Gabriel Teixeira Soares das Neves

O ENSINO DE MATEMÁTICA ATRAVÉS DO ESTUDO DE TÉCNICAS CRIPTOGRÁFICAS UTILIZANDO O FORMATO *WEBQUEST*

Brasil

24 de outubro de 2016

Gabriel Teixeira Soares das Neves

O ENSINO DE MATEMÁTICA ATRAVÉS DO ESTUDO DE TÉCNICAS CRIPTOGRÁFICAS UTILIZANDO O FORMATO *WEBQUEST*

Dissertação de Mestrado apresentada ao Programada de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática por ter completado o Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).

Universidade Federal do Rio de Janeiro – UFRJ

Instituto de Matemática

Programa de Pós-Graduação

Orientador: Prof.ª Monique Robalo Moura Carmona, Ph.D.

Brasil

24 de outubro de 2016

CIP - Catalogação na Publicação

Teixeira Soares das Neves, Gabriel
TN511e O Ensino de Matemática Através do Estudo de Técnicas Criptográficas Utilizando o Formato WebQuest / Gabriel Teixeira Soares das Neves. -- Rio de Janeiro, 2016.
92 f.

Orientadora: Monique Robalo Moura Carmona.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Matemática, 2016.

1. Ensino Básico. 2. Criptografia. 3. Tecnologias Educacionais. 4. Recursos Computacionais. 5. WebQuest. I. Robalo Moura Carmona, Monique, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

Gabriel Teixeira Soares das Neves

O ENSINO DE MATEMÁTICA ATRAVÉS DO ESTUDO DE TÉCNICA CRIPTOGRÁFICAS UTILIZANDO O FORMATO *WEBQUEST*

Dissertação de Mestrado apresentada ao Programada de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática por ter completado o Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).

Trabalho aprovado. Brasil, 24 de agosto de 2016:

Prof. Monique Robalo Moura Carmona, Ph.D.
Instituto de Matemática - UFRJ
Orientadora/Presidente

Prof. Marisa Beatriz Bezerra Leal, D.Sc.
Instituto de Matemática - UFRJ

Prof. Rafael Brandão de Rezende Borges, D.Sc.
Instituto de Matemática e Estatística - UERJ

Brasil
24 de agosto de 2016

A todos os meus alunos:
os que foram, os que são e os que serão.
Vocês são meus maiores professores.

Agradecimentos

Aos meus pais e irmãos, Luciara Teixeira Soares, Augusto Oliveira das Neves Júnior, Joana Teixeira Soares das Neves e Samuel Teixeira Soares das Neves, do meu lado desde o inicio, me apoiando em todas minhas decisões e sempre me mostrando o que eu não conseguia ver, me falando o que eu precisava ouvir.

À minha namorada, Natália Souza Brito Pereira, pelo amor, paciência e amizades que foram tão importantes para que eu pudesse me dedicar com a paz de espírito necessária à realização desse sonho.

À professora Monique Robalo Moura Carmona, pela imensurável ajuda nessa empreitada, pela confiança, pela generosidade, pela orientação nesse trabalho, pelos inúmeros conselhos e, acima de tudo, pela compreensão nos momentos de dificuldade. A amizade continuará e, certamente, a parceria em muitos projetos porvir.

À equipe de professores que compõe o corpo docente do PROFMAT do Instituto de Matemática da UFRJ: guardarei lembranças e inspirações de cada um com muito carinho. Seguirei o exemplo de postura e de humildade em minha prática profissional.

Aos amigos da primeira turma do PROFMAT da UFRJ, com os quais criei amizade quando ainda cursava a especialização, e que foram determinantes na minha trajetória. E aos amigos da segunda turma do PROFMAT, os quais conheci já como aluno do mestrado, e que tornaram as sexta-feiras muito mais suaves.

Aos amigos de anos Ian Neves Queiroz, Gabriel Xavier Serra Carneiro de Novaes e Alice Soares de Alencar, por tantas vezes cederem um colchão quando eu estava longe de casa.

Ao Instituto Federal Fluminense e sua equipe de professores, em especial aos professores do Laboratório de Computação Física e à coordenação de Informática, que sempre estiveram dispostos a adequar meus horários de modo que eu pudesse me dedicar à atividades do mestrado.

À CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela concessão da bolsa que, por meses, tornou as atividades do mestrado possíveis.

"(...) quem forma se forma e re-forma ao formar e quem é formado forma-se e forma ao ser formado. É neste sentido que ensinar não é transferir conhecimentos, conteúdos nem formar é ação pela qual um sujeito criador dá forma, estilo ou alma a um corpo indeciso e acomodado. Não há docência sem discência, as duas se explicam e seus sujeitos apesar das diferenças que os conotam, não se reduzem à condição de objeto, um do outro."

(Paulo Freire)

Resumo

Identificar o papel que as novas tecnologias devem desempenhar no ensino básico é um desafio colocado aos professores que se encontram em sala de aula. Frequentemente o computador ainda assume um papel secundário na dinâmica da aprendizagem, tendo a função de ilustrar algum tópico ou reproduzir através de videoaulas as aulas tradicionais.

São propostas aulas no formato *WebQuest* no intuito de propiciar a exploração e experimentação usando recursos computacionais como processo de ensino-aprendizagem. Visa-se desenvolver uma abordagem moderna que dialogue com a realidade e interesse dos estudantes de hoje.

O tema escolhido foi aplicações de matemática à criptografia como fator que despertasse o curiosidade dos alunos. Exploramos as cifras de substituição, cifra de Hill, o conceito de cifra assimétrica e a cifra RSA, que são métodos de relevante interesse no desenvolvimento teórico da criptografia e que nos permitem abordar tópicos de matemática como contagem, funções, matrizes, MMC e MDC.

Palavras-chave: *Ensino Básico, Criptografia, Tecnologias Educacionais, Recursos Computacionais, WebQuest.*

Abstract

Identify the role that new tecnologies should play in the education system is a challenge set to the teachers. The computer still plays a secondary role in the dynamics of learning, either is just used to illustrate some topic or is available to exibit video classes, which is mostly a media reproduction of a tradicional class.

It is proposed courses in the WebQuest format, in order to encourage exploration and experimentation using computer resources as a teaching-learning process. The aim is to develop a modern approach that is able to dialogue with the reality and interests of the current students.

The topic chosen was the use of mathematical applications in cryptography in order to stimulate the curiosity of the students. We explore the substitution ciphers, Hill cipher, the concept of asymmetric cipher and RSA cipher, which are methods of relevant interest in the theoretical development of encryption and allows us to address topics in mathematics such as counting, functions, matrices, LCM and GCD.

Key-words: *Basic School, Cryptography, Educational Technology, Computing Resources, WebQuest.*

Sumário

Lista de ilustrações

Lista de tabelas

Introdução

Novas tecnologias surgem todos os dias e modificam a forma de se produzir conteúdo e gerar conhecimento. Existem, hoje, muitas discussões acerca do papel que essas tecnologias devem desempenhar no âmbito escolar. É necessário identificar quais os dispositivos mais eficazes para a aprendizagem por parte dos estudantes, acostumados ao acesso fácil e variado de informação através da *internet*.

As iniciativas mais populares ainda tendem a trazer, em suas abordagens, o ensino tradicional para dentro do ambiente computacional. Videoaulas, testes e exercícios que repetem exaustivamente técnicas, ainda são comuns nessas plataformas.

Através do estudo de aplicações da matemática, objetiva-se problematizar alguns temas do currículo de matemática do ensino fundamental e médio e levar novas tecnologias para a sala de aula de modo que rompa com os paradigmas educacionais mais tradicionais. Não se pretende negar ou abolir elementos como aulas expositivas e exercícios repetitivos, mas incentivar os alunos a se envolverem ativamente na geração de seu conhecimento, através da resolução de problemas de forma exploratória com o auxílio da *internet*. As atividades desenvolvidas terão o formato conhecido como *WebQuest*, idealizada em 1995 por Bernie Dodge, da Universidade de San Diego, e que tem como proposta a utilização da internet como ferramenta investigativa e criativa na execução de tarefas na escola.

O tema escolhido para as atividades propostas é criptografia. A escolha se deve ao seu papel de destaque no panorama do desenvolvimento tecnológico atual, por abordar articuladamente uma variedade satisfatória de conteúdos da matemática do ensino fundamental e médio e por instigar a curiosidade por parte dos alunos.

No capítulo 1 são apresentados e revisados os conceitos matemáticos necessários para a atividade de criptografia.

No capítulo 2 apresentam-se os métodos criptográficos utilizados nas propostas de atividades, começando pelas cifras de substituição, passando pela cifra de Hill e chegando à cifra assimétrica e a cifra RSA. Os métodos são todos definidos, exemplificados e possuem alguns de seus aspectos teóricos e práticos discutidos.

No capítulo 3 é justificado pedagogicamente o formato em que as atividades são aplicadas em sala de aula. A abordagem é conduzida inteiramente através de recursos computacionais, seja pela da busca de informações na *web*, seja através de recursos computacionais que servem para implementarmos as cifras utilizadas.

No capítulo 4 discorre-se sobre a experimentação das propostas apresentadas. São

discutidos aspectos positivos e negativos da abordagem e limitações encontradas. É feito um diagnóstico do perfil dos alunos e do papel que a tecnologia e a problematização desempenham em suas atividades escolares.

Por fim, no capítulo 5, são tecidas algumas conclusões com base nas observações e diagnósticos das experiências discutidas no capítulo anterior e trabalhos futuros.

Conceitos Preliminares de Criptografia

A criptografia (do grego, *kryptos* significa "escondido", "oculto", e *gráphein*, "escrita") é o estudo de técnicas para codificar informações de modo que apenas o receptor, escolhido pelo emissor, seja capaz de revelar o conteúdo da mensagem. O desenvolvimento da área surge como consequência da evolução e necessidade de segurança dos meios de comunicação.

Contando, inicialmente, com métodos intuitivos e práticos, as primeiras cifras desenvolvidas são as cifras de substituição, que consistem em modificar a ordem das letras do alfabeto de forma sistemática. Como exemplo, um dos primeiros métodos criptográficos formais amplamente utilizados foi a cifra de César, uma cifra de substituição utilizada pelo imperador Júlio César para proteger mensagens de conteúdo militar e, de acordo com (FIGUEIREDO, 2012, p.2), descrita em sua biografia, escrita pelo historiador romano Suetônio, como a substituição sucessiva de cada letra do alfabeto pela letra que se encontra três posições anteriores a ela, fazendo D ser cifrado como A, C como Z e assim sucessivamente.

Junto com a criptografia, surge outro campo de estudo, a *criptoanálise*, que trata das técnicas de como quebrar um método criptográfico e possibilitar que uma pessoa indevida tenha acesso à mensagem que se quer enviar com segurança. O desenvolvimento da criptografia e da criptoanálise possuem uma relação dialógica, isto é, o avanço científico de uma área motiva o avanço da outra. Essa relação é um dos fatores que justificam o avanço teórico e prático da criptografia que, inicialmente quase artesanal, conta hoje com uma robusta teoria matemática.

É chamado de *texto claro* a mensagem aberta, legível; de *texto cifrado* o texto convertido, criptografado; de *cifra* o método utilizado para criptografar, ou *cifrar* uma mensagem; e de *chave*, o segredo de implementação da cifra utilizada. Quanto ao funcionamento das chaves, há dois tipos de cifras: a *cifra simétrica*, que possui apenas uma chave utilizada na cifragem e decifragem da mensagem; e a *assimétrica*, que envolve duas chaves, uma utilizada para cifrar, chamada de chave *pública*, e outra para decifrar a mensagem, chamada de chave *privada*, como esquematizado na figura 1.

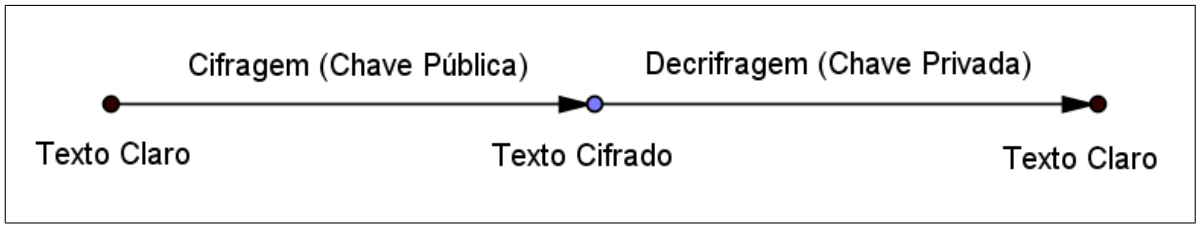


Figura 1 – Esquema de Funcionamento de uma Cifra Assimétrica.

Quando alguém tenta decifrar indevidamente uma mensagem criptografada cria-se a situação chamada de *ataque*, quando temos as figuras do *atacante*, denotado na literatura geralmente como "Eva", além das partes que se comunicam, geralmente chamadas de "Bob" e "Alice", como exemplificado no esquema da figura 2.

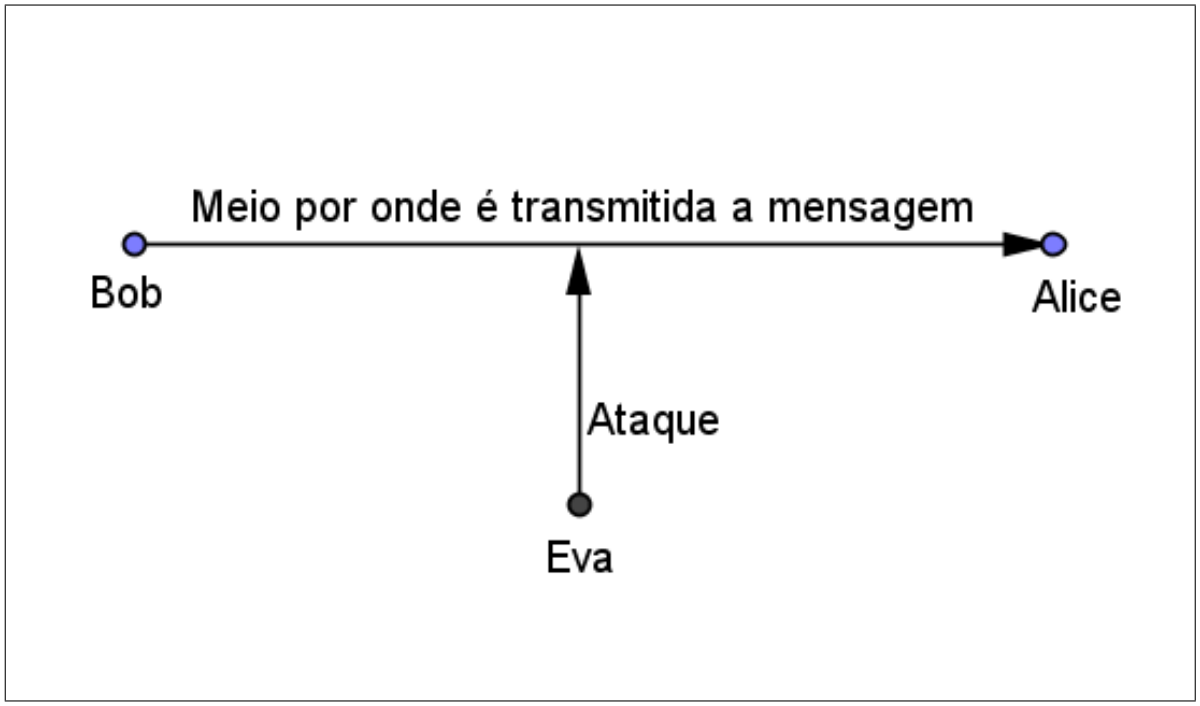


Figura 2 – Esquema de Ataque.

