usados. Esses são fatores que contribuem para que a informação da senha seja perdida na memória. Outro risco ao usuário é o armazenamento da senha em banco de dados digitais em texto plano (literal, sem nenhuma forma de criptografia), o que diante de uma invasão de sistema pode entregar de modo irrestrito os acessos aos dados como afirma Roccia:

> Uma importante etapa da autenticação por senha é o modo como ela será armazenada. Um método simples consiste em guardar a senha do usuário em texto plano no banco de dados. Porém, se algum agente malicioso conseguir acesso a essas informações, todas as senhas serão expostas, e a privacidade dos usuários será comprometida. Uma alternativa é criptografar a senha antes de armazená-la. Assim, mesmo que ocorra um vazamento de dados, as senhas estarão protegidas. Porém, é possível descriptografar essas senhas, ainda mais se a chave da criptografia também for comprometida. (ROCCIA, 2021, p. 4-5)

Portanto é necessária uma educação para a Segurança Digital, para criação de hábitos que reforcem a segurança do sujeito dentro da Era da Informação. Silva & Stein, 2007, também coadunam que: “Especificamente no caso de códigos secretos, ou senhas, é importante que sejam mantidos em segredo, uma vez que protegem informações confidenciais. Algumas senhas ainda devem ser periodicamente alteradas.” (Silva; Stein, 2007, p. 47)

Para facilitar o processo de geração de senhas aplicado a fins de potencializar o Ensino de Matemática para os estudantes do Ensino Médio é proposta neste trabalho uma abordagem que contemple:

1. Os aspectos de segurança recomendáveis na criação de senhas: unindo a necessidade de caracteres diversos que fiquem relativamente protegidos contra Ataques de Dicionários e Híbrido, e senhas que fujam dos padrões viciosos facilmente identificáveis abordados em Ataques de Força Bruta, aliando também a necessidade de memorização, com senhas que façam algum sentido para o usuário.

2. Introdução ao Contexto Histórico-Prático da Criptografia, para que o estudante entenda como são protegidas as informações atualmente e o contexto histórico que possibilitou tais métodos de segurança.

3. A perspectiva das tendências de ensino Matemático abordadas nos capítulos iniciais, que unam aspectos comuns as profissões, tecnologias, necessidades sociais e anseios do estudante ao ensino de matemática.

4. A aplicação de conteúdo do ensino de matemática de forma significativa que reforce o aprendizado numa perspectiva aplicada e diferenciada, para esta sequência especificamente a Análise Combinatória, Funções Afim, subsidiadas por aplicações na Aritmética Modular.

A Sequência está dividida em três partes: 1) Introdução a Criptografia e Códigos; 2) Aplicações da Função Afim para a Criptografia; 3) Avaliando segurança de Senhas com a Análise Combinatória, cada subseção dentro das sequências é uma atividade distinta. Deste modo, o estudante do Ensino Médio do 2º Ano, público-alvo da sequência, parte de uma Questão-Problema desafiadora que é: “Como se proteger digitalmente?”, onde seguindo a metodologia de Resolução de Problemas e Investigação Matemática, os conteúdos matemáticos surgirão como propostas de solução para a questão problema e a Criptografia virá como contexto.

As Aplicações da Teoria Semiótica tanto de Tratamento quanto de Conversão são usadas com a Criptografia, dentro dos tratamentos realizados na função afim, bem como as conversões ocorridas dentro da Criptografia RSA através da Aritmética Modular, assim como nas conversões entre linguagens textuais, gráficas, algoritmos, tabelas entre outros, onde o foco é que o aprendizado se fixe com o estudante representando as informações através dos diferentes Sistemas de Registro Semiótico apresentados, também nas mensurações de espaços

amostrais de senhas onde as informações são transformadas de problemas de linguagem escrita para equações algébricas.

7.2. Introdução à Criptografia e Códigos – Sequência 1

As atividades serão dadas em sequência para os alunos, sem que saibam qual será a atividade subsequente, a intenção é que ao final desta Sequência Didática eles percebam que se o código utilizado for muito simples, será facilmente quebrado. Será noticiado que ao final das Quatro Etapas de Atividade, a equipe que melhor atender as recomendações de cada atividade será premiada, o prêmio virá como motivação, contudo ao final todos os alunos serão premiados, em menor ou maior grau, informação que não será dada inicialmente.

7.2.1 Jogo dos Códigos

Objetivo: Introduzir o Contexto da Criptografia e Segurança Digital, contextos de Cifras de Substituição e Transposição, fazer o levantamento dos conhecimentos prévios dos estudantes, orientar os estudantes a construção de códigos para uma participação ativa.

1) Inicialmente será feita uma apresentação do contexto da necessidade do uso de senhas, com aspectos históricos da Criptografia e de como ela funciona.

2) Questionamentos serão feitos acerca os conhecimentos prévios que os sujeitos trazem, incentivando a pesquisa e a memória de temas como espionagem e o valor de informações secretas.

3) O Professor escreverá seu nome no quadro utilizando uma cifra de substituição, e pedirá que os alunos tentem decifrar. Exemplo: Numa cifra que divida o alfabeto em duas linhas, em que as letras da linha superior sejam trocadas pelas da inferior, e o mesmo com as da segunda linha teremos “Professor” = “Cebsrffbe”.

Quadro 5 - Alfabeto dividido em duas linhas

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

Fonte: Elaborado pelo autor

4) Proposição de um trabalho de Decifragem do verso abaixo, a informação que os estudantes terão será apenas as substituições feitas no nome do professor para que identifiquem o padrão utilizado, assim terão apenas partes da informação de um código.

Texto Original	Texto Criptografado
“Meus olhos te ofereço:	“Zrhf byubf gr bsrerpb:
espelho para a face	Rfcryub cnen n snpr
que terás, no meu verso,	Dhr grenf, ab zrh irefb
quando, depois que passes.”	Dhnaqb, qrcbvf dhr cnffrf
jamais ninguém te esqueça.”	Wnznvf avathrz gr rfdhrpn.”