Os ataques mais comuns são: o *ataque de texto cifrado*, quando o atacante possui conhecimento de exemplos de diferentes textos cifrados por uma mesma cifra, e o *ataque de texto conhecido*, quando o atacante possui conhecimento de alguns textos cifrados e seus correspondentes textos claros.

Atualmente, na era da informação, é fácil enumerar os processos que envolvam algum tipo de criptografia: desde um simples *e-mail* ou mensagem de texto, até transações bancárias e informações confidenciais de instituições governamentais. Quando a matemática computacional passa a embasar boa parte da criptografia moderna, envolvendo conceitos de análise combinatória, aritmética modular, matrizes, entre outros, a criptografia e a criptoanálise passam a experimentar uma nova fase em seu desenvolvimento.

1 Conceitos Matemáticos Fundamentais

A criptografia nos dá oportunidade de estudar diversos assuntos de matemática. Neste trabalho serão abordados os assuntos de contagem, funções, matrizes e aritmética modular. Nesta seção faremos um resumo teórico de cada um desses assuntos, começando por explicar o papel que cada um desempenha no panorama teórico da criptografia.

1.1 Contagem

O problema de se conhecer a quantidade de chaves possíveis de serem criadas em uma determinada aplicação criptográfica é fundamental para se ter noção da segurança envolvida no processo. Para explorarmos esse fato, conceitos de contagem são utilizados e podem ser abordados em sala de aula.

Considere o seguinte exemplo: uma pessoa mora em Copacabana e estuda no CT da UFRJ. Quando ela perde a linha 485, pode pegar, para o centro, quatro linhas diferentes de ônibus ou o metrô. Do centro ela possui 8 opções de ônibus para a estação rodoviária da UFRJ. Da estação, há duas linhas que levam ao CT. Levando em conta essas informações, de quantas formas essa pessoa pode ir de casa para o CT, caso perca o ônibus da linha 485?

Para responder a pergunta as possibilidades são elencadas como segue:

- Possibilidades de percurso Copacabana - Centro: 1 metrô + 4 linhas de ônibus = 5 possibilidades.
- Possibilidades de percurso Centro - Estação da UFRJ: 8 linhas de ônibus = 8 possibilidades.
- Possibilidades de percurso Estação da UFRJ - CT: 2 ônibus = 2 possibilidades.

Esse tipo de problema é resolvido utilizando o *Princípio Multiplicativo*, ou *Princípio Fundamental da Contagem*, conhecido como *PFC*, que diz que, se há N possibilidades de fazer uma tarefa E_1, e M possibilidades de realizar a tarefa E_2, então há $N \times M$ possibilidades de realizar E_1 seguido de E_2.

Generalizando o PFC (FIGUEIREDO, 2012, p. 2):

Definição 1.1.1 (Princípio Fundamental da Contagem)**.** *Se uma tarefa T_1 pode ser feita de N_1 maneiras, uma tarefa T_2 de N_2 maneiras, ..., uma tarefa T_k de N_k maneiras, então o número de maneiras de realizar $T_1, T_2, \ldots T_k$, em sequência, é $N_1 \times N_2 \times \ldots N_k$.*

No caso acima, por exemplo, a pergunta possui como solução

$$5 \times 8 \times 2 = 80 \text{ possibilidades}$$

1.2 Matrizes

Em criptografia é comum converter letras em números para que se possam fazer operações com o texto. Os métodos mais antigos cifram letra a letra, mas para melhorar a segurança surgiu o interesse em cifrar blocos de texto separadamente, o que introduziu a utilização da álgebra de matrizes na criptografia.

Definição 1.2.1. *Uma matriz A sobre um conjunto $\mathbb{K}$ (neste texto sempre $\mathbb{K} = \mathbb{N}$) é um arranjo num retângulo $m \times n$ (m linhas e n colunas) de $m \cdot n$ elementos $a_{ij} \in \mathbb{K}$ ($i = 1, \ldots, m$ e $j = 1, \ldots, n$):*

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1m} \\ \vdots & \ldots & \vdots \\ a_{n1} & \ldots & a_{nm} \end{pmatrix}$$

Denotaremos $A = [a_{ij}]_{m \times n}$.

A matriz em que $m = n$ diz-se quadrada de ordem n (ou m), uma vez que possui número de colunas igual ao de linhas.

Definimos a soma entre duas matrizes do mesmo tipo $m \times n$ como a soma termo a termo correspondente de cada matriz. Isto é, sejam A e B duas matrizes $m \times n$, então:

$$A + B = [a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} = [a_{ij} + b_{ij}]_{m \times n} \; 1 \leq i \leq m \text{ e } 1 \leq j \leq n$$

A multiplicação por $\alpha \in \mathbb{K}$ é definida como a multiplicação, termo a termo da matriz, isto é:

$$\alpha A = \alpha [a_{ij}]_{m \times n} = [\alpha a_{ij}]_{m \times n} \; 1 \leq i \leq m \text{ e } 1 \leq j \leq n$$

Dadas duas matrizes $A = [a_{ij}]_{m \times n}$ e $B = [b_{ij}]_{n \times p}$, definimos o produto AB como a matriz $C = [c_{ij}]_{m \times p}$ tal que

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Dada uma matriz A de ordem n, diz-se que A é invertível se existe B de ordem n, tal que:

$$A \cdot B = B \cdot A = I$$

sendo I a matriz quadrada, chamada de *identidade*, de ordem n, cujos termos a_{ii}, da diagonal, são todos iguais a 1, e os demais iguais a 0. Neste caso, chamamos a matriz B de *matriz inversa* de A e denota-se B por A^{-1}.

1.3 Funções

O estudo de funções é o que mais recebe atenção no ensino médio e possui papel importante em diversas aplicações, inclusive na criptografia.

Definição 1.3.1. *Sejam X e Y dois conjuntos quaisquer. Uma função é uma relação $f : X \to Y$ que, a cada elemento $x \in X$ associa um, e só um, elemento $y \in Y$. Além disso,*

- *os conjuntos X e Y são chamados domínio e contradomínio de f, respectivamente;*
- *dado $x \in X$, o elemento $y = f(x) \in Y$ é chamado imagem de x por f.*
- *o conjunto $f(X) = \{y \in Y; \exists x \in X, f(x) = y\} \subset Y$ é chamado de conjunto imagem de f;*

Definição 1.3.2. *Uma função $f : X \to Y$ é dita*

- *Injetiva se, para cada $y \in Y$, existir apenas um ou nenhum $x \in X$ tal que $f(x) = y$.*
- *Sobrejetiva se o conjunto imagem coincidir com o contradomínio.*
- *Bijetiva no caso de satisfazer ambas as condições supracitadas.*

As funções bijetivas formam uma relação *biunívoca* entre os elementos de seu domínio e contradomínio. Isso permite obter uma nova função, chamada *inversa de f*, denotada $f^{-1} : Y \to X$ do seguinte modo:

$$f(x) = y \Leftrightarrow f^{-1}(y) = x.$$

Um método criptográfico que se utilize de uma função f no processo de cifragem, precisará da função f^{-1} na decifragem. Apesar de, no entanto, estarem intimamente relacionadas, o conhecimento de uma dessas funções pode não fornecer informações relevantes para o conhecimento da outra, o que se configura como uma característica interessante para o estudo da criptografia. Em métodos assimétricos, o processo de cifrar uma mensagem e o processo de decifra-la, apesar de relacionados, não dependem de uma mesma chave.

Exemplo 1.3.3 (**Cifragem e decifragem de mensagem utilizando funções**). *Fazendo a correspondência* $A \Rightarrow 1, B \Rightarrow 2, ..., Z \Rightarrow 26$*, pode-se cifrar a mensagem MATEMATICA, utilizando a função*

$$f(x) = 2x + 3.$$

De modo que o seguinte esquema é obtido:

Texto claro	M	A	T	E	M	A	T	I	C	A
P	13	1	29	5	13	1	20	9	3	1
$f(P)$	28	4	42	12	28	4	42	20	8	4

Quadro 1 – Criptografia da palavra $MATEMATICA$.

Bob enviará a mensagem "27 - 3 - 41 - 11 - 27 - 3 - 41 - 19 - 7 - 3" para Alice, que, conhecendo a inversa de f*,*

$$f^{-1}(x) = \frac{x-3}{2}.$$

poderá decifrá-la.

1.4 Aritmética Modular

Na natureza e na tecnologia são frequentes os fenômenos periódicos, cíclicos, como, por exemplo, o tempo do relógio, que se repete a cada 24 horas. Fenômenos como este operam com uma aritmética conhecida como *aritmética modular*. A Ciência da Computação utiliza essa aritmética largamente em suas aplicações, tornando-a, então, essencial para o estudo de criptografia também.

Definição 1.4.1. *Se* a *e* b *são inteiros e* m *um inteiro maior do que 0, dizemos que* a *é congruente a* b *módulo* m *o que denotamos por* $a \equiv b \bmod m$*, se* m *divide* $(a - b)$*, o que, por sua vez, é denotado por* $m|(a - b)$*.*

Por exemplo, $9 \equiv 5 \bmod 2$, pois $2|(9 - 5)$.

Existem três propriedades da aritmética modular que tornam sua manipulação parecida com a igualdade:

- Reflexividade: $a \equiv a \bmod m \ \forall a \in \mathbb{Z}$.
- Simetria: se $a \equiv b \bmod m$, então $b \equiv a \bmod m$.
- Transitividade: se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Desmontração. *Reflexividade: como* $m|0$ *e* $a - a = 0$*, então* $a \equiv a \ mod \ m$*. Simetria: Se* $a \equiv b \ mod \ m$*, então* $m|(a - b)$*, e isso significa que* $a = b + km$*. Por outro lado, ao multiplicar a equação por* -1*, fica-se com* $b = a + (-k)m$*, ou seja,* $m|(b - a)$*, e, por consequência,* $b \equiv a \ mod \ m$*. Transitividade: Se* $a \equiv b \ mod \ m$*, então tem-se que* $a = b + k_1 m$*, e se* $b \equiv c \ mod \ m$*,* $b = c + k_2 m$*. Somando as equações, obtém-se* $a = c + (k_1 + k_2)m$*, e* $a \equiv c \ mod \ m$*.*

Satisfazer essas propriedades faz da aritmética modular uma *relação de equivalência.* Uma consequência desse fato é que uma relação de equivalência cria uma partição do conjunto em que é definida.

Definição 1.4.2. *Sejam* $m > 0$ *e a inteiros. A classe de equivalência de a pela relação de congruência módulo m, chamada de classe de congruência módulo m, a qual denotaremos por* $\overline{a}$*, é definida como*

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \ mod \ m\}.$$

Para ilustrar a ideia de classe de congruência, segue o exemplo para o módulo 2.

Primeiramente a classe do 0,

$$x \in \overline{0} \Leftrightarrow x \equiv 0 \bmod 2 \Leftrightarrow 2|(x - 0) \Leftrightarrow 2|x,$$

isto é, $\overline{0}$ é o conjunto dos números pares, ou seja, dos números que deixam resto 0 na divisão por 2.

Agora, a classe do 1:

$$x \in \overline{1} \Leftrightarrow x \equiv 1 \bmod 2 \Leftrightarrow 2|(x - 1) \Leftrightarrow x = 2k + 1,$$

isto é, $\overline{1}$ é o conjunto dos números ímpares, ou seja, dos números que deixam resto 1 na divisão por 2.

Naturalmente, tem-se que o próprio $2 \in \overline{0}$, e, assim, $\overline{0} = \overline{2}$. Analogamente, $\overline{3} = \overline{1}$, e é possível concluir que $\overline{0}$ e $\overline{1}$ são todas as classes módulo 2, fato denotado por $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, que é chamado de espaço quociente da relação de congruência módulo 2 e consiste no conjunto das classes de equivalência de uma congruência módulo 2.

Proposição 1.4.3. *Sejam a, r e m inteiros, com* $0 \leq r < m$*, sendo r o resto da divisão de a por m. Então* $a \equiv r \ mod \ m$*.*

Desmontração. *Utilizando o algoritmo da divisão euclidiana, teremos que* $a = mk + r$*, onde* $0 \leq r < m$*. Ou ainda,* $mk = a - r$*, o que significa que* $m|(a - r)$ *e, por, conseguinte,* $a \equiv r \ mod \ m$*.*

A partir da proposição acima, é possível concluir que todo número natural será congruente módulo m a um dos números do conjunto $\{0, 1, 2, \cdots, m-2, m-1\}$, de possíveis restos da divisão por m, e, sendo assim, não existem outras classes de equivalência além das classes $\overline{0}, \overline{1}, \cdots, \overline{m-2}, \overline{m-1}$. Por outro lado, números pertencentes a classes distintas não podem ser congruentes (HEFEZ, 2011, p. 111). Consequentemente, o conjunto das classes de equivalência de uma congruência módulo m é

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-2}, \overline{m-1}\}.$$

Definição 1.4.4. *O conjunto dos inteiros $\{r_1, r_2, \ldots, r_s\}$ é um sistema completo de resíduos módulo m se*

1. *$r_i \not\equiv r_j \ mod\ m$, para $i \neq j$*
2. *para todo inteiro n existe um r_i tal que $n \equiv r_i \ mod\ m$*

$\mathbb{Z}_m$, forma, então, um sistema completo de resíduos módulo m.

Operações com as Classes de Congruência

Definido o que são e quais são as classes de congruência módulo m, é necessário definir uma álgebra para elas. Fazer soma de horas em um relógio é o mesmo que fazer a operação de soma entre as classes de congruência módulo 24. Por exemplo, se são 19 horas, após 8 horas serão $19 + 8 = 27 \equiv 3 \bmod 24$, ou seja, 3 horas. Ou seja, em $\mathbb{Z}_{24}$, $\overline{19} + \overline{8} = \overline{3}$. Matematicamente, isso significa que $\overline{a} + \overline{b} = \overline{a+b}$.

Proposição 1.4.5. *Em $\mathbb{Z}_m$, definimos as seguintes operações entre classes de congruências distintas:*

1. *$\overline{a+b} = \overline{a} + \overline{b}$*
2. *$\overline{a.b} = \overline{a}.\overline{b}$*

Desmontração. ***1.*** *Sejam $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$, então,*

$$\overline{a'} = \overline{a} \Rightarrow a' \equiv a \ mod\ m \Rightarrow a' = a + k_1 m, k_1 \in \mathbb{Z},$$

e

$$\overline{b'} = \overline{b} \Rightarrow b' \equiv b \ mod\ m \Rightarrow b' = b + k_2 m, k_2 \in \mathbb{Z},$$

tem-se que,

$$a' + b' = a + k_1 m + b + k_2 m = (a+b) + (k_1 + k_2)m \Rightarrow a' + b' \equiv a + b \ mod\ m,$$

portanto, $\overline{a+b} = \overline{a'} + \overline{b'} = \overline{a} + \overline{b}$.