(Cecília Meireles – Primeiro Poema da Rosa)

5) Revelação da criptografia usada na cifra, sendo possível a mesma seja descoberta pelos alunos antes, apenas com as informações da substituição da palavra ‘professor’.

6) Exemplificar as Cifras de Transposição e de Substituição no Slide para que os alunos tenham exemplos de como criar seus códigos, sendo Cifra de Transposição aquela que embaralha as letras gerando Anagramas e a Cifra de Substituição nessa as letras serão substituídas por outras seguindo alguma regra ou critério específico.

7) Proposta do Trabalho em Equipe: A turma será dividida em 5 grupos, o que resulta em grupos de no máximo 8 participantes cada, considerando turmas de até 40 alunos. Cada grupo deverá criar um código, seja de substituição de algumas letras, seja codificando algumas palavras, ou emogis, ou caracteres presentes no teclado do Whatsapp, para que possam se comunicar entre si por meio do Whatsapp, dessa forma terão que utilizar caracteres disponíveis no teclado do aplicativo, na perspectiva de que apenas os integrantes do grupo compreendam o teor da mensagem, os caracteres disponíveis serão expostos em Slide para que os estudantes possam se embasar.

8) Orientações a serem ressaltadas: Na criação do código e sua comunicação, não podem ser utilizadas imagens e palavras de conotação sexual, nem qualquer forma de diálogo discriminatório, seja racial, étnico, de gênero ou outros.

9) AVALIAÇÃO: Para avaliação dessa atividade, o professor deverá ser incluído em cada grupo de Whatsapp criado para o registro dos diálogos, de modo a avaliar se a comunicação está de fato acontecendo, se os alunos estão conseguindo criptografar suas

mensagens e desencriptar os textos dos colegas. Os estudantes deverão redigir um Relatório sobre o código criado, apontando as motivações para as escolhas da criptografia usada, bem como um glossário, para que seja possível ao leitor, não criador do código, desencriptar uma mensagem por ele utilizada.

Exemplo de Código, possível com Emogis:

Quadro 6 - Exemplo de possível alfabeto codificado

😀=A	😘=B	😳=C	🍀=D	🦁=E	😘=F	😔=G	🙃=H	😊=I
😌=J	🦋=K	🐭=L	😈=M	🤑=N	😪=O	😬=P	🤓=Q	😎=R
👺=S	😤=T	👻=U	❤️=V	☠️=W	🌞=X	🌈=Y	🧸=Z	

Fonte: Elaborado pelo autor

Exemplo de Mensagem utilizando o código:

🤑😀😪 👺🦁 😬😪🍀🦁 😔😊👺😀😎 🍀👻😀👺 ❤️🦁🧸🦁👺 🤑😪 🤩🦁👺🤩😪 😎😊😪

Mensagem decodificada: "Não se pode pisar duas vezes no mesmo rio" – de autoria do filósofo Heráclito, natural de Éfeso em 540 a.c.

7.2.2 Teste do Código

Objetivo: Incentivar o trabalho em Equipe, fortalecer o conceito intuitivo de Cifra de Substituição, promover a tomada de decisões eficientes de segurança.

1) Cada turma será organizada nas mesmas equipes formadas na atividade anterior.

2) Os integrantes da Equipe terão conversas, via grupo de Whatsapp (onde o professor estará presente em cada grupo) utilizando o código criado na Atividade 01.

3) Os estudantes avaliarão se conseguem manter comunicação com o código criado, do contrário deverão reformulá-lo e revisar o Relatório Entregue ao professor. O que comum na criação dos códigos ao longo da história, que alguns sejam deixados de lado por sua falta de praticidade.

4) A avaliação da atividade será feita analisando a reformulação entre o primeiro e o segundo relatório, quanto melhor ficar em detrimento do primeiro, melhor será o nível do entendimento do grupo acerca da atividade, como todos deverão se comunicar no código dentro do grupo de Whatsapp, esta atividade proporciona um olhar individualizado sobre o uso do código por parte de cada estudante.

7.2.3 Codificando uma Mensagem

O objetivo dessa atividade é o trabalho em código com mensagens mais longas.

1) Os estudantes, nos grupo, serão orientados a criar uma mensagem codificada.

2) A mensagem deverá ser revisada em termos de concordância, evitar ‘estrangeirismos’, e ser constituída por palavras presentes no dicionário da língua portuguesa.

3) Essa mensagem será publicizada num grupo de Whatsapp geral, onde estão os demais colegas participantes das outras equipes.

4) A atividade será avaliada em questão de concordância com o próprio Glossário apresentado. Se houve assertividade em criptografar a mensagem utilizando o código criado pela equipe.

7.2.4 Ataques Criptográficos

Objetivo: Simular um Ataque Criptográfico de Força Bruta, para que o estudante perceba como uma simples camada de criptografia torna a informação muito mais segura.

1) As mesmas equipes anteriores tentarão decifrar as mensagens que as demais equipes publicizaram no grupo geral do Whatsapp, cada equipe tentará compreender a mensagem criptografada das outras equipes.

2) Haverá uma premiação simbólica para a Equipe que melhor compreender as mensagens criptografadas, cada equipe deverá entregar escrito a possível tradução de cada mensagem criptografada das outras equipes. Contudo, todas as equipes serão premiadas.

3) Diálogo com os estudantes usando a temática da espionagem e alguns fatos históricos sobre quebras de Criptografias, acerca das possíveis consequências de vazamentos de informações confidenciais.

4) Avaliação: Os estudantes percebam que códigos muito simples não representam grande segurança criptográfica, porém por mais simples que seja, exige um esforço do invasor para obtê-lo. Os diálogos produzidos no momento serão importantes para mensurar o entendimento da atividade. A avaliação da atividade também será feita recolhendo as traduções feitas por cada equipe e avaliando a qualidade da compreensão da importância da Criptografia no momento de discussão.

7.3 Como se comunicar secretamente - Sequência 2

7.3.1 A Cifra de César como Função Afim

Inicialmente questionar aos alunos quem foi César, questionando-os sobre os famosos "Césares" da história romana e pedindo que pesquisem qual César teria sido o criador da cifra. Com o uso dos Disco de Cifras impressos, adaptação do invento de Leon Albert, arquiteto italiano que automatizou a Cifra de César e amplificou seu uso.

Pedir que os alunos cifrem a frase de J.R.R. Tolkien: "Ações não valerão menos porque não foram elogiadas" utilizando a cifra original de César, que era o deslocamento das letras de 3 casas para a direita, deve ficar "Dgrhp qdr ydohudr jhqrp srutxh qdr irudp hormldgdv". Observar se conseguem utilizar corretamente a cifra.

Em seguida processo de Generalização partindo do problema: "Seria possível transformar a Cifra de César em número? Como?", após as sugestões dadas para os alunos construir um modelo em quadro. Este modelo trará dois novos problemas, que serão abordados com enfoque na Investigação Matemática:

Problema 01) Será necessário transformar as letras em números para que a função funcione (o que poderá ser organizado em tabela como no exemplo abaixo):

Problema 02) Frequentemente haverão resultados maiores do que 26, o que fazer? As soluções virão em numerar as letras de 0 a 25, e usar o algoritmo da Divisão de Euclides para que a resposta seja o resto, algoritmo esse que servirá de pré-requisito para a atividade seguinte onde será introduzida a Função Aritmética Modular, que virá solucionar de modo mais eficiente

os dois problemas levantados. Possivelmente os estudantes darão a perspectiva de se reiniciar a contagem, o que poderá será trabalhado de modo investigativo em sala.

Para Subsidiar a Experiência os alunos receberão dois círculos de Papel que funcionarão como o disco de César, mas, também será disponibilizado um app para Smarthphone que cumpre a função, Caesar Cipher Disk. Será avaliado os modelos apresentados pelos estudantes com possíveis soluções para cifrar alfabetos com funções.

7.3.2 Função de Aritmética Modular

Aula expositiva sobre a Divisão de Euclides, em seguida abordando a Função da Aritmética Modular sob a nomenclatura de Função Resto.

Mostrar que: equivale $\begin{array}{c|c} D & d \\ r & q \end{array}$ a $\boldsymbol{D = d \times q + r.}$

Em seguida mostrando a função resto: $D\ (resto\ d) = r$, onde resto de D na divisão por d é r. Para posteriormente apresentar a expressão $D \equiv r(mod\ d)$.

Apresentar, em slide desenho, de relógio, fazendo a analogia com o caráter cíclico da aritmética modular, comprando-a com a "função relógio". Propor diálogo com os alunos questionando como esse novo conhecimento pode ajudar na solução dos problemas da atividade anterior, no problema de números maiores que 26. A avaliação será a participação dos estudantes e contribuições de possíveis usos da Aritmética Modular.

7.3.3 Unindo Funções Afins e Aritmética Modular

Mostrar o modelo da cifra de césar na função afim, $f(x) = x + 3$, abordando que a bijetividade da função afim é um fator importante para sua aplicação criptográfica, e para o caso específico da aritmética modular, as funções afim com coeficiente angular 1 ou -1, pois sua inversa sempre gera imagens inteiras, já que na aritmética modular se trabalha apenas com os números inteiros.

Por seguinte dividir os alunos nas mesmas 5 equipes da atividade anterior, e propor que eles se comuniquem no Grupo de WhatsApp utilizando o modelo da Cifra de César, porém com um deslocamento diferente de 3. Dizendo inclusive que eles podem usar deslocamentos

negativos e explanando como caso surja o questionamento. Antes do início da atividade os alunos serão informados que um print do diálogo deverá ser compartilhado no Grupo Geral para que os colegas tentem decifrar a conversa num Ataque Criptográfico de Força Bruta em Equipe.

Avaliação será o uso correto da Cifra de César nos diálogos do grupo, percebendo se há uma comunicação efetiva, bem como se os colegas conseguem desencriptar os prints de Conversas dos outros grupos, nessa atividade se espera um maior número de desencriptações corretas, considerando que todos conhecem o tipo da criptografia usada, após essa etapa promover um diálogo para que os estudantes expressem o porquê essa quebra de código foi mais simples que a anterior e ilustrar esse fato com Fatos Históricos do Contexto da Criptografia.

Ao fim do processo de Desencriptação, abordar o conceito matemático de Função Inversa, reforçado pelo caráter da Bijeção de Uma Função Afim, em que o aluno deverá perceber que apenas as funções inversas de Coeficiente Angular 1 e de Coeficientes Lineares (constante) inteiros estão aptas ao uso na aritmética modular, pois este tipo de função só admite resultados inteiros.

7.3.4 Contextualização sobre a criptografia contemporânea

Dialogar com os alunos questionando as atuais criptografias usadas, e como elas estão relacionadas com a Aritmética Modular que eles estavam usando, contudo aplicada aos números primos, falar sobre a história da Criptografia RSA. Demonstrar o funcionamento da RSA, seu processo de encriptação e desencriptação, expondo sua forte base na Aritmética dos Números Primos.

Fazer a demonstração do funcionamento da Criptografia RSA, através do exemplo do Diálogo de Alice e Bob, supracitado na seção sobre essa criptografia e que faz parte da literatura clássica do tema. Em seguida dividir os estudantes em 3 grupos, para desenvolverem o próprio modelo de Criptografia RSA para que dois dialoguem enquanto um terceiro tenta interceptar as mensagens. Pedir que as conversas sejam textos curtos e rápidos, dada a demanda de tempo maior que o uso dessa criptografia num modo analógico tem.

7.4 O Que é uma senha forte? – Sequência 03

Nesta parte da Sequência são abordadas as escolhas possíveis que vários tipos de senha permitem, com a Análise Combinatória sendo o instrumento de contagem de escolhas.