2. *Temos que*

$$a'.b' = (a + k_1 m)(b + k_2 m) = ab + ak_2 m + bk_1 m + k_1 k_2 m^2 = \\ = ab + (bk_1 + ak_2 + k_1 k_2 m)m \Rightarrow \\ \Rightarrow a'.b' \equiv a.b \ mod \ m,$$

de onde concluímos que $\overline{a.b} = \overline{a'}.\overline{b'} = \overline{a}.\overline{b}$.

Com o exposto são definidas não só a soma e a multiplicação, mas também a associatividade, a comutatividade, o elemento neutro e um inverso aditivo. Além disso há a distributividade da multiplicação em relação à soma.

Proposição 1.4.6. *A classe* $\overline{a}$ *possui inverso módulo* m *denotado* $\overline{a}^{-1}$*, e que satisfaz* $\overline{a}.\overline{a}^{-1} \equiv 1 \ mod \ m$*, se, e somente se,* $mdc(a, m) = 1$.

Desmontração. *Seja* $\overline{a} \in \mathbb{Z}_m$*. Se* $\overline{a}$ *possui inverso* $\overline{a}^{-1}$ *módulo* m*, então:*

$$\overline{a}.\overline{a}^{-1} = \overline{1} \Rightarrow aa^{-1} \equiv 1 \ mod \ m \Rightarrow m|(aa^{-1} - 1) \Rightarrow aa^{-1} - 1 = km \Rightarrow aa^{-1} - km = 1.$$

Seja agora $mdc(a, m) = d$*. Como* $d|a$ *e* $d|m$*, então:*

$$d|(aa^{-1} - km) \Rightarrow d|1 \Rightarrow d = 1$$

Inversamente, se $mdc(a, m) = 1$*, então existem* k_1 *e* k_2*, tais que* $ak_1 + mk_2 = 1$ *(FIGUEIREDO, 2009). Então,* $ak_1 - 1 = -mk_2$ *é múltiplo de* m*, ou seja,*

$$ak_1 \equiv 1 \ mod \ m \Rightarrow \overline{a}\overline{k_1} = \overline{1}.$$

Ou seja, $\bar{a}$ *possui inversa em* $\mathbb{Z}_m$.

Definição 1.4.7. *Seja* $m \in \mathbb{N}$*, a função* φ *de Euler, denotada por* $\varphi(m)$*, representa quantidade de inteiros menores ou igual a* m *e co-primos a* m*, isto é, tais que* $mdc(k, m) = 1$*:*

Exemplos:

- $\varphi(1) = 1$;
- $\varphi(2) = 1$;
- $\varphi(4) = 2$.

Em particular, se p é um número primo, ele não possuirá divisor positivo e menor do que ele, assim sendo:

$$\varphi(p) = p - 1$$

e mais geralmente, se um número a é primo em relação a p, ele também o será em relação a p^k, para qualquer $k \geq 1$, e vice-e-versa. Como p é primo, então, apenas os múltiplos de p menores ou iguais a p^k dividirão p^k. Seja a um múltiplo de p menor que p^k então

$$a = bp,\ p \leq\ b < p^{k-1}.$$

Portanto, haverá p^{k-1} entre 0 e p^k que não são contabilizados na função $\varphi(p^k)$, então

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Teorema 1.4.8. *Sejam m e n inteiros positivos tais que $mdc(m,n) = 1$, então*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Desmontração ((HEFEZ, 2011)). *Vamos dispor os números de 1 até mn da seguinte maneira:*

1	$m+1$	$2m+1$	$\ldots$	$(n-1)m+1$
2	$m+2$	$2m+2$	$\ldots$	$(n-1)m+2$
3	$m+3$	$2m+3$	$\ldots$	$(n-1)m+3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
m	$2m$	$3m$	$\ldots$	nm

Se na linha r, onde estão os termos $r, m+r, \ldots, (n-1)m+r$, tivermos $mdc(m,r) = d > 1$, então nenhum termo nesta linha será primo com nm, uma vez que estes termos, sendo da forma $km + r, 0 \leq k \leq n-1$, são todos divisíveis por d que é o máximo divisor comum de m e r. Logo, para encontrarmos os inteiros desta tabela que são primos com mn, devemos olhar na linha r somente se $(m,r) = 1$. Portanto temos $\varphi(m)$ linhas onde todos os elementos são primos com m.

Devemos, pois, procurar em cada uma dessas $\varphi(m)$ linhas, quantos elementos são primos com n, uma vez que todos são primos com m. Como $(m,n) = 1$, os elementos $r, m+r, 2m+r, \ldots, (n-1)m+r$ formam um sistema completo de resíduos módulo n. Logo, cada uma destas linhas possui $\varphi(n)$ elementos primos com n e, portanto, como eles são primos com m, eles são primos com mn. Isto nos garante que $\varphi(mn) = \varphi(m)\varphi(n)$.

Como um número sempre pode ser decomposto em fatores primos, o teorema acima nos permite calcular φ pra qualquer número natural.

Teorema 1.4.9 (Teorema de Euler). *Se m e a são inteiros, com $m > 0$ tais que $mdc(a,m) = 1$, então*

$$a^{\varphi(m)} \equiv 1\ mod\ m.$$

Para prosseguir com a demonstração do resultado acima, é necessário o seguinte resultado:

Lema 1.4.10. *Seja* $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ *o conjunto das classes de congruência que possuem inversa módulo* m*. Seja, agora,* b *um número que possui inverso módulo* m*, então,*

$$\{ba_1, ba_2, \cdots, ba_{\varphi(m)}\}$$

também é um conjuto de representante das classes de congruência que possuem inversa módulo m*.*

Desmontração. *Como o produto de números invertíveis módulo* m *também é invertível módulo* m*, os números* $ba_1, ba_2, \cdots, ba_{\varphi(m)}$ *são todos invertíveis módulo* m*. Para o que segue precisamos:*

1. *Provar que estes inteiros representam classes distintas módulo* m*.*
2. *Provar que eles representam* ***todas*** *as classes com inversa módulo* m*.*

Para o primeiro item, como $mdc(a, m) = 1$*,*

$$ba_i \equiv ba_j \ mod\ m \Rightarrow b^{-1}ba_i \equiv b^{-1}ba_j \ mod\ m \Rightarrow a_1 \equiv a_j \ mod\ m \Rightarrow i = j.$$

O segundo segue do fato de $\{ba_1, ba_2, \cdots, ba_{\varphi(m)}\}$ *possui* $\varphi(m)$ *elementos, todos invertíveis módulo* m *em classes de congruências distintas, o que prova que formam um conjunto representante das classes de congruência invertíveis módulo* m*.*

Desmontração. *(Teorema de Euler): Seja* $\{a_1, \cdots, a_{\varphi(m)}\}$ *um conjunto de representantes de classes de congruência invertíveis módulo* m*. Pode-se, dela, formar um novo conjunto do mesmo tipo com os elementos* $\{ba_1, \cdots, ba_{\varphi(m)}\}$*, com* $mdc(b, m) = 1$*. Assim, teremos*

$$\begin{aligned} ba_1 \cdot \cdots \cdot ba_{\varphi(m)} &\equiv a_1 \cdot \cdots \cdot a_{\varphi(m)} \ mod\ m \Rightarrow \\ b^{\varphi(m)}(a_1 \cdot \cdots \cdot a_{\varphi(m)}) &\equiv a_1 \cdot \cdots \cdot a_{\varphi(m)} \ mod\ m \Rightarrow \\ a^{\varphi(m)} &\equiv 1 \ mod\ m \end{aligned}$$

2 Criptografia

Os métodos criptográficos aqui tratados foram escolhidos levando em conta sua relevância histórica, teórica e de suas aplicações em tecnologia dentro de um curso de ensino médio. Eles serão divididos em dois grandes grupos: as cifras simétricas e as cifras assimétricas.

A cifra de César, primeiro método criptográfico que será tratado, é reconhecidamente o primeiro método formal de criptografia, datado do primeiro século antes de Cristo. Serão, ainda, abordados métodos que surgiram na tentativa de solucionar problemas operacionais enfrentados, como é o caso da cifra de Hill e o conceito das cifras assimétricas. Por fim, abordaremos a cifra RSA, um dos métodos mais utilizados em aplicações comerciais atuais.

2.1 Cifras Simétricas

As cifras simétricas foram as primeiras a serem concebidas e são caracterizadas por só dependerem de uma chave, que serve tanto para o processo de cifragem como para o processo de decifragem do método.

2.1.1 A Cifra de César

A cifra de César consiste em associar, sequencialmente, cada letra do alfabeto com outra letra a uma distância fixa, distância essa que consistirá na chave do método. Desse modo, sendo a distância igual a 5, a letra “A” passa a ser representada por “F”, “B” por “G”, e assim sucessivamente. Em sua implementação é de praxe que, ao invés de se lidar com letras, se faça a conversão de forma ordenada entre as letras do alfabeto e os numerais de 1 a 26, como exemplificado no quadro 2. Cifras como a de César, que consistem na troca sistemática entre letras, são chamadas de *cifras de substituição*.

Índice	**Letra**	**Aplicação do método**	**Índice**	**Letra**
1	A	$\longrightarrow$	6	F
2	B	$\longrightarrow$	7	G
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
25	Y	$\longrightarrow$	4	D
26	Z	$\longrightarrow$	5	E

Quadro 2 – Correspondência letra-número do alfabeto criada na Cifra de César de chave 5.

Exemplo 2.1.1. *Encriptar a mensagem "SOL" utilizando a cifra de César e a chave 5.*

Para uma cifra com chave que desloca as letras em 5 posições, que gera um quadro como a 2.

Desse modo a mensagem "SOL" ficaria cifrada da seguinte maneira:

Texto claro	S	O	L
Correspondência pré-cifra	19	15	12
Correspondência pós-cifra	24	20	17
Texto cifrado	X	T	Q

Quadro 3 – Aplicação da Cifra de César

O que nos fornece a mensagem cifrada "XTQ"

Cifras de substituição não fornecem segurança. Esta vulnerabilidade se deve ao fato de que a frequência com que cada letra aparece em um determinado idioma é mais ou menos constante independente do texto, o que torna fácil a criptoanálise do método mediante a distribuição de frequências das letras do alfabeto. A língua portuguesa, por exemplo, possui distribuição de frequências das letras apresentada no quadro 4.

Letra	**Frequência (%)**		**Letra**	**Frequência (%)**
A	14,47		N	4,81
B	1,00		O	10,45
C	3,80		P	2,45
D	4,71		Q	1,24
E	12,89		R	6,26
F	1,01		S	7,46
G	1,21		T	4,29
H	1,29		U	4,88
I	6,86		V	1,76
J	0,30		W	0,00
K	0,00		X	0,34
L	2,99		Y	0,00
M	5,09		Z	0,43

Quadro 4 – Frequência das letras do alfabeto da Língua Portuguesa, baseado na análise do livro *Memórias Póstumas de Brás Cubas* (FIGUEIREDO, 2012).

Apesar disso, a cifras de substituição ainda são utilizadas em processos que não exijam grande segurança, "não para confidencialidade mas para ocultar uma mensagem do olhar casual. Ou seja, força o leitor a decifrar a mensagem caso queira realmente descobrir seu significado. A variação ROT13, que utiliza o deslocamento de 13 posições é,

por exemplo, utilizada em sites para ocultar *spoilers* (descrição do que acontecerá em um filme ou seriado), respostas de perguntas e material ofensivo" (FIGUEIREDO, 2012, p. 5).

Exemplo 2.1.2 (Decifragem do ROT13 através da análise de frequência)**.** *Decifrar o seguinte texto cifrado:*

Nzbh qndhryn irm pbzb fr sbffr n hygvzn Orvwbh fhn zhyure pbzb fr sbffr n hygvzn R pnqn svyub frh pbzb fr sbffr b havpb R ngenirffbh n ehn pbz frh cnffb guzvqb Fhovh n pbafgehpnb pbzb fr sbffr zndhvan Rethrh ab cngnzne dhngeb cnerqrf fbyvqnf Gvwbyb pbz gvwbyb ahz qrfraub zntvpb Frhf byubf rzobgnqbf qr pvzragb r yntevzn Fragbh cen qrfpnafne pbzb fr sbffr fnonqb Pbzrh srvwnb pbz neebm pbzb fr sbffr hz cevapvcr Ororh r fbyhpbh pbzb fr sbffr hz anhsentb Qnapbh r tnetnyubh pbzb fr bhivffr zhfvpn R gebcrpbh ab prh pbzb fr sbffr hz oronqb R syhghbh ab ne pbzb fr sbffr hz cnffneb R fr npnobh ab punb srvgb hz cnpbgr synpvqb Ntbavmbh ab zrvb qb cnffrvb choyvpb Zbeerh an pbagenznb ngencnyunaqb b gensrtb

Nzbh qndhryn irm pbzb fr sbffr b hygvzb Orvwbh fhn zhyure pbzb fr sbffr n havpn R pnqn svyub frh pbzb fr sbffr b cebqvtb R ngenirffbh n ehn pbz frh cnffb oronqb Fhovh n pbafgehpnb pbzb fr sbffr fbyvqb Rethrh ab cngnzne dhngeb cnerqrf zntvpnf Gvwbyb pbz gvwbyb ahz qrfraub ybtvpb Frhf byubf rzobgnqbf qr pvzragb r gensrtb Fragbh cen qrfpnafne pbzb fr sbffr hz cevapvcr Pbzrh srvwnb pbz neebm pbzb fr sbffr b znkvzb Ororh r fbyhpbh pbzb fr sbffr zndhvan Qnapbh r tnetnyubh pbzb fr sbffr b cebkvzb R gebcrpbh ab prh pbzb fr bhivffr zhfvpn R syhghbh ab ne pbzb fr sbffr fnonqb R fr npnobh ab punb srvgb hz cnpbgr gvzvqb Ntbavmbh ab zrvb qb cnffrvb anhsentb Zbeerh an pbagenznb ngencnyunaqb b choyvpb

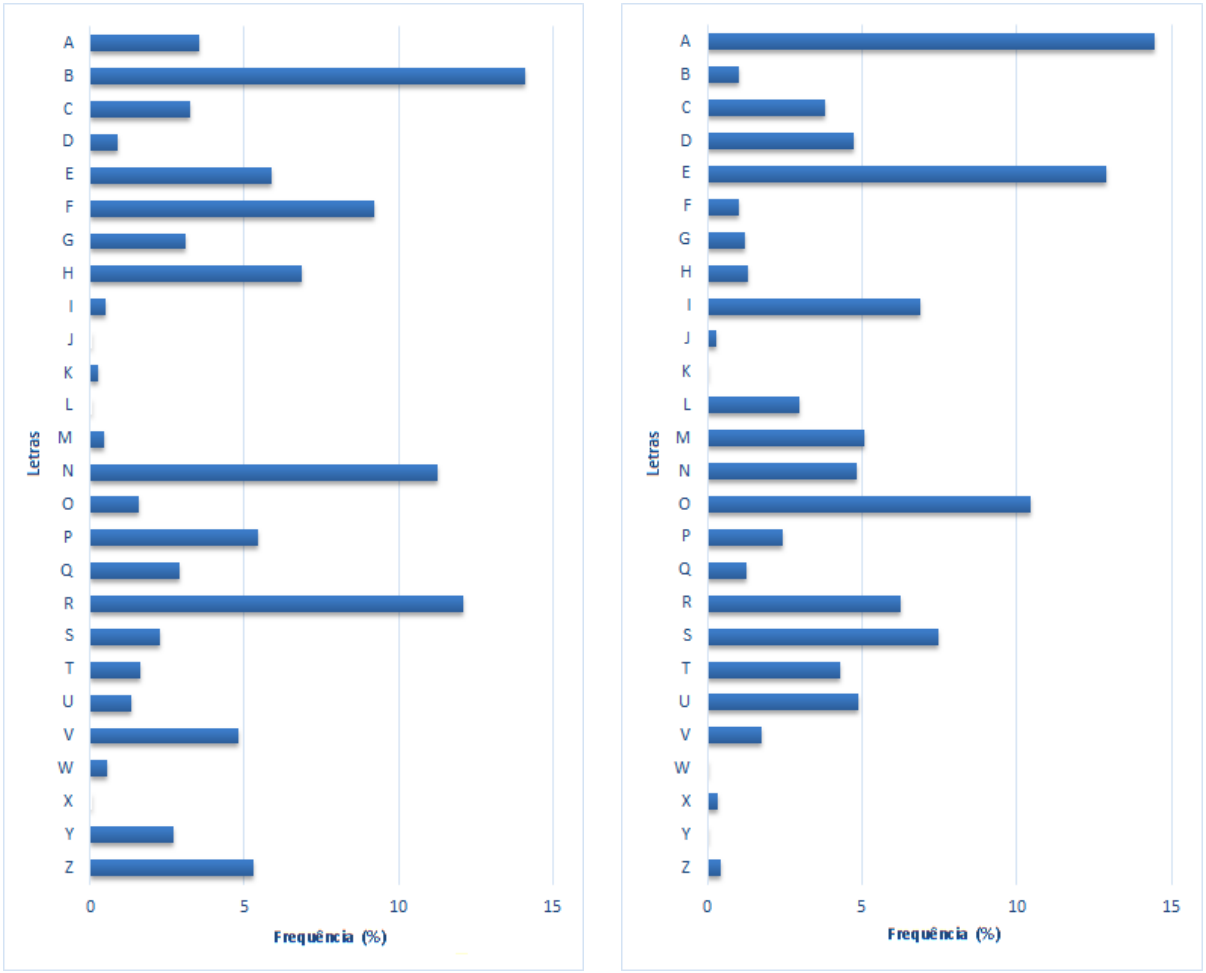
Nzbh qndhryn irm pbzb fr sbffr zndhvan Orvwbh fhn zhyure pbzb fr sbffr ybtvpb Rethrh ab cngnzne dhngeb cnerqrf synpvqnf Fragbh cen qrfpnafne pbzb fr sbffr hz cnffneb R syhghbh ab ne pbzb fr sbffr hz cevapvcr R fr npnobh ab punb srvgb hz cnpbgr oronqb Zbeerh an pbagen-znb ngencnyunaqb b fnonqb

Cbe rffr cnb cen pbzre cbe rffr punb cen qbezve N pregvqnb cen anfpre r n pbaprffnb cen fbeeve Cbe zr qrvkne erfcvene cbe zr qrvkne rkvfgve Qrhf yur cnthr

Cryn pnpunpn qr tenpn dhr n tragr grz dhr ratbyve Cryn shznpn r n qrftenpn dhr n tragr grz dhr gbffve Crybf naqnvzrf cvatragrf dhr n tragr grz dhr pnve Qrhf yur cnthr

Cryn zhyure pnecvqrven cen abf ybhine r phfcve R crynf zbfpnf ovpurvenf n abf orvwne r pboeve R cryn cnm qreenqrven dhr rasvz inv abf erqvzve Qrhf yur cnthr

Solução: *Camparemos os gráficos de ambos as análises de frequência das letras no texto e na língua portuguesa:*



(a) Análise de frequência das letras no texto analisado.

(b) Análise de frequência das letras do alfabeto na língua portuguesa.

Figura 3 – Análise de Frequências

No texto cifrado, podemos identificar três picos ocorrendo nas letras "N", "R" e "V", a uma mesma distância que as letras "A", "E" e "I" na língua portuguesa, caso análogo com o que ocorre entras as letras "B" e "F" no texto cifrado e "O" e "S" da língua portuguesa, além do vale que vai da letra "H" até "M" na figura 3a e entre as letras "V" e "Z" na figura 3b. Essas informações nos fazem acreditar que o "A" está sendo cifrado como "N", "B" como "O" e assim suscetivamente. Se fizermos as substituições de acordo com esse padrão obtemos o seguinte texto:

Amou daquela vez como se fosse a ultima Beijou sua mulher como se fosse a ultima E cada filho seu como se fosse o unico E atravessou a rua com seu passo timido Subiu a construcao como se fosse maquina Ergueu no patamar quatro paredes solidas Tijolo com tijolo num desenho magico Seus olhos embotados de cimento e lagrima Sentou pra descansar como se fosse sabado Comeu feijao com arroz como se fosse um principe Bebeu e solucou como se fosse um naufrago Dancou e gargalhou como se ouvisse musica E tropecou no ceu como se fosse um bebado E flutuou no ar como se fosse um passaro E se acabou no chao feito um pacote flacido Agonizou no meio do passeio publico Morreu na contramao atrapalhando o trafego

Amou daquela vez como se fosse o ultimo Beijou sua mulher como se fosse a unica E cada filho seu como se fosse o prodigo E atravessou a rua com seu passo bebado Subiu a construcao como se fosse solido Ergueu no patamar quatro paredes magicas Tijolo com tijolo num desenho logico Seus olhos embotados de cimento e trafego Sentou pra descansar como se fosse um principe Comeu feijao com arroz como se fosse o maximo Bebeu e solucou como se fosse maquina Dancou e gargalhou como se fosse o proximo E tropecou no ceu como se ouvisse musica E flutuou no ar como se fosse sabado E se acabou no chao feito um pacote timido Agonizou no meio do passeio naufrago Morreu na contramao atrapalhando o publico

Amou daquela vez como se fosse maquina Beijou sua mulher como se fosse logico Ergueu no patamar quatro paredes flacidas Sentou pra descansar como se fosse um passaro E flutuou no ar como se fosse um principe E se acabou no chao feito um pacote bebado Morreu na contra-mao atrapalhando o sabado

Por esse pao pra comer por esse chao pra dormir A certidao pra nascer e a concessao pra sorrir Por me deixar respirar por me deixar existir Deus lhe pague

Pela cachaca de graca que a gente tem que engolir Pela fumaca e a desgraca que a gente tem que tossir Pelos andaimes pingentes que a gente tem que cair Deus lhe pague

Pela mulher carpideira pra nos louvar e cuspir E pelas moscas bicheiras a nos beijar e cobrir E pela paz derradeira que enfim vai nos redimir Deus lhe pague

Descobrimos, por fim, que a canção Construção, do compositor Chico Buarque, havia sido cifrada com uma cifra de César com chave 13, isto é, através da ROT13, citada anteriormente.

2.1.2 Cifra de Hill

Visando tornar a análise de frequência ineficaz, em 1929, o matemático norte-americano Lester S. Hill publica o livro *Cryptography in an Algebraic Alphabet*, no qual ele propõe método criptográfico envolvendo aritmética de matrizes (FIGUEIREDO, 2013), de modo que uma mesma letra fosse cifrada de forma diferente dependendo da posição em que aparece no texto, característica chamada de *difusão*.

O algoritmo da cifra de Hill, também um cifra de substituição, se inicia com a correspondência letra-número feita de forma análoga às cifras de substituição, como indicado no quadro 5.

A	B	C	...	X	Y	Z
0	1	2	...	23	24	25

Quadro 5 – Exemplo de correspondência letra-número para cifra de Hill.

Em seguida, o texto claro é dividido em blocos de n caracteres que são arrumados na forma de vetores de n posições. Em um alfabeto de 26 letras, a cifra de Hill opera com classes de congruência módulo 26, e sua chave consiste numa matriz K de ordem n, cujo determinante deve possuir inverso mod 26. Sendo $\vec{P}$ um dos blocos, o seu correspondente cifrado é o vetor $\vec{C}$ resultado da multiplicação de K pelo vetor que contém o texto claro $\vec{P}$, isto é

$$\vec{C} = K \cdot \vec{P}$$

Para decifrar a mensagem é aplicada a inversa de K módulo 26 que, de acordo com (ZATTI; BELTRAME, 2006), é definida como a matriz, denotada por K^{-1}, tal que

$$K \cdot K^{-1} = K^{-1} \cdot K \equiv I_n \bmod 26$$

sendo

$$K^{-1} = (det\ K)^{-1} \cdot \overline{K} \bmod 26$$

sendo $(det\ K) \neq 0$, $(det\ K)^{-1}$ o inverso multiplicativo mod 26 (quadro 6) do determinante de K e $\overline{K}$ a adjunta de K (ZATTI; BELTRAME, 2006).

$(det\ K)$	1	3	5	7	9	11	15	17	19	21	23	25
$(det\ K)^{-1}$	1	9	21	15	3	19	7	23	11	5	17	25

Quadro 6 – Inversos multiplicativos módulo 26.

Conclui-se, então, que,

$$\vec{P} = K^{-1} \cdot (K \cdot \vec{P}) = (K^{-1} \cdot K) \cdot \vec{P} = I_n \cdot \vec{P} = \vec{P}$$

Na etapa final é tomado o equivalente módulo 26 do vetor resultante.

Exemplo 2.1.3. *Aplicar a cifra de Hill à palavra LUA, utilizando a chave* 3×3

$$K = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 6 & 1 \\ 5 & 3 & 4 \end{pmatrix}.$$

Solução: *Primeiramente, note que a matriz K possui determinante -19, e* $-19 \equiv 7 \ mod\, 26$*, e, desse modo, possui inversa módulo 26. Utilizando o quadro 6,*

$$K^{-1} = -19^{-1} \begin{pmatrix} 21 & -5 & -4 \\ -11 & -1 & 3 \\ -18 & 7 & -2 \end{pmatrix} = 15 \begin{pmatrix} 21 & -5 & -4 \\ -11 & -1 & 3 \\ -18 & -7 & -2 \end{pmatrix} =$$
$$\begin{pmatrix} 315 & -75 & -60 \\ -165 & -15 & 45 \\ -270 & 105 & -30 \end{pmatrix} \equiv \begin{pmatrix} 3 & 3 & 18 \\ 17 & 11 & 19 \\ 16 & 1 & 22 \end{pmatrix} \ mod\, 26$$

Considerando a conversão da palavra através do quadro 5

$$P = \begin{pmatrix} 12 \\ 20 \\ 0 \end{pmatrix}.$$

A mensagem cifrada por K será

$$C = K \cdot P = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 6 & 1 \\ 5 & 3 & 4 \end{pmatrix} \begin{pmatrix} 12 \\ 20 \\ 0 \end{pmatrix} = \begin{pmatrix} 52 \\ 168 \\ 120 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 12 \\ 16 \end{pmatrix} \ mod\, 26$$

que fornece nos a mensagem ALP.

O receptor da mensagem terá acesso a mensagem ALP. Para recuperar o texto claro, ele deverá aplicar K^{-1} *a C. Ou seja, ele calculará*

$$P = K^{-1} \cdot C = \begin{pmatrix} 3 & 3 & 18 \\ 17 & 11 & 19 \\ 16 & 1 & 22 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \\ 16 \end{pmatrix} = \begin{pmatrix} 324 \\ 436 \\ 364 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 20 \\ 0 \end{pmatrix} \ mod\, 26$$

que corresponde à mensagem original.

Por se tratar de um esquema criptográfico que apenas envolve operações lineares, a cifra de Hill apresenta grandes vulnerabilidades. É possível quebrá-lo desde que haja posse de alguns exemplares de texto claro e seus correspondentes cifrados. Para ilustrar esse fato, (FIGUEIREDO, 2013) propõe o seguinte exemplo:

Exemplo 2.1.4. *Suponha que utilizamos blocos de tamanho 2. Então a chave é uma matriz quadrada invertível de ordem* 2×2*, que podemos representar por:*

$$K = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}$$

O atacante conhece 2 blocos de texto claro e seus correspondentes cifrados:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \to \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}; \begin{pmatrix} p_3 \\ p_4 \end{pmatrix} \to \begin{pmatrix} c_3 \\ c_4 \end{pmatrix}$$

Cada par $\binom{c_i}{c_{i+1}}$ *é o produto da matriz* K *pelo par correspondente* $\binom{p_i}{p_{i+1}}$*. Portanto*

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \to \begin{cases} k_1 p_1 + k_2 p_2 = c_1 \\ k_3 p_1 + k_4 p_2 = c_2 \end{cases}$$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} p_3 \\ p_4 \end{pmatrix} = \begin{pmatrix} c_3 \\ c_4 \end{pmatrix} \to \begin{cases} k_1 p_3 + k_2 p_4 = c_3 \\ k_3 p_3 + k_4 p_4 = c_4 \end{cases}$$

Este sistema pode ser facilmente resolvido utilizando os métodos usuais de sistemas lineares. Caso algum deles seja indeterminado, basta conseguirmos mais um par de texto claro e texto cifrado e tentar novamente. O desafio no desenvolvimento teórico da criptografia passa a incluir a criação de métodos com o mínimo de linearidade em seus processos sem perder de vista a sua viabilidade de implementação.

Um exemplo de método que une a difusão dada pela multiplicação por matrizes, mas inclui etapas que visam tonar o método menos linear, é o DES. Nele há etapas que envolvem multiplicação de matrizes, mas também há geração de sub-chaves, operações lógicas binárias, como o *ou exclusivo*. Sua implementação, no entanto, foge aos objetivos do presente texto e recomendamos (FIGUEIREDO, 2013) para maior aprofundamento.

2.2 Cifras Assimétricas

Cifras simétricas exigem confiabilidade tanto de quem manda quanto de quem recebe a mensagem pois usa a mesma chave para os processos de cifragem e decifragem. Numa empresa, isso significa que despedir um funcionário pode comprometer toda a

segurança dos meios de comunicação utilizados em suas atividades. As cifras assimétricas possuem características que as tornaram populares em transações bancárias e atividades empresariais diversas por contornarem problemas como este.

Métodos assimétricas utilizam duas chaves em sua implementação, uma, chamada de chave pública, para cifrar o texto claro, e outra, chamada de chave privada, para decifrar a mensagem cifrada. Apesar das chaves estarem relacionadas, é importante que o conhecimento da chave pública não nos forneça informações para a obtenção da chave privada de forma praticável.

Em sua implementação, Alice divulga sua chave pública, que servirá para que Bob cifre as mensagens que necessitar lhe enviar com segurança. A única forma de um atacante decifrar a mensagem enviada por Bob para Alice seria com o conhecimento da chave privada, utilizada no processo de decifragem, da qual apenas Alice possui conhecimento.