7.4.1 O Padrão de Caracteres ASC-II e Combinação Completa

Expor ao estudante, por meio de slides, este padrão internacional de caracteres ASCII, no sentido de subsidiar informações acerca do universo de escolhas de caracteres possíveis.

Para apresentar a combinação completa será utilizada o problema: Como distribuir 9 bombons, distintos entre si, em 4 caixas, podendo até 3 delas ficarem vazias. Espera-se que os estudantes criem alguns modelos utilizando Arranjos ou Combinação Simples, onde deverá ser exposto para eles a questão de que os 4 grupos (caixas) não estão bem definidos, como comumente acontece em problemas de Combinação Simples para a formação de x times com y indivíduos cada. Até esta atividade o PFC não havia sido introduzido de modo formal aos alunos, mas espera-se que as temáticas prévias os permitam intuir o seu cálculo.

Retomar com o estudante a Codificação dos 9 bombons usada anteriormente sob a forma de algoritmo $\boldsymbol{x_1\, x_2\, x_3 + x_4\, x_5 + x_6\, x_7\, x_8 + x_9 = 9,}$ transcendendo esse contexto para o uso de Caracteres distintos para a criação de senhas, semelhante ao Estudo de Caso de uma Senha de 8 Caracteres, abordado no capítulo de aplicações da Análise Combinatória, apresentando a Combinação Completa como solução para o contexto do problema.

Ao final os estudantes deverão calcular quantos Configurações de senhas podem ser construídos utilizando Maiúsculas, Minúsculas, Dígitos ou Caracteres Especiais, utilizando a Combinação Completa. E quantas senhas Com Repetição e Sem Repetição podem ser feitas, utilizando o Princípio Fundamental da Contagem. A avaliação dessa atividade é a absorção dos conteúdos apresentados através do cálculo e da argumentação coerente dos estudantes nas respostas, bem como suas dúvidas e participação em sala.

7.4.2 Uso da Análise Combinatória para determinar força de uma senha

Perguntar aos alunos, em que contextos de suas vidas são exigidas senhas, questionando onde são pedidas, com que frequência as usam, a quantidade de caracteres que têm cada senha, os tipos de caracteres usados. Explanar sobre alguns tipos de senhas que não tenham aparecido nas exposições da turma. Montar algumas senhas de 4, 6 e 8 dígitos na lousa, questionando a quantidade de decisões possíveis, tanto para a restrição de todos os caracteres serem distintos, quanto quando não houver essa restrição, deste modo o Princípio Multiplicativo da Contagem estará sendo explicado de modo indutivo através da Resolução de Problemas.

Abordar o problema da senha numérica de 8 caracteres em que a configuração é de uma data de aniversário, com a seguinte pergunta: “Quantas senhas possíveis podem ser feitas com datas de aniversário, considerando uma população de 0 a 100 anos? Qual a porcentagem relativa a uma senha de 8 dígitos sem restrições as senhas de data de aniversário representam?”

Abordar alguns vícios de senhas simples, como o de sequências, ou de caracteres repetidos, alternâncias, etc. A avaliação será feita através das possibilidades apresentadas pelos grupos, em seguida analisadas em sala de aula e se necessário respondidas pelo professor.

7.4.3 Ataques Criptográficos e seus tipos

Questionar aos alunos quais as técnicas que eles usaram para tentar decifrar a criptografia das mensagens colegas, explanar sobre os ataques criptográficos mais comuns, que são feitos por meio de softwares avançados: Ataque de Dicionário, Ataque Híbrido e Ataque de Força-Bruta. Sobre cada explanação pedir que os alunos desenvolvam tipos de senhas que possam evitar as ações específicas deles, e construam sua senha ideal. Analisar como as diferentes composições de caracteres aumentam ou diminuem a segurança segundo a análise combinatória.

A aula será avaliada através das senhas construídas pelos estudantes, se elas se encaixam em senhas resistente a cada um dos tipos de ataques abordados.

7.4.4 Avaliando senhas dentro dos padrões de segurança

Exposição de recomendações de órgãos de segurança digital sobre o uso de senhas, abordando uma senha de 8 caracteres, e a possibilidade de senhas possíveis utilizando as

recomendações abordadas, especialmente com o acréscimo de letras maiúsculas e caracteres especiais (também chamados de símbolos). Explicar a diferença entre *arranjo* e *combinação*, pois no universo de senhas, a mudança de posição de um caractere gera uma nova senha.

Pedir que os alunos criem um padrão de criação de senhas. Em que escolham quantas letras minúsculas, maiúsculas, dígitos e caracteres serão exigidos, será o objeto da avaliação. Eles deverão calcular quantas senhas possíveis existem no padrão que criaram. Aqui haverá uso da combinação completa.

7.4.5 Criando algoritmos de criação de senhas (Produto Final)

Os estudantes, nos mesmos 5 grupos, serão provocados à uma construção de uma tabela no *excel*, podendo também ser feita de modo analógica, em papel, a depender das disponibilidades de equipamentos da escola. Nessa tabela uma palavra-chave será adicionada e a mesma gera um conjunto de senhas dentro dos padrões de segurança através do uso das funções lineares dentro da aritmética modular, conferindo certa aleatoriedade a cada senha, sendo que a palavra-chave é inserida para mostrar as senhas e em seguida deletada, a única coisa a mostra serão os algoritmos de criação de cada senha, de modo que possam lembrar de várias senhas através de uma única palavra chave.

Um exemplo de uma possível tabela está abaixo, onde o estudante deve inserir uma palavra-geradora, no exemplo SUPERSTICAO (foi substituído o ‘ç’ por c e ignorada a acentuação, para fins didáticos, para que o estudante não trabalhasse com caracteres em excesso), essa palavra-geradora deverá ter significação para o estudante afim de facilitar sua memorização.