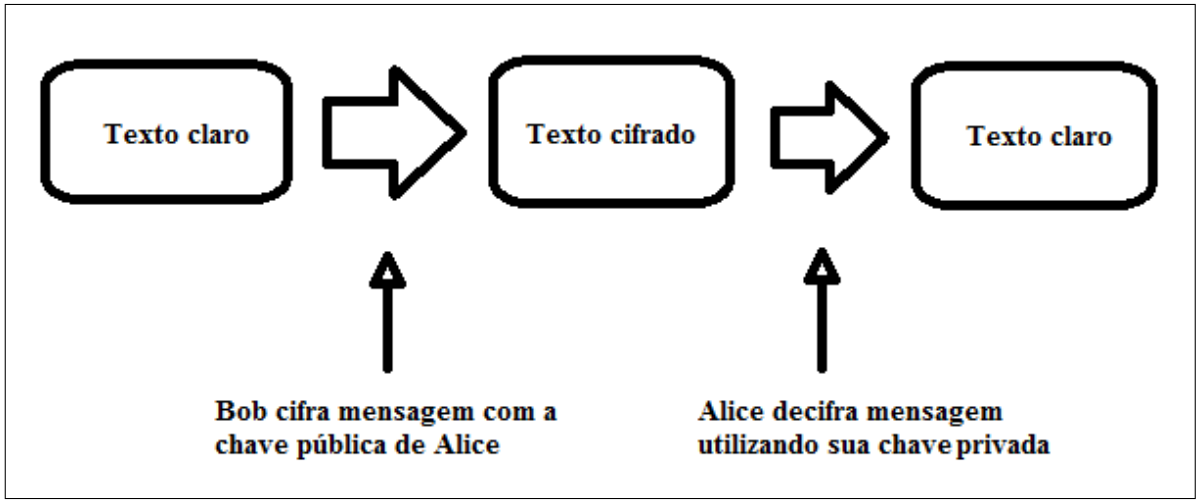


Figura 4 – Processo de cifragem/decifragem de uma cifra de chave pública genérica.

Note que esse conceito não envolve o método criptográfico em si, mas o processo de implementação do método. O esquema geral de funcionamento, concebido por Whitfield Diffie, foi conceitualmente proposto em 1975, e em 1977 surgiu o primeiro e mais famoso esquema do tipo até hoje, o RSA (FIGUEIREDO, 2013).

2.2.1 RSA

Criada por Ronald Rivest, Adi Shamir e Leonard Adlerman, na época todos pesquisadores do M. I. T. (Massachussets Institute of Technology), esse foi o primeiro sistema criptográfico de chave pública concebido e permanece com grande importância, sendo amplamente utilizado por empresas e em transações financeiras.

Dividimos a explicação do algoritmo do método RSA em *pré-codificação* e *codificação*. Na pré-codificação as letras são convertidas em números e as chaves geradas. A parte de

codificação envolverá o método em si, tendo posse das informações fornecidas pela etapa anterior.

Pré-Codificação

Após a conversão de letras em números como feito nas seções anteriores, as chaves que serão utilizadas no processo são determinadas e é feita a divisão em blocos da mensagem a ser codificada. Para a geração das chaves são escolhidos dois números primos p e q cujo produto $n = pq$ fará parte de ambas as chaves do método. Em seguida a mensagem é quebrada em blocos de tamanho s, $0 \leq s \leq n$.

Codificação: O Algoritmo

O algoritmo é iniciado calculando $\varphi(n)$, de acordo com a definição 1.4.7. Será necessário ainda fornecer um número e, parte da chave pública do método, invertível módulo $\varphi(n)$, isto é, $mdc(e, \varphi(n)) = 1$. O inverso multiplicativo de e módulo $\varphi(n)$, que denotaremos d, deve ser calculado, de modo que teremos as seguintes chaves

- Chave Pública: par (e, n).
- Chave Privada: par (d, n).

Sendo P um bloco de texto de nossa mensagem clara, conseguimos o correspondente cifrado C dele através de

$$C \equiv P^e \bmod n,$$

sendo que $C^d \bmod n$ refere-se a elevação à n-ésima potência dos valores de cada posição do vetor C seguido do cálculo do módulo referente a n de cada um desses valores. Ou seja, o processo de cifragem envolve uma operação de exponencial módulo n, o que pode ser feito de forma simples.

Decifrando o RSA

O processo de decifragem do algoritmo é parecido com o de cifragem, envolvendo uma exponenciação utilizando a parte privada da chave d, de modo que

$$P \equiv C^d \bmod n,$$

pois, como $ed \equiv 1 \bmod \varphi(n)$, tem-se que

$$C^d = (P^e)^d = P^{ed} = P^{1+k\varphi(n)} = P(P^{\varphi(n)})^k,$$

para algum $k \in \mathbb{Z}$.

Pelo teorema de Euler, se $mdc(P, n) = 1$, então $P^{\varphi(n)} \equiv 1 \bmod n$, logo

$$C^d = P(P^{\varphi(n)})^k \equiv P \bmod n,$$

recuperando a mensagem clara.

Exemplo 2.2.1 (Codificação e decodificação do método RSA)**.** *Vejamos como utilizar o método RSA para cifrar uma mensagem dada.*

Geração de chaves

Passo 1: *Escolher dois números primos grandes $p \neq q$, de modo que seja impraticável a fatoração de $n = pq$ por meio de força bruta. Por exemplo, sejam $p = 887$ e $q = 911$, que nos fornece $n = pq = 887 \times 911 = 808057$..*

Passo 2: *Calcular o valor da função de Euler $\varphi(n)$*

$$\varphi(808057) = \varphi(887)\varphi(911) = (887 - 1) \times (911 - 1) = 886 \times 910 = 806260$$

Passo 3: *Escolher um inteiro e tal que $1 < e < \varphi(n)$ e $mdc(e, \varphi(n)) = 1$. Seja $e = 51$*

Passo 4: *Calcular d tal que $1 < d < \varphi(n)$ e $de \equiv 1$ mod $\varphi(n)$. No caso, $d = 790451$*

As chaves obtidas foram:

- *Chave pública: o par de números $(e, n) = (51, 808057)$*
- *Chave privada: o par de números $(d, n) = (744680, 808057)$*

Processo de cifragem

Suponha que a mensagem que queremos cifrar seja $D = 10000$. O método RSA de criptografia divide a mensagem em blocos de tamanho fixo. É importante notar que a conversão de cada bloco em inteiro não deve gerar um número maior do que n. A mensagem cifrada é o inteiro C, $1 \leq C \leq n$, tal que $C \equiv P^e$ mod n, então

$$C \equiv 10000^{51} \ mod \ 808057$$

Então, $C = 443869$.

Processo de decifragem

Para recuperarmos a mensagem, basta calcular

$$P \equiv C^d \ mod \ n$$

então,

$$443869^{790451} \equiv 1000 \ mod \ 808057$$

o que nos devolve $P = 1000$.

Existem técnicas para calcular equivalências com exponenciais como as acima, e para aprofundamento recomendamos (HEFEZ, 2011). Já com números primos relativamente pequenos se comparados aos utilizados comercialmente, as exponenciais são incalculáveis à mão ou mesmo na maioria das calculadoras científicas comuns.

Exemplo 2.2.2 (Quebrando o RSA e entendendo sua segurança)**.** *A chave pública de Alice é (23, 143). Bob utiliza essa chave para criptografar uma mensagem para Alice. Bob envia a mensagem C = 2. Quebre o código, descubra a chave privada de Alice e revele a mensagem original.*

Solução: Vamos descobrir a chave privada de Alice e decifrar a mensagem:

Para tanto, temos que a chave pública de Alice é (23, 143). Já a mensagem cifrada é C = 2.

Inicialmente temos que, se n = 143, então os primos envolvidos foram 11 e 13. Daí,

$$\varphi(143) = \varphi(11.13) = \varphi(11) \cdot \varphi(13) = (11-1)(13-1) = 10 \times 12 = 120.$$

Temos que o inverso de 23 módulo 120 é 47 (chave privada de Alice), que pode ser calculado via algoritmo de Euclides.

Daí, a função decifragem ($D(C) = C^{chave \ privada} \ mod \ n$) *fica:*

$$2^{47} \equiv 7 \ mod \ 143.$$

Recuperando a mensagem original D = 7.

Para primos pequenos foi simples quebrar o método RSA pois o número 143 é de fácil fatoração e nos retorna os primos 11 e 13 facilmente. A segurança é garantida apenas se houver certeza de que d não pode ser calculado através da força bruta com o conhecimento de n e e, que formam a chave pública. Isso se deve ao fato do problema de fatorar números muito grandes ser computacionalmente impraticável. Para isso, os

primos em questão devem ter cerca de 100 algarismos, de modo que n tenha cerca de 200 algarismos! Os computadores atuais ainda não possuem o poder de processamento necessário para realizar a fatoração de um número dessa magnitude em tempo razoável.

O problema de escolher primos para o método pode ser desafiador e foge aos objetivos do presente trabalho. No livro *Elementos*, Euclides demonstra que existem infinitos números primos, o que torna possível a implementação do RSA. As perguntas que restam, no entanto, são relacionadas à distribuição dos primos no conjunto dos números naturais. A frequência dos primos aumenta ou diminui conforme analisamos números maiores? Num esforço que começa com uma demonstração de Euler sobre a infinidade de primos, passa por um importante artigo de B. Riemann e se conclui no trabalho de vários matemáticos, em especial J. Hadamard, foi possível constatar que, definido $\pi(x)$ como a quantidade de primos menores ou iguais a um número natural x, então vale o limite

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

> Até o momento, não se conhece um algoritmo para fatoração de inteiros grandes, em um computador clássico, que funcione em tempo polinomial. (...) Portanto, para chaves suficientemente grandes, o RSA é seguro (...). O inteiro de 663 bits foi fatorado como parte do esforço de quebrar o RSA-200, um dos desafios RSA. (...) Este feito foi alcançado com um grande número de computadores, trabalhando de forma distribuída. Estima-se que um computador com processador de 2.2 Ghz levaria algo em torno de 75 anos para fatorar esse inteiro. Normalmente, são usadas chaves RSA de 1024 a 2048 bits, o que dá uma idéia da segurança que estes algoritmos oferecem. (FIGUEIREDO, 2009, p. 12)

O desafios são propostos pela própria empresa responsável pelo desenvolvimento do método, a RSA Laboratories, e consistem na fatoração de um número semiprimo (produto de dois primos distintos) fornecido pela companhia. O primeiro desafio fatorado foi o RSA-100 e o último foi o RSA-220, em 2016, consistindo de um número com 220 dígitos. O maior desafio é o RSA-2048, que consiste em um número de 617 dígitos, e o prêmio oferecido para que conseguir superá-lo é de $200.000,00 (FIGUEIREDO, 2009).

3 Metodologia Pedagógica

Resolver problemas encontrados no dia-a-dia é um dos fatores que impulsionam o desenvolvimento teórico da matemática. De acordo com os Parâmetros Curriculares Nacionais (BRASIL, 1997, p. 40) "a matemática do ensino médio (...) é uma ferramenta que serve para a vida cotidiana e para muitas tarefas específicas em quase todas as atividades humanas". Sendo assim, uma abordagem que tenha como foco problemas a serem resolvidos possui grande potencial no ensino da matemática.

Nas últimas décadas, a humanidade presenciou um enorme avanço tecnológico que influenciou diretamente a forma como lidamos com a informação. Se por um lado a internet permitiu um acesso jamais visto por parte da população aos mais diversos conteúdos, por outro possibilitou que qualquer um pudesse criar e divulgar conteúdo, o que sucedeu numa inevitável perda de controle sobre a qualidade do material disponível na rede.

Numa tentativa de possibilitar a exploração da internet em sala de aula, de modo fazer bom proveito do conteúdo e propiciar a conversão de informação em conhecimento, é proposto o formato de aula denominado *WebQuest*. De acordo com seu site oficial

> Uma *WebQuest* é um formato de lição em pesquisa orientada, no qual a maior parte ou toda a informação com a qual os estudantes trabalham vem da internet.[1]

A ideia foi desenvolvida pelo pesquisador Bernie Dodge, da San Diego State University, em 1995 e visa propiciar a construção do conhecimento em sala de aula de forma interativa, através da pesquisa orientada motivada, geralmente, por situações-problema. É uma abordagem construtivista, centrada no desenvolvimento da autonomia do aluno.

3.1 O formato de aula *WebQuest*

Na aplicação das atividades que serão descritas neste trabalho foi utilizado o formato *WebQuest*, que se organiza tendo como base as seguintes seções (exemplos seguem no apêndice A):

- **Introdução:** como o título sugere, aqui devem ser feitas algumas considerações históricas e teóricas preliminares acerca do tema a ser trabalhado. Uma possibilidade é introduzir o tema é através de um problema, como sugere a figura 5

[1] Livre tradução

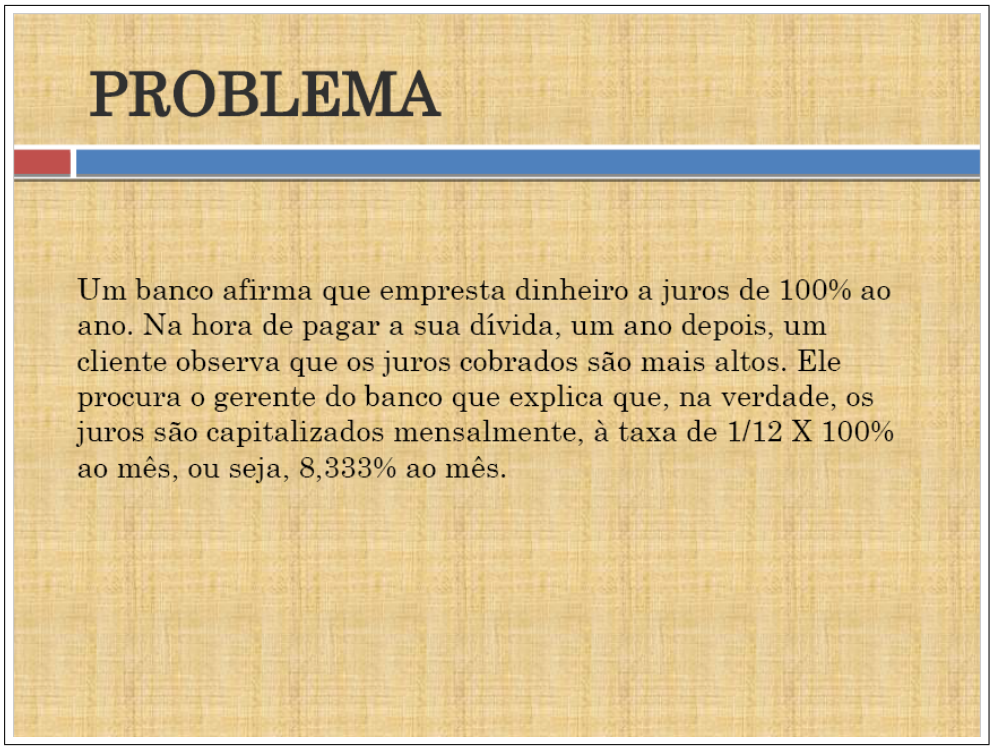


Figura 5 – Exemplo de problema introduzindo as atividades.

- **Tarefa:** aqui devem ser apresentadas as tarefas de modo sucinto e sequencial, como na figura 6.

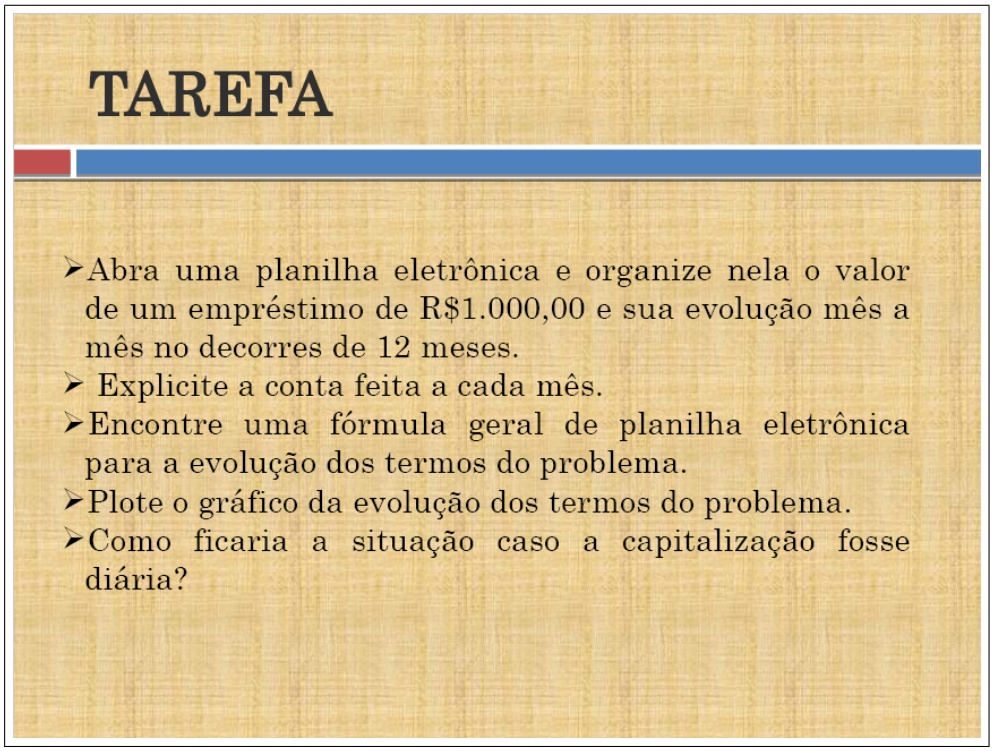


Figura 6 – Exemplo de tarefa em uma *WebQuest*.

- **Processo:** onde é proposto um roteiro rudimentar para a realização das atividades,

com dicas, elucidações e sugestão de recursos e fontes a serem utilizados, como na figura 7.

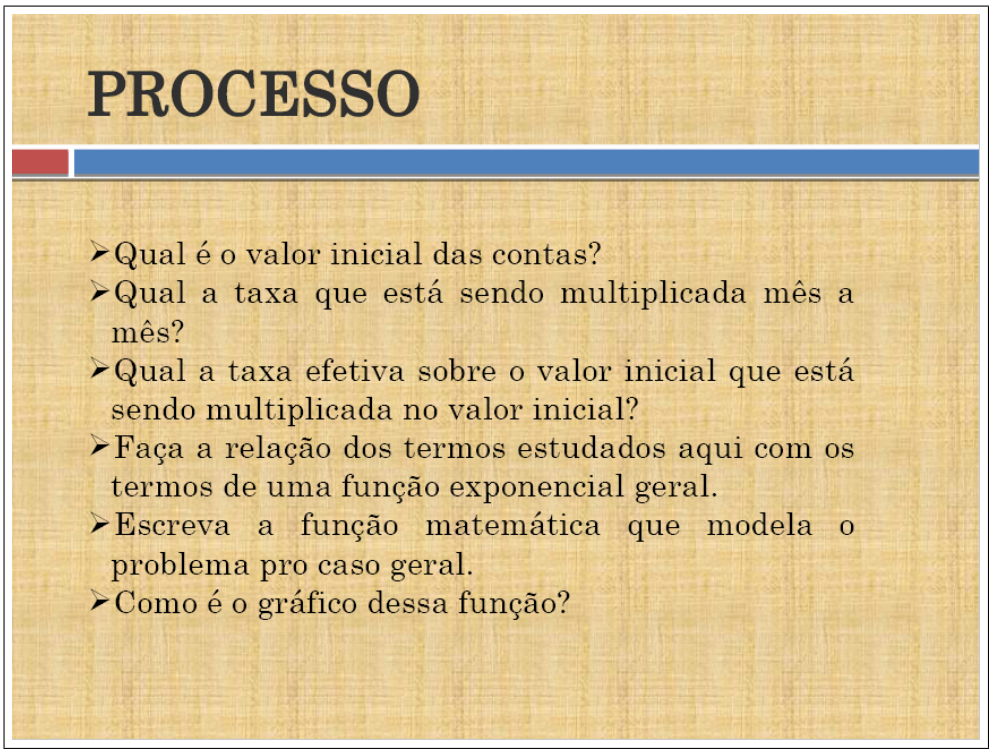


Figura 7 – Exemplo de processo em uma *WebQuest*.

- **Recursos:** onde são listadas as fontes e ferramentas utilizadas para a elaboração do projeto, uma espécie de bibliografia, como pode ser visto nas *WebQuests* em apêndice A.

- **Avaliação:** nesta seção devem ser apresentados os critérios de avaliação. O objetivo é fazer com que o aluno desenvolva a análise autocrítica, fazendo, ele mesmo, a primeira avaliação de seu projeto, como também pode ser visto nas *WebQuests* em apêndice A.

- **Conclusão:** aqui o professor deve levar o aluno à síntese final do que foi aprendido e fazê-lo refletir.

A organização em uma aula nesse formato é de suma importância, e é interessante notar que se confunde com as etapas para resolução de problemas apontadas por George Polya em sua obra *How to Solve It?*. Atividades do tipo devem ser "planejadas deliberadamente para fazer o melhor uso possível do tempo do aprendiz"(DODGE, 1995, p. 10). Uma vez que a internet entra em cena, instrumentos de controle para o aproveitamento intelectual do aluno devem ser elaborados para impedir que não haja dispersão parte da turma.

No artigo em que originalmente propõe a ferramenta, Bernie Dodge enumera a importância das etapas de criação da *WebQuest* reforçando o papel de uma introdução que atraia a atenção, uma atividade factível e interessante, um conjunto de fontes para o processo que seja confiável e forme um arcabouço teórico completo, uma descrição clara do processo utilizado para realizar as tarefas, dicas sobre recursos que auxiliem os alunos a organizar as informações adquiridas e, por fim, uma conclusão que dê sentido e sensação de completude à investigação proposta.

> As WebQuests têm a virtude da simplicidade. Podem ser desenvolvidas para alunos desde o ensino fundamental à pós-graduação. À medida em que mais e mais recursos aparecem na *World Wide Web*, será ainda mais fácil planejar atividades que engajem os aprendizes em investigações ativas e com bom uso do tempo disponível (DODGE, 1995, p. 13)

Tomou-se especial cuidado para criar situações que proporcionem ao aluno a oportunidade de aprender com a prática, em detrimento do que é feito em experiências como a do *Khan Academy*, que, muitas vezes, apenas transfere o ensino tradicional para o computador, contando, por exemplo, com vídeo-aulas meramente expositivas.

3.2 A Autonomia

O conflito de gerações que ocorre atualmente é notório. A geração presente nas salas de aula desde cedo é conhecedora da internet e enfrenta dificuldades em criar uma relação dialógica fluente com seus professores. Novas tecnologias chegam à sala de aula como uma revolução, rompendo diversos paradigmas educacionais e enfrentando forte resistência por parte dos professores. O computador traz consigo novas possibilidades pedagógicas e não deve ser encarado como algo estranho à realidade em sala de aula. Ele é inerente à realidade dos alunos e, portanto, deve ser também à prática docente. De acordo com Paulo Freire, "a aprendizagem da assunção do sujeito é incompatível com o treinamento pragmático ou com o elitismo autoritário dos que se pensam donos da verdade e do saber articulado"(FREIRE, 2005, p. 42), o que significa que participar da realidade em que os alunos estão inseridos é essencial para a prática docente.

Com base no *construtivismo*, a metodologia proposta neste trabalho visa incentivar os estudantes a interagirem com seus colegas, com o professor e com a internet tendo em vista a construção do conhecimento. A proposta preza pelo desenvolvimento da autonomia, a atitude pró-ativa na aquisição do conhecimento e pela a interação dentro de sala.

O uso da internet no ambiente escolar ainda gera controvérsias. A rede é rica de informações que precisam ser tratadas sob olhar crítico para que sejam transformadas em conhecimento, "para isso, habilidades como selecionar informações, analisar as informações obtidas e, a partir disso, tomar decisões, exigirão linguagem, procedimentos e formas de

pensar matemáticos que devem ser desenvolvidos ao longo do Ensino Médio"(BRASIL, 1997, p. 41). A *WebQuest* tem se mostrado uma ferramenta eficaz para dar sentido e objetividade à pesquisa na internet e, para isso, se faz valer, de forma orientada, dos recursos disponíveis na própria *web*, ajudando no desenvolvimento do pensamento crítico e investigativo dos alunos. Sobre isso os PCNs dizem o seguinte:

> Esse impacto da tecnologia, cujo instrumento mais relevante é hoje o computador, exigirá do ensino de Matemática um redirecionamento sob uma perspectiva curricular que favoreça o desenvolvimento de habilidades e procedimentos com os quais o indivíduo possa se reconhecer e se orientar nesse mundo do conhecimento em constante movimento.

É necessário que haja esforço para que a aprendizagem se dê de forma condizente com o dinamismo da informação. Mais especificamente, para que o aluno consiga lidar com esse fenômeno, é necessário que sua autonomia seja desenvolvida. De acordo com (MORTIMER, 1996, p. 22), "a aprendizagem se dá através do ativo envolvimento do aprendiz na construção do conhecimento". Nesse sentido as *WebQuests* são pensadas de forma que a construção dos conceitos relativos ao problema apresentado crie a necessidade do desenvolvimento teórico matemático por parte dos alunos, com o aprendizado e a aplicação ocorrendo simultaneamente, o que propicia o desenvolvimento da autonomia do estudante. Sobre isso, os PCNs dizem que

> A resolução de problemas é peça central para o ensino de Matemática, pois o pensar e o fazer se mobilizam e se desenvolvem quando o indivíduo está engajado ativamente no enfrentamento de desafios. Essa competência não se desenvolve quando propomos apenas exercícios de aplicação dos conceitos e técnicas matemáticos, pois, neste caso, o que está em ação é uma simples transposição analógica: o aluno busca na memória um exercício semelhante e desenvolve passos análogos aos daquela situação, o que não garante que seja capaz de utilizar seus conhecimentos em situações diferentes ou mais complexas.

Kant acreditava que "a educação não deve ser puramente mecânica e nem se fundar no raciocínio puro, mas deve apoiar-se em princípios e guiar-se pela experiência", e que "a criança não deve ser um imitador cego, sob a pena de que jamais seja um homem ilustrado e de mente serena", como cita (ZATTI, 2007, p. 31 e 34). É sabido que alunos diferentes aprendem de formas diferentes, e num mundo em constante mudança, o aluno precisa, antes de mais nada, aprender a aprender, a revisitar e rever seus conceitos. Em suma, é necessário que o aluno saia de sala sem precisar do professor para que possa continuar seu aprendizado e usufruírem do que foi aprendido.

É importante frisar que nem sempre a intuição do aluno será suficiente para sua aprendizagem, podendo ficar a cargo do docente forçar a conversão dessa intuição em conhecimento científico. "Aprender ciências envolve um processo de socialização das práticas da comunidade científica e de suas formas particulares de pensar e de ver o mundo"

(MORTIMER, 1996, p. 24), e esse processo pode não ocorrer de forma totalmente natural. Seguindo este mote, (FREIRE, 2005, p. 27) diz que, em relação ao docente, "faz parte de sua tarefa não apenas ensinar os conteúdos mas também ensinar a pensar certo". Unindo esse raciocínio com o tema das *WebQuests*, podemos citar (FREIRE, 2005, p. 37) quando diz que "não há (...) pensar sem entendimento e o entendimento, do ponto de vista do pensar certo, não é transferido mas co-participado".

Ainda segundo (FREIRE, 2005, p. 22 e 24), "ensinar não é transferir conhecimento, mas criar as possibilidades para sua produção ou a sua construção". Mais adiante, ele continua dizendo que "inexiste validade no ensino de que resulta um aprendizado em que o aprendiz não se tornou capaz de recriar ou de refazer o ensinado, em que o ensinado que não foi apreendido não pode ser realmente aprendido pelo aprendiz". Nesse sentido, a *WebQuest* abre mão de exercícios repetitivos como forma de aprendizado. É feita uma inversão de ordem. Ao contrário da maioria dos livros didáticos, onde as aplicações costumam aparecer após os conceitos serem sedimentados através de exercícios mecânicos, no intuito de verificar o aprendizado, o proposto aqui é que as aplicações sirvam como paradigma básico de aprendizado, como sugere os Parâmetros Curriculares Nacionais do Ensino Médio, quando fala do ensino de funções:

> Os problemas de aplicação não devem ser deixados para o final desse estudo, mas devem ser motivo e contextos para o aluno aprender "funções". A riqueza de situações envolvendo "funções" permite que o ensino se estruture permeado de exemplos do cotidiano, das formas gráficas que a mídia e outras áreas do conhecimento utilizam para descrever fenômenos de dependência entre grandezas.

Exercícios mecânicos e repetitivos, no entanto, possuem seu valor dentro da matemática e não devem ser ignorados "pois eles cumprem a função do aprendizado de técnicas e propriedades, mas de forma alguma são suficientes para preparar os alunos"(BRASIL, 1999, p. 113). O que se deseja é que os exercícios não sirvam de paradigma para o ensino, mas para exercitar o conhecimento adquirido. Uma abordagem centrada unicamente nesses exercícios gera consequências que vão além da escola e acompanha o aluno por toda sua vida.

> Na escola, os encaminhamentos aritméticos e algébricos perpassam, em maioria, problemas estáticos: contas, medições, equações, análise de dados. Mesmo o ensino de funções, que tem início no final do Ensino Fundamental, segue uma abordagem mais substantiva, que meramente expõe a forma dos gráficos e a interpretação de alguns coeficientes. Raros são os momentos em que se destacam processos de modelagem, nos quais as variações das funções são consideradas de forma central. Esse, sim, é um dos pontos problemáticos do nosso Ensino Médio. Em um curso de cálculo, o foco deve se dar sobre a matematização, a análise e a síntese das relações variacionais. (MOTTA, 2014, p. 4)

Além disso, métodos de aprendizagem que envolvem muita liberdade, mais especificamente abordagens construtivistas, podem demandar muito tempo em sala de aula.

> A aplicação dessas estratégias em sala de aula tem resultado numa relação de custo-benefício altamente desfavorável. Gasta-se muito tempo com poucos conceitos, e muitas vezes esse processo não resulta na construção de conceitos científicos, mas na reafirmação do pensamento de senso-comum. A prática de sala de aula contribui para o aumento da consciência do estudante sobre suas concepções mas não consegue dar o salto esperado em direção aos conceitos científicos. (MORTIMER, 1996, p. 24)

Desse modo, as *WebQuests* adquirem o papel de ajudar o professor tanto a desenvolver como a disciplinar e focar a autonomia de seus alunos, ponto importante no aprendizado. De acordo com (ZATTI, 2007, p. 33), Kant defendia que a disciplina é importante "para que o homem aprenda a guiar sua vontade pela razão e assim possa ser autônomo".