Para otimizar o trabalho será usado o aplicativo de planilhas eletrônicas Excel, dentro dele serão utilizadas as funções ‘Proc’ e ‘Mod’, a primeira cria um banco de dados onde caracteres são relacionados a números de uma lista, (conforme imagem abaixo na tabela Banco de Dados), onde a cada letra número e caractere será dada uma numeração na lista, a fim de que sua posição numérica possa ser usada nos cálculos, a função é digitada como “=PROC(Célula onde está o caracteres; Coluna dos Caracteres; Coluna dos Números relacionados a cada caractere)”, de modo que quando a Palavra-Geradora é digitada, esta será convertida em números.

A função “MOD” automatiza o cálculo da aritmética modular, digitada “=Mod(número; divisor)” assim a fórmula transforma o número em seu resto, numa divisão pelo divisor. Na tabela em questão esse número vem da lista com o qual o caractere é referenciado, que será transformado em um novo número por uma função afim dentro de uma função modular, no exemplo abaixo utilizou-se a função “MOD” no excel da forma: =MOD(CÉLULA DO CARACTERE *6+5;51), que equivale a $6x + 5(mod\ 51)$.

Para a tabela de banco de dados usadas com estudantes foram usados 51 caracteres (26 maiúsculas, 10 dígitos e 15 caracteres especiais, numerados de 0 a 50. O resultado do cálculo será um número de 0 a 50 que será relacionado novamente pela função “PROC” a um novo caractere, criando-se uma senha para utilizar nos mais distintos contextos.

Ressalta-se que a referida função do excel não faz distinção entre letras maiúsculas e minúsculas, motivo pelo qual se optou só por caracteres de letras maiúsculas na atividade, quando realizada de modo analógico essa dificuldade inexiste. Como mostrado na tabela abaixo o estudante através de uma única palavra-geradora poderá gerar inúmeras senhas, e para lembra-las basta re-inserir a palavra-geradora na tabela.

Tabela 6 - Exemplo de utilização tabela geradora de senhas

Palavra Geradora	S	U	P	E	R	S	T	I	C	A	O
Convertido em Número	18	20	15	4	17	18	19	8	2	0	14
Parâmetro 01	11	23	44	29	5	11	17	2	17	5	38
Senha 01	L	Y	_	3	F	L	R	C	R	F	*
Convertido em Número	18	20	15	4	17	18	19	8	2	0	14
Parâmetro 02	16	30	46	20	9	16	23	48	6	43	39
Senha 02	Q	4	!	U	J	Q	Y	,	G	@	&
Convertido em Número	18	20	15	4	17	18	19	8	2	0	14
Parâmetro 01	11	23	44	29	5	11	17	2	17	5	38
Senha 03	L	Y	_	3	F	L	R	C	R	F	*

Fonte: Elaborada pelo autor

A intenção é que diante do aprendido sobre as fraquezas humanas da criptografia, o usuário possa confiar na memória apenas uma informação significativa para ele, que gere um conjunto de senha com caracteres “aleatórios”, que seria mais difícil de memorizar, após cada vez que a tabela for utilizada o estudante deverá apagar a palavra-geradora, de modo que um usuário mal intencionado que tenha acesso a tabela, não consiga descobrir as senhas do usuário por desconhecer sua palavra-geradora. Para aumentar a segurança da tabela pode ser protegida

por senha para acrescentar mais uma camada de criptografia, ou ter esse processo feito de modo analógico, através de uma folha impressa.

A avaliação dessa atividade é se o estudante conseguiu construir a tabela unindo as funções afim com a aritmética modular, e se ao se deparar com as novas senhas ele consegue avaliar se houve um aumento de segurança, por meio da análise combinatória em detrimento de um uso da palavra-geradora como senha.

Ao final da aplicação das sequências, espera-se que o estudante desenvolva maior consciência sobre a segurança digital, adquira conhecimento básico sobre o mundo da criptografia, use de maneira satisfatória a função afim e perceba o raciocínio e utilidade por trás da análise combinatória especialmente aplicando o princípio fundamental da contagem.

7.5 Observações do professor-pesquisador

Essa sequência foi aplicada em uma escola pública da rede estadual de educação da Bahia, para duas turmas de 2º Ano do Ensino Médio, num contexto de Escola de Educação em tempo integral, em que a quantidade de aulas de matemáticas semanais eram 5, destas, 2 foram reservadas para o trabalho da Sequência, esta desenvolvida durante 10 aulas, anteriormente planejadas para 8, foram criadas ao todo 10 equipes de estudantes, 5 em cada uma das 2 turmas trabalhadas.

Sugere-se que a aplicação da sequência seja distribuída da seguinte forma:

Parte 1 da Sequência: I) Introdução à criptografia e códigos + Jogo dos Códigos (Criação) – 1 aula; II) Teste do Código – 1 aula; III) Codificar mensagens + Ataques criptográficos – 1 aula

Parte 2 da Sequência: IV) A cifra de césar como função afim - 1 aula; V) Função de Aritmética Modular - 1 aula; VI) Contextualização sobre a criptografia atual – 1 aula.

Parte 3 da Sequência: VII) o padrão de caracteres ASCII e combinação completa; VIII) uso da análise combinatória para determinar força de uma senha – 1 aula; XIX) ataque criptográfico e seus tipos + avaliando senhas dentro dos padrões de segurança – 1 aula; X) criando algoritmos de criação de senhas – 1 aula.

O uso do aplicativo de mensagens para a seção 6.2 da sequência proporcionou uma comunicação facilitada e mais rápida do que se utilizado papel para desenvolver os diálogos,

especialmente por que a maioria dos grupos desenvolveram seu código através de emogis (caracteres gráficos do aplicativo), o que só seria possível dentro daquele ambiente. alguns grupos escolheram para as atividades códigos tão complicados que precisaram ser reformulados, ocorreu em 3 equipes, entre elas, duas não se reformularam por considerar cansativo, estando de certo modo dispersos e desinteressados, parando assim a atividade, ainda que tenham sido orientados quanto a escolhas eficientes de código previamente e no decorrer da atividade.

No jogo de quebras de código os estudantes utilizaram as técnicas de análise de frequência, intuitivamente, através de palavras de 1, 2 ou 3 letras, três equipes conseguiram "quebrar o código" dos colegas com sucesso, esta atividade mostrou-se motivadora. houve casos de espionagem onde alguns estudantes observaram de longe informações dos escritos das outras equipes, diante disso aconteceu a contraespionagem, onde os códigos eram mudados, o que mostra a história da guerra entre criptoanalistas e criptógrafos, se repete sempre que existe alguém com a intenção de desvendar uma comunicação secreta e outra pessoa em mantê-la secreta.

As atividades sobre cifra de César e funções afim ocorreram sem dificuldades, e vieram a ser uma forma de recuperação de aprendizado, para alguns estudantes das equipes, visto que o conteúdo havia sido trabalhado no 1º ano do ensino médio, bem como 8º e 9º ano do ensino fundamental, assim oportunizou-se através da sequência a consolidação de um conteúdo já conhecido por alguns, e para outros uma nova oportunidade de aprendizado daquilo que não foi estabelecido anteriormente.

Esperava-se uma maior dificuldade de compreensão inicial dos estudantes acerca da Aritmética Modular, visto que não é um conteúdo abordado claramente no Ensino Médio, contudo a apresentação da mesma como 'função relógio', uma função de caráter cíclico, onde exemplos como marés, ciclo menstrual, estações do ano foram dados para contextualização permitindo melhor assimilação do uso da função. Também sua relação com a divisão euclidiana, permitiu que a compreensão da mesma acontecesse sem grandes percalços, por meio do entendimento do resto da divisão.

As atividades que envolveram análise combinatória, especialmente o princípio fundamental da contagem ocorreram sem muitas dificuldades. a forma intuitiva de calcular mostrada inicialmente, onde foi aplicada sem apresentação como fórmulas, trouxe mais naturalidade ao processo de aprendizagem, onde as fórmulas, quando inseridas, eram trazidas

dentro de um contexto com exemplos já previamente trabalhados. Percebeu-se um avanço no aprendizado deste conteúdo, bem como na habilidade da aplicação dele.

A combinação completa carregou certa dificuldade adicional para o processo abstração do conteúdo, contudo o aparato trazido pela semiótica em que o problema em texto era convertido em imagens, depois para o código estrelas-e-barras, por conseguinte apresentado na forma de algoritmo mostrou-se uma forma eficaz de apresentação do conteúdo, alguns estudantes pelas dificuldades crônicas de aprendizagem, carregadas até então, tiveram maior dificuldade, outros precisariam de um processo de recuperação de aprendizado para de fato desenvolverem as habilidades propostas, processo esse não contemplado nessa sequência. Porém de modo geral, a maioria da turma conseguiu assimilar o objeto combinação completa.

A abordagem da segurança digital e criptografia apresentada aos alunos se mostrou de fato motivadora, onde os estudantes trouxeram diversas contribuições de seus conhecimentos e experiências de segurança com aplicativos dos mais diversos tipos e usos. Os contextos históricos da criptografia, apresentados através de ilustrações, permitiram ao estudante entender a necessidade temporal de cada criptografia, e a dinâmica de avanço constante das medidas de proteção de informações sensíveis, após as aulas de contextos históricos alguns estudantes traziam informações advindas de pesquisas feitas em casa, que enriqueceram a sequência.

A criação da planilha eletrônica geradora de senhas, prevista para a Atividade 13 teve que ser adaptada para um formato analógico, folha impressa, devido a indisponibilidade de horários do laboratório de informática da escola, bem como a pouca quantidade de máquinas oferecida, contudo essa adaptação não trouxe prejuízos para a realização da atividade. Grande parte dos grupos conseguiu desenvolver a Tabela de modo satisfatório, convencidos da utilidade da mesma, bem como, bem sucedidos no uso das Funções Afim, Aritmética Modular e Análise Combinatória, necessárias às atividades.

Durante a aplicação da Sequência encontrou-se dificuldades nos fatores: tempo, clima, limitações tecnológicas. Embora as duas aulas de aplicação da sequência ocorressem de modo geminado, as diversidades dos graus de compreensão do aluno sobre a atividade (o que demandava explicações e atendimentos individualizados que necessitavam de um tempo maior), bem como, a dinamicidade da rotina de uma escola como atrasos de alunos, palestras não previstas, avaliações governamentais, entre outros, compuseram um desafio maior para a realização da sequência no tempo estabelecido.

O clima excessivamente quente, próprio de uma região do semiárido nos meses finais do ano, e a ausência de refrigeração adequada na escola proporcionou uma maior agitação e desconforto por parte dos estudantes, o que inevitavelmente afetava a aplicação da sequência. Por fim a dificuldade de acesso a recursos tecnológicos adequados, foi remediada com a contratação de um serviço de internet para possibilitar um wi-fi de qualidade para o uso do Whatsapp, além de não ter sido possível realizar as atividades em computadores, não havendo tempo hábil para um replanejamento envolvendo os smartphones.

8 CONSIDERAÇÕES FINAIS

Neste trabalho visou-se articular formas de aprendizagem da análise combinatória através de um eixo temático da segurança digital. Neste eixo, utilizou-se enfoque da criptografia, campo que se mostrou especialmente profícuo para aplicações dos mais diversos conteúdos, ainda que o principal objeto deste foi a sua aplicação da sequência didática com a análise combinatória. Encontraram-se também fatores positivos para sua aplicação com as funções afins.

O uso da teoria dos registros de representação semiótica, articulados aos objetos matemáticos, constituem um campo de exploração relevante visto que, para a teoria, o aprendizado ocorre na articulação entre dois ou mais tipos de registro, onde o professor amparado na teoria pode modificar o planejamento de suas aulas aderindo a esta abordagem.

Através dos objetos trabalhados, o objetivo de gerar uma consciência acerca da segurança digital foi visto como atingido, e a análise combinatória apresentou-se como um instrumento eficaz para contabilizar as possíveis senhas feitas em cada contexto, determinando o conjunto universo, o nível de segurança de uma senha, as mudanças positivas e negativas que algumas configurações de caracteres na escolha de senhas têm em detrimento de outras.