3.3 Competências e Habilidades

Os PCNs do ensino médio classificam em três categorias as competências a serem desenvolvidas nessa etapa da educação básica. São elas

- representação e comunicação, que envolvem a leitura, a interpretação e a produção de textos nas diversas linguagens e formas textuais características dessa área do conhecimento;
- investigação e compreensão, competência marcada pela capacidade de enfrentamento e resolução de situações-problema, utilização dos conceitos e procedimentos peculiares do fazer e pensar das ciências;
- contextualização das ciências no âmbito sócio-cultural, na forma de análise crítica das ideias e dos recursos da área e das questões do mundo que podem ser respondidas ou transformadas por meio do pensar e do conhecimento científico.

Já de acordo com (BRASIL, 1999, p. 113) "(...) a escola que tem como objetivo preparar o aluno para um aprendizado permanente e prepará-lo para a vida precisa refletir sobre o significado dessas competências para decidir sobre quais delas trabalhar". Seguindo esse mote, as atividades apresentadas aqui são construídas de modo a trabalhar, principalmente, os seguintes pontos:

- **Investigação e compreensão**:

  - Reconhecer, utilizar, interpretar e propor modelos para situações-problema, fenômenos ou sistemas naturais ou tecnológicos.

- **Contextualização sociocultural:**

  - Compreender o conhecimento científico e o tecnológico como resultados de um construção humana, inseridos em um processo histórico e social;
  - compreender a ciência e a tecnologia como partes integrantes da cultura humana contemporânea.

4 Descrição de Atividade

Neste capítulo descreveremos as atividades propostas, o público escolhido para a aplicação e o formato das *WebQuests*, fatores determinantes da pesquisa desenvolvida.

4.1 Identificação do Público

Participaram da atividade 37 jovens de 15 a 18 anos de idade, do primeiro (24 alunos) e terceiro (13 alunos) anos do ensino médio, matriculados nos cursos técnicos de informática, ambos na modalidade integrados com o ensino médio, do Instituto Federal de Educação, Ciência e Tecnologia Fluminense (IFF), *campus* Quissamã. Houve, ainda, experiências preliminares em dois momentos anteriores, um informal e outro na disciplina Criptografia, mas que não serviram de base para os apontamentos aqui feitos.

Os estudantes do IFF provém, em grande parte, de zonas rurais e comunidades humildes. Por isso mesmo, possuem um perfil definido pela curiosidade e pensamento crítico, o que pode ser justificado pelo fato de muitos enxergarem o IFF como forma de ascensão social. Simultaneamente, este mesmo público provém, largamente, do ensino público municipal e estadual, o que pode significar que alguns apresentam lacunas em conteúdos básicos. Apesar de gerar um desafio na tarefa docente, esse fato não deve ser tratado como um fator limitador no processo de ensino-aprendizagem.

4.2 Ações Didáticas

A ações consistiram em 4 atividades, com duração de 4 aulas de 50 minutos cada, aplicadas no laboratório de informática no último bimestre do ano letivo de 2015 nas aulas de Matemática. Cada aluno tinha um computador a sua disposição.

Como já mencionado, os assuntos abordaram foram:

- contagem;
- matrizes;
- funções;
- MMC e MDC.

A utilização de planilhas eletrônicas e recursos computacionais diversos é peça fundamental tanto na tarefa de dar aplicabilidade aos conceitos matemáticos, como para aproximá-los do cotidiano e do interesse dos alunos, que podem utilizar esses conhecimentos extraclasse em suas vidas pós-escolares.

Cabe ao professor introduzir a filosofia da abordagem aos alunos, bem como instigar a curiosidade dos alunos desde o primeiro momento. Para isso foi tirado proveito da exibição do filme "O Jogo da Imitação", de Morten Tyldum.

4.3 *WebQuests*

O formato *WebQuest*, organizado em *slides*, foi utilizado em todas as atividades, o que significa que compartilham diversas características bem definidas e que já foram explicadas no capítulo 3. Destacaremos os fatores mais relevantes das atividades desenvolvidas, que constam integralmente no apêndice A.

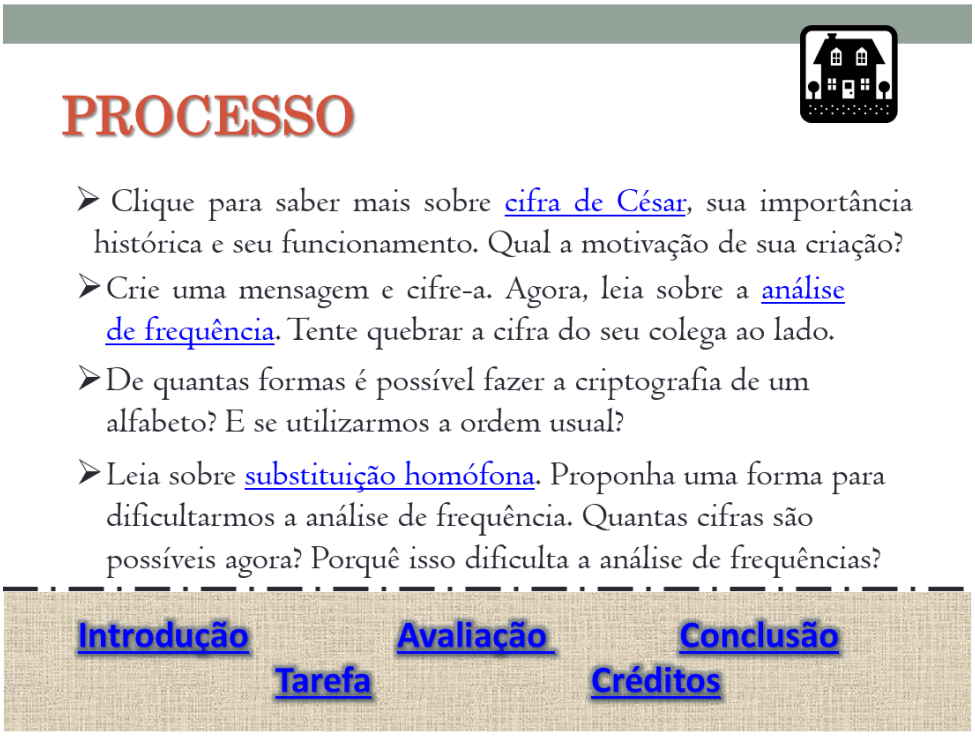
4.3.1 Atividade 1

Esta *WebQuest* introduz os primeiros conceitos de contagem através da discussão da segurança das cifras de substituição.

A cifra de César é quase inteiramente baseada na matemática do ensino fundamental, o que possibilita sua aplicação imediata pelos alunos. É proposto o desafio de cifrar uma mensagem e decifrar a mensagem do colega. Para tanto, o aluno é instigado a explorar o conceito de análise de frequência de letras, e, naturalmente, entender alguns conceitos de estatística, utilizando diversas ferramentas disponíveis na internet.

Uma vez que mensagens são decifradas, cabe ao aluno entender o motivo de haver poucas chaves possíveis para o método criptográfico estudado. Conceitos de contagem se mostram necessários e são motivados, tanto através da reflexão, como através da pesquisa feita. O aluno deve ser capaz de identificar o problema de segurança da cifra de César devido à permanência da ordem das letras.

(a) Atividades propostas



(b) Processo envolvido na atividade

Figura 8 – *WebQuest*: Cifra de Substituição

Por fim, com base no que foi aprendido, o aluno deverá dar sugestões de como diminuir a possibilidade da criptoanálise da cifra através do conceito de *desordenamento*, que se refere a cifras de substituição que não preservam a ordem entre as letras. Apesar

de dificultar o ataque por força bruta, é importante que o aluno aprenda que essas cifras permanecem vulneráveis a ataques de análise de frequência de letras.

4.3.2 Atividade 2

A *WebQuest* acerca da cifra de Hill aborda a aritmética das matrizes. São exploradas as operações básicas entre matrizes, incluindo o conceito de matrizes inversas. Sua realização pressupõe apenas o conhecimento das quatro operações entre números naturais e deve se dar, preferencialmente, após o estudo das cifras de substituição.

O processo da atividade (figura 9) tenta induzir os alunos a conceberem a ideia de criar "blocos" de números. Nesse momento apresenta-se a cifra de Hill, os alunos pesquisam e a implementam num *software* de planilha eletrônica.

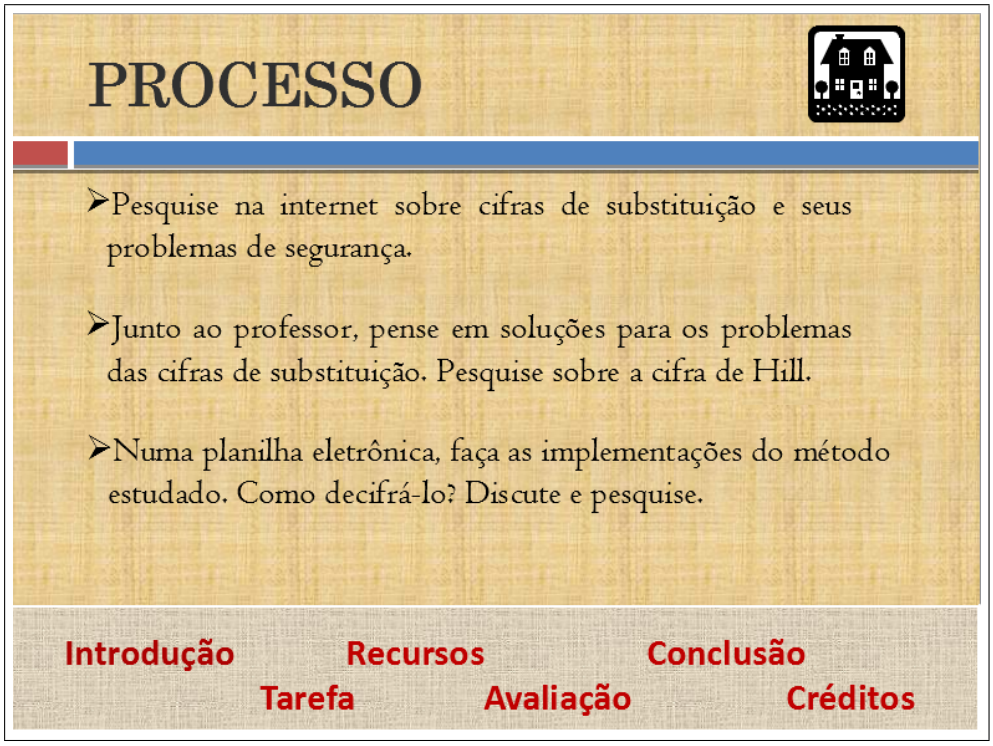


Figura 9 – Na própria Web Quest havia as fontes a serem consultadas pelo alunos.

Durante a implementação do método, todas as operações aritméticas entre matrizes são postas em prática no computador (figura 10). Isso permite que os alunos tenham contato com a soma e multiplicação de matrizes, antes mesmo de serem definidas. O professor deve, então, tirar proveito da situação e instigar a curiosidade dos alunos para a formalização da teoria sobre a aritmética entre matrizes, o que possibilita a conversão das informações coletadas em conhecimento e expõe o diálogo entre teoria e aplicação. O erro deve ser valorizado e servir de motivação da construção conceitual do conhecimento matemático.

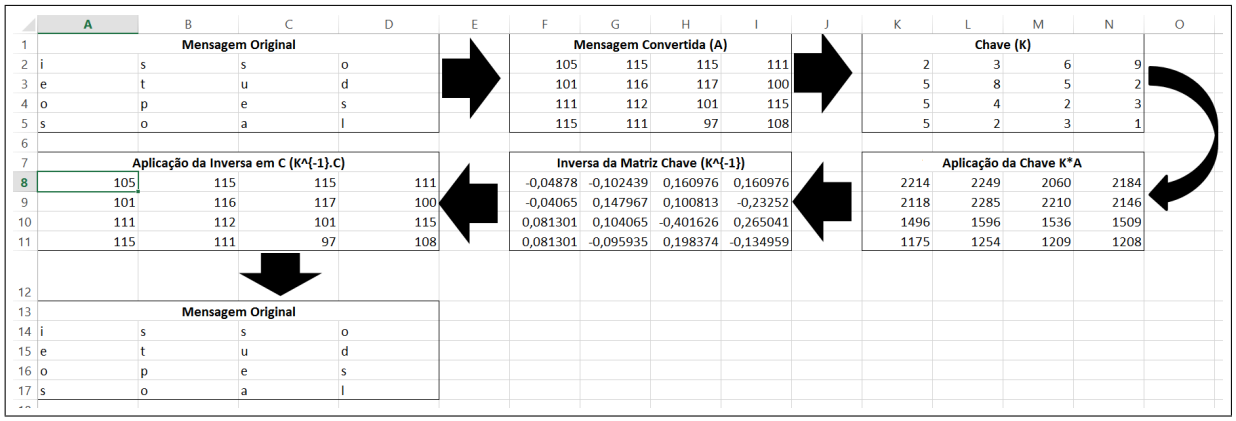


Figura 10 – Processo realizado pelos alunos na atividade de cifragem e decifração de mensagem.

O mesmo deve ocorrer no momento da decifragem. O espírito de competitividade pode ser explorado para que, seguindo o mote de querer quebrar o código do colega, os alunos se motivem a explorar o conceito de matrizes inversas.

O *software* de planilha eletrônica cria a possibilidade de serem feitas manipulações no algoritmo original da cifra de Hill, tais como aplicação repetida da chave, ou aplicá-la na forma de soma ao invés de multiplicação.

4.3.3 Atividade 3

A *WebQuest* que tratou do conceito de cifra assimétrica aproveitou a problematização do assunto para motivar a discussão sobre inversão das funções estudadas no ensino médio. Dada uma função f, podemos pensa-la como a chave pública, enquanto que sua inversa, f^{-1}, seria a chave privada.

O processo de cifragem não traz muitas novidades à turma, mas o processo de decifragem propicia um bom momento para se discutir a existência de função inversa e, consequentemente, domínio, imagem e propriedades de funções injetoras, sobrejetoras e bijetoras. Inicialmente, é estudado o caso da inversão da função afim, seguido de outros casos, como, por exemplo, o da função quadrática, que, por não ser bijetora, introduz discussões sobre restrições no domínio.

O desenvolvimento da aula é centrado no desafio entre os estudantes, que devem criar funções com inversas mais difíceis de serem encontradas, motivado pela dinâmica entre cifragem e decifragem.

4.3.4 Atividade 4

A cifra RSA pode ser trabalhada de modo que precise de poucos pré-requisitos, mesmo que seu pleno funcionamento exija um conhecimento em teoria dos números

que foge ao escopo do ensino médio. Particularmente, essa atividade se firma como um estudo do algoritmo do método RSA, no intuito de dar uma demonstração mais ampla de como conceitos matemáticos simples surgem em aplicações tecnológicas avançadas. Essa abordagem se motivou, também, pela constatação do fato de algumas das ideias envolvidas nesse assunto não condizem com o nível de conhecimento de alunos do ensino médio e fundamental.