Trabalhar com a tabela geradora de senhas junto com o estudante permite a articulação dos conteúdos matemáticos elencados no trabalho: análise combinatória, aritmética modular, funções afins. Aplicados ao contexto da segurança Digital, entregando ao estudante um instrumento útil para sua proteção de dados confidenciais, mostrando a matemática como uma ferramenta imprescindível aos processos cotidianos de suas vidas.

O aprendizado combinado dos diferentes competências e habilidades da Base Nacional Comum Curricular (BNCC) especialmente no que tange a investigação matemática, articulação de conteúdos e especialmente na articulação entre Aritmética, Álgebra e Probabilidade e Estatística, também ao tratamento da informação. Os recursos digitais mostram-se imprescindíveis para a apresentação e aplicação de um contexto tão ligado com a tecnologia como a criptografia.

Não se retendo as dificuldades, percebeu-se o retorno dos estudantes na compreensão acerca dos objetos matemáticos abordados, que o princípio fundamental da contagem pode ser introduzido de modo intuitivo, livre de fórmulas favorecendo uma compreensão da Análise Combinatória menos engessada a algoritmos, todavia sem desprezá-los. Sabendo que a teoria semiótica é um apoio interessante, que vale o estudo para diversas aplicações matemáticas e que a criptografia é uma área matemática, que especialmente para conteúdos algébricos e

aritméticos, é polivalente podendo dinamizar o ensino, e aplicar diversas teorias matemáticas em vista de potencializar o aprendizado dos sujeitos. Para futuros trabalhos, é intenção deste pesquisador, aprofundar a pesquisa do uso da criptografia e aritmética para outras aplicações com funções, propriedades da potenciação e máximos divisores comuns.

REFERÊNCIAS

ALMEIDA, Helber Rangel Formiga Leite de. Das tecnologias às tecnologias digitais e seu uso na educação matemática. Presidente Prudente: Revista Nuances - estudos sobre Educação, v. 26, n. 2, p. 224-240, maio/ago. 2015

ALMEIDA, Pedro Quaresma de; PINHO, Augusto. Análise de Frequências da Língua Portuguesa. Portugal: Universidade de Coimbra, 2006.

BEZERRA, Marcos José da Silva. O ensino de análise combinatória para turmas da Educação de Jovens e Adultos com foco no princípio multiplicativo. Universidade Federal do Pará, 2021.

BRASIL, Banco Central. Relatório Integrado do Banco Central – 2022.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília: MEC, 2018

CAVALCANTI, Felipe Lima. Estratégias de Resoluções: problemas utilizando o Princípio Multiplicativo em Análise Combinatória. Universidade Federal do Pará, 2022.

CARNEIRO, Framilson José Ferreira. Criptografia e Teoria dos Números. Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

COUTINHO, S. C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2014.

DUVAL, Raymond. Registros de representação semiótica e funcionamento cognitivo do pensamento. Tradução revisada: Méricles Thadeu Moretti. UFSC, 2023

EVES, Howard. Introdução à história da matemática / Howard Eves; tradução Hygino H. Domingues. 5a ed. – Campinas, SP: Editora da Unicamp, 2011

HEFEZ, Abramo. Aritmética. Rio de Janeiro: SBM, 2014.

LAMONATO, Maíza & PASSOS, Carmem Lúcia Brancaglion. Discutindo resolução de problemas e exploração-investigação matemática: reflexões para o ensino de matemática. Campinas: Zetetiké – FE/Unicamp, V. 19, nº 36, 2011.

LIMA, Elon Lages. Números e Funções Reais - Coleção Profmat. Editora: SBM, 2012.

LIMA, Sandra Fernandes de Oliveira. Um Sistema para Transposição Automática de Seqüências MIDI baseada em Alcance Vocal. Universidade Federal de Uberlândia, 2006.

MORGADO, Augusto César & CARVALHO, Paulo Cezar Pinto. Matemática Discreta – Coleção Profmat. Editora: SBM, 2015.

PERETTI, Lisiane & COSTA, Gisele Maria Tonin da. Sequência Didática na Matemática. Instituto de Desenvolvimento Educacional do Alto Uruguai, Revista de Educação do Ideal. Vol. 8 – Nº 17 - Janeiro - Junho 2013

ROCCIA, Rubens Douglas. Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas. Universidade de São Paulo, 2021.

SCHEINERMAN, Edward. Matemática Discreta: uma introdução - tradução da 2a edição norte-americana. Tradução de All tasks. Cengage Learning Edições Ltda, 2011.

SILVA, Ana Lourdes Moreno Rodrigues. A criptografia como estimulo à aprendizagem matemática. Universidade Estadual do Sudoeste da Bahia, 2021

SILVA, Denise Ranghetti Pilar da Silva & STEIN Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. Porto Alegre: PUCRS, Revista Ciências & Cognição, 2007; Volume 10.

SILVEIRA, Everaldo & MIOLA, Rudinei José. Professor-pesquisador em educação matemática. Curitiba: Intersaberes, 2013.

SINGH, Simon. O Livro dos Códigos; tradução de Jorge Calife. 14ª Edição, Rio de Janeiro: Record, 2022.

SUN-TZU. A arte da guerra; tradução de Neury Lima. 3ª Edição, Barueri: Novo Século Editora Ltda.

ZABALA, Antoni. A prática educativa : como ensinar. tradução: Ernani F. da F. Rosa. Porto Alegre: Penso, 2014.

APÊNDICE A – ATIVIDADE 01: CRIAÇÃO DE CÓDIGO

PROFMAT	**Aplicação em Escola de Ensino Médio**	UESB
	Atividade 01 – Sequência Didática – Segurança Digital	
	Professor: Nathan Lopes **Componente Curricular:** Matemática — **Série**: 2º Ano	
Equipe: (01) (02) (03) (04) (05)	**Turma:** (A) (B)	

Glossário da Criação do Código

01) Resuma as suas escolhas para utilizar esse código. Descreva como usar ele, para que pessoas fora do grupo também utilizem.

_____

_____

_____

_____

_____

_____

_____

_____

02) Glossário. Tente reproduzir abaixo os caracteres usados e o que cada um significa

APÊNDICE B – ATIVIDADE 02: TESTE CÓDIGOS

PROFMAT	**Aplicação em Escola de Ensino Médio** **Atividade 02 – Sequência Didática – Segurança Digital**		UESB
	Professor: Nathan Lopes **Componente Curricular:** Matemática	**Série**: 2º Ano	
Equipe: (01) (02) (03) (04) (05)		**Turma:** (A) (B)	

Usando a Cifra de César matematicamente com Função Resto e a Função Afim

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Código	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	N	O	P	Q	R	S	T	U	V	X	Y	W	Z
Código	13	14	15	16	17	18	19	20	21	22	23	24	25

01) Utilizando a Cifra de César de chaves 15, 22, 17, 9, 8, 24. Cifre o nome de 6 pássaros da escolha de vocês.

Nome do Pássaro Nome cifrado

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

02) Cifre a frase entregue a equipe, utilizando a cifra de César de chave a sua escolha. Coloque sua frase cifrada num pedaço de papel a parte:

_____

_____

_____

_____

03) Decifre o Texto da Equipe que lhe passou:

_____

_____

PROFMAT	**Aplicação em Escola de Ensino Médio** **Atividade 03 – Sequência Didática – Segurança Digital**	UESB
	Professor: Nathan Lopes **Componente Curricular:** Matemática **Série**: 2º Ano	
Equipe: (01) (02) (03) (04) (05)	**Turma:** (A) (B)	

APÊNDICE C – ATIVIDADE 03: AVALIANDO SEGURANÇA

01) Ao longo de nossa jornada, percebemos que o fator humano é o maior risco para a segurança digital das pessoas, pois são nos maus hábitos de escolhas de senhas que reside a maior chance de invasões. Avaliem o grau de escolha de suas senhas, marque S para sempre, N para nunca ou T para talvez.

( ) Não repito senhas.

( ) Não anoto senhas, e quando anoto, guardo em local seguro.

( ) Uso senhas com no mínimo 6 ou mais caracteres

( ) Uso caracteres diversos em minhas senhas

( ) Com periodicidade as senhas troco minhas senhas

( ) Uso ao menos um caractere de cada tipo.

( ) Não coloco caracteres em sequência como “123”, “987”, “ABC” ou “mno”

( ) Evito utilizar nomes relacionados a minha família, datas de nascimento e outras informações pessoais

( ) Utilizo caracteres que são imunes ao Ataque de Dicionário

( ) Utilizo caracteres que são imunes ao Ataque Híbrido

Cada resposta tem uma pontuação S = +2, N = -2, T = 1. A pontuação final dos integrantes foi?

02) Sabendo que dentro do Sistema ASC II, temos 95 caracteres digitáveis, contudo um deles, o caractere de “Espaço”, não é aplicável para senhas, então entre os aplicáveis temos: 10 dígitos, 26 letras maiúsculas, 26 letras minúsculas e 32 caracteres especiais.

Diante disso, quantas senhas de seis Caracteres são possíveis, usando caracteres diferentes, sendo as senhas:
Usarmos apenas dígitos:_____

Usarmos apenas letras minúsculas: _____

Usando dígitos e letras minúsculas: _____

Usando dígitos e letras minúsculas/maiúsculas: _____

Usando todos os tipos de caracteres: _____

03) Criem uma senha de seis caracteres, seguindo os Padrões de Segurança Internacionais, analisados em sala.

_____

04) Tomando as letras D,m,M,C para representar respectivamente Dígitos, Letras Minúsculas, Letras Maiúsculas e Caracteres Especiais. Represente com essas letras o formato da senha escolhida:

_____

05) Quantas senhas são possíveis com esse formato? O que podemos comparar da Senha criada pelo grupo em relação as senhas que utilizam apenas um tipo de Caractere**.**

_____

06) Quantas maneiras tem de utilizar os 4 tipos de caracteres para uma senha de 6 dígitos?

_____

PROFMAT	**Aplicação em Escola de Ensino Médio** **Atividade 04 – Sequência Didática – Segurança Digital** **Professor:** Nathan Lopes **Componente Curricular:** Matemática **Série**: 2º Ano **Equipe: (01) (02) (03) (04) (05)** **Turma:** (A) (B)	**UESB**

APÊNDICE D – ATIVIDADE 04: TABELA GERADORA DE SENHA

01) Aprendendo a criar uma Tabela Geradora de Senhas:

Para esta atividade vamos criar senhas de 6 caracteres, mas, vocês podem utilizar para quantos caracteres quiser. Usaremos a seguinte tabela abaixo, que é uma adaptação do ASC II

Caractere	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
Código	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Caractere	**J**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**A**	**B**
Código	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Caractere	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**
Código	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Caractere	**V**	**W**	**X**	**Y**	**Z**	**,**	**.**	**;**	**:**	**!**	**?**	**@**	**#**	**$**	**%**	**&**	*****	**(**	**)**
Código	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
Caractere	**+**	**-**	**=**	**_**	**[**	**]**	**<**	**>**	****	**/**									
Código	76	77	78	79	80	81	82	83	84	85									

Vocês construirão uma tabela que a partir de uma palavra-chave só, seja capaz de gerar várias senhas. Para isso vamos usar a Função Resto, e como nós não precisaremos converter os valores em converter o código para a palavra original, pode usar uma função afim de sua escolha, lembrando que a escolha da função Afim está ligada ao seu caráter de Bijetividade.

Crie 4 senhas através de uma palavra chave

Caractere: Palavra-Chave									
Código do Caractere	000	000	000	000	000	000	000	000	000
Função 01:									
Senha 01									
Função 02:									
Senha 02									
Função 03:									
Senha 03									
Função 04:									
Senha 04									