A introdução da tarefa já frisa o mote de integrar a matemática básica à tecnologia de ponta, seguindo a orientação de (BRASIL, 1999, p. 119) que aponta, sobre a matemática, que,

> (...) os temas selecionados devem ter relevância científica e cultural. Isso significa que, além das justificativas relativas às aplicações e à linguagem, sua importância está em seu potencial explicativo, que permite ao aluno conhecer o mundo e desenvolver sentidos estéticos e éticos em relação a fatos e questões desse mundo.

A tarefa (figura 11) faz com que os alunos se depararem com conceitos de MMC e MDC já vistos no ensino fundamental por meio do estudo direto do algoritmo do método. É uma oportunidade de rever e mostrar novas aplicabilidades. O processo (figura 12) consta de uma bibliografia preparada (que se encontra na reprodução da *WebQuest* no apêndice A) com enfoque no desenvolvimento dos conceitos de MMC e MDC envolvidos no RSA, para que os alunos tenham uma descrição mais intuitiva e simples do método. Além disso, por não se tratar de um método trivial do ponto de vista conceitual, muitas dúvidas surgem e instruções pontuais sobre a funcionalidade do método por parte do professor se fazem indispensáveis.

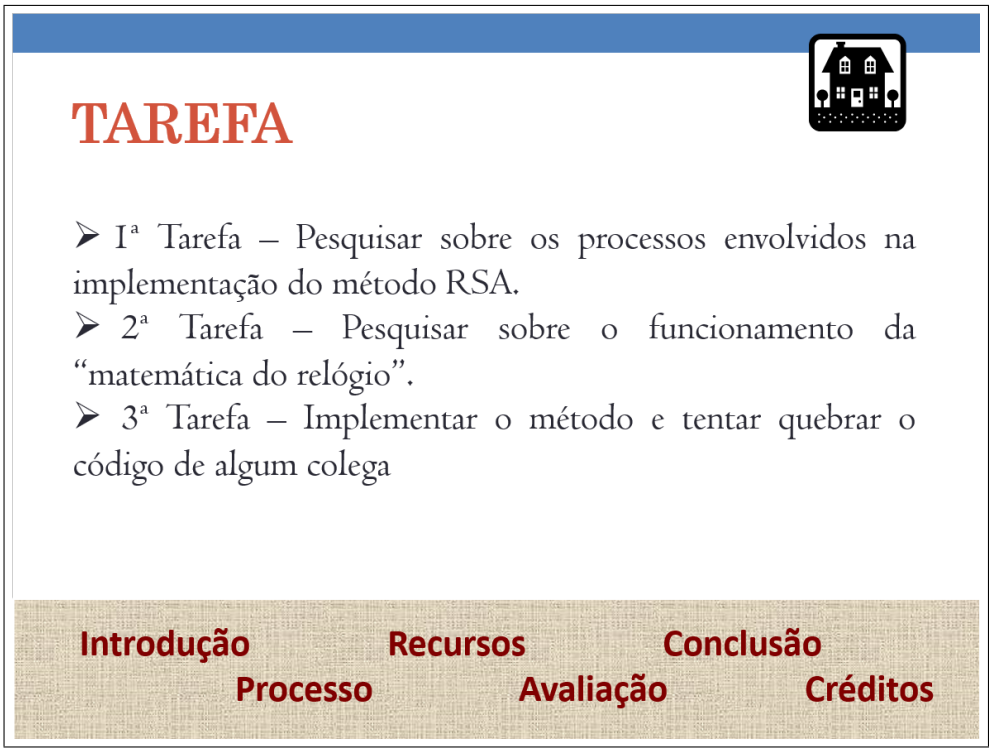


Figura 11 – Tarefas da *WebQuest* sobre o método RSA

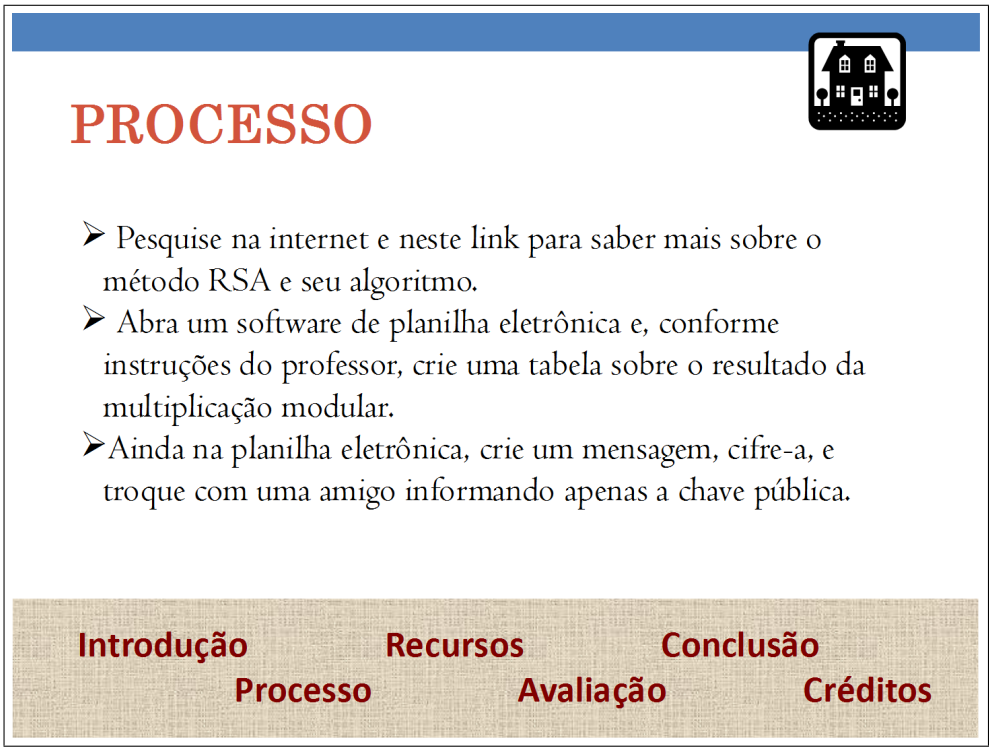
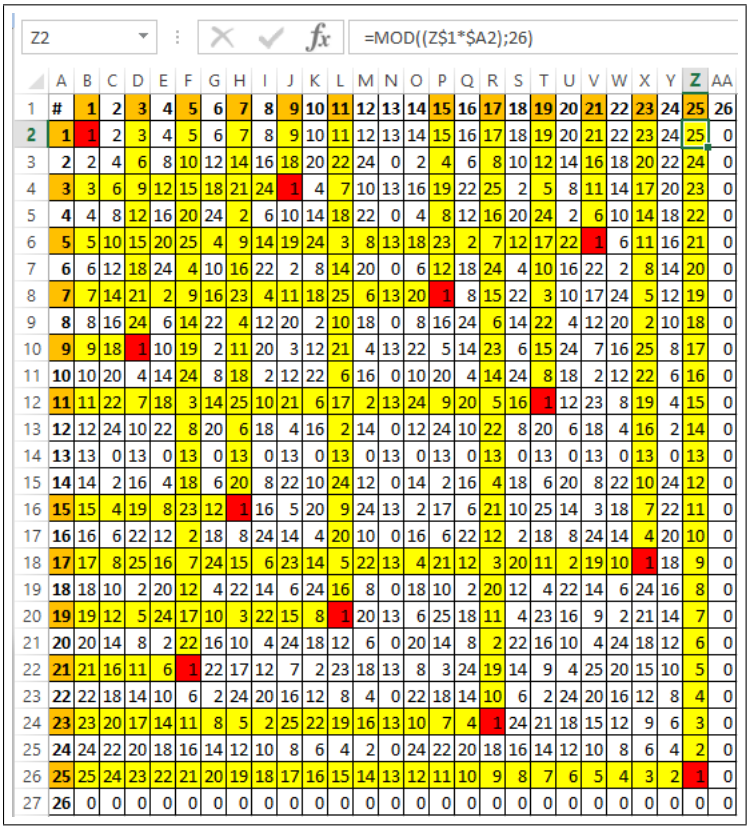


Figura 12 – Processo proposto

Conceitos avançados não devem ser evitados, mas abordados de forma cuidadosa, favorecendo a intuição sobre a formalidade. É o caso do inverso de um número de acordo com o módulo m, $m \in \mathbb{N}$, conceito envolvido na decifragem do método. Recursos computacionais

são utilizados para que a aritmética entre classes de congruência seja intuída e melhor entendida. Em particular, conforme proposto em (GOMES, 2014), a utilização de uma planilha eletrônica como mostrado na figura 13 é capaz de explicitar o comportamento periódico e facilitar o entendimento do conceito.



	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	AA
1	#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
3	2	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24	0
4	3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0
5	4	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22	0
6	5	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0
7	6	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20	0
8	7	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0
9	8	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0
10	9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	0
11	10	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16	0
12	11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	0
13	12	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14	0
14	13	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0
15	14	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12	0
16	15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	0
17	16	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10	0
18	17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	0
19	18	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8	0
20	19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	0
21	20	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6	0
22	21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	0
23	22	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4	0
24	23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	0
25	24	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2	0
26	25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
27	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figura 13 – Modelo proposto para entendimento do inverso multiplicativo da aritmética modular:o número da linha e coluna dos 1's são inversos multiplicativos módulo 26.

Nessa atividade em particular, por não ser motivada por conteúdos apresentados no ensino médio, mas pela percepção da presença de conteúdos básicos da matemática na tecnologia de ponta, a conclusão ganha destaque e reforçasse a necessidade de que seja escrita pelos alunos. Deve ser avaliado se cada estudante foi capaz de capturar a importância crucial da matemática para o desenvolvimento tecnológico, em especial a reinterpretação e valorização de alguns assuntos do ensino fundamental, como MDC e MMC, que são, muitas vezes, mal compreendidos.

5 Resultados e discussões

A princípio, a ideia de estudar matemática sem partir da exposição teórica criou certo estranhamento por parte dos alunos, com alguns manifestando desconfiança e descontentamento ao sair da rotina tradicional. Em contrapartida, outros gostaram da proposta e encararam como um desafio. O tema criptografia traz consigo uma carga imaginária que gera grande curiosidade e interesse entre os alunos, em especial de informática.

O formato de aula em *WebQuest* gerou dúvidas, especialmente por ter sido apresentado através de *slides*, que habitualmente são utilizados apenas na exposição do conteúdo. Os alunos demoraram alguns minutos para compreender a abordagem, fato indicado pelas constantes dúvidas de teor operacional, e coube ao professor fazer parte do trabalho a que a *WebQuest* se propunha.

Por parte do professor, é importante não expor o conteúdo de forma clássica, mesmo quando os alunos demonstram dificuldades. Formalizar a teoria estudada precocemente pode inviabilizar a possibilidade de fazer com que os estudantes consigam lidar com suas próprias dificuldades. Optou-se por estimular o diálogo nos momentos de dúvidas, de modo que, com a contribuição do entendimento de cada um, a turma fosse capaz de construir a compreensão do conteúdo por completo.

Entretanto, houve momentos em que foi necessário facilitar o processo ensino-aprendizagem, e numa abordagem deste tipo não é trivial encontrar a medida certa dessa influência. Apesar do livre acesso à internet, redes sociais, mesmo sendo acessadas, não mostraram grande empecilho na abordagem. Quando os resultados e as informações procuradas pelo aluno fugiram do esperado, o foco e sensação de continuidade da construção do conhecimento precisaram ser mantidos pela ação externa do docente.

A apresentação de problemas como paradigma central para a construção do conhecimento traz consigo a ideia de que os alunos são capazes de, a partir de problematizações apresentadas pelas *WebQuests* e pelo professor, pesquisar, discutir e aprender os conceitos necessários autonomamente e motivar a necessidade da formalização teórica do conteúdo estudado em momento subsequente. Essa perspectiva, no entanto, por não corresponder ao tradicional, criou efeito controverso nas turmas. Muitos alunos demonstraram vontade de desistir antes de começar as atividades, sentindo falta de um arcabouço teórico *a priori*.

As impressões imediatas ao fim das atividades foram otimistas, com a animosidade inicial superada. Muitos alunos mostraram empolgação com o assunto criptografia. Evidências disso foram a diminuição significativa de ausências em sala de aula e questiona-

mentos que iam além dos conteúdos do currículo básico do ensino médio, como polinômios interpoladores de Lagrange, curiosidade que surgiu quando o estudo de funções foi abordado e física quântica, tema levantado quando citado o estágio atual de desenvolvimento da criptografia.

O desenvolvimento teórico da criptografia deu sentido à construção conceitual dos conteúdos trabalhados. A utilização de planilhas eletrônicas e ambientes computacionais fez com que houvesse uma conversação constante entre teoria e prática, com os alunos frequentemente assumindo, espontaneamente ou em resposta a estímulos das problematizações da *WebQuest* ou do professor, uma postura crítica em relação ao computador, querendo saber, por exemplo, o que havia por traz das fórmulas dos *softwares* de planilha eletrônica.

Foi aplicado um questionário (que se encontra no Apêndice B deste trabalho) antes e outro após a aplicação das *WebQuests* que no texto designaremos por primeiro e segundo questionário. 32 responderam ao primeiro e 26 ao segundo. No segundo questionário incluiu-se mais duas perguntas acerca das impressões que os alunos tiveram com a experiência. Antes da aplicação do questionário foi explicado a diferença entre problemas e exercícios.

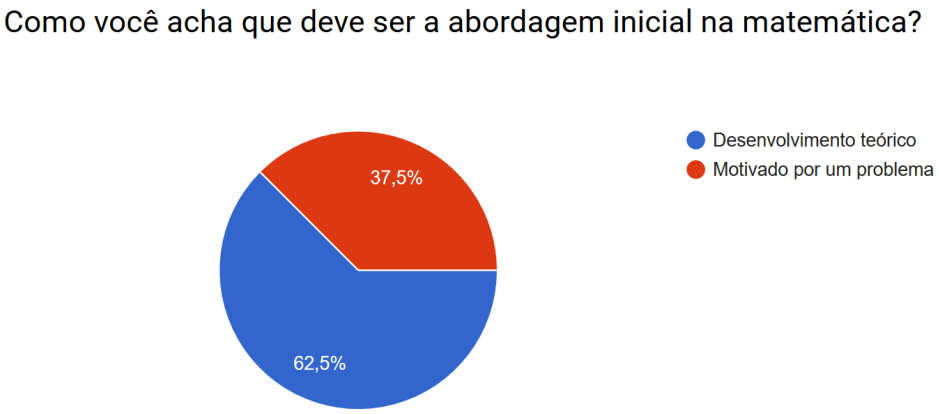
Quanto à utilização de tecnologias (figura 14), 50% dos alunos afirmaram nunca ter tido professores de matemática que utilizassem tais ferramentas. Após as atividades, os alunos mudaram de opinião e esse número cresceu para 76%. Houve uma mudança, para os alunos, do significado do uso de ferramentas tecnológicas em sala de aula. Antes limitava-se a exposição do conteúdo através de *slides*, criação de textos digitados no computador, vídeo-aulas e criação de tabelas estáticas em planilhas eletrônicas - de certa maneira um uso passivo do computador. O computador não era visto como um instrumento de experimentação.

(a) Primeira aplicação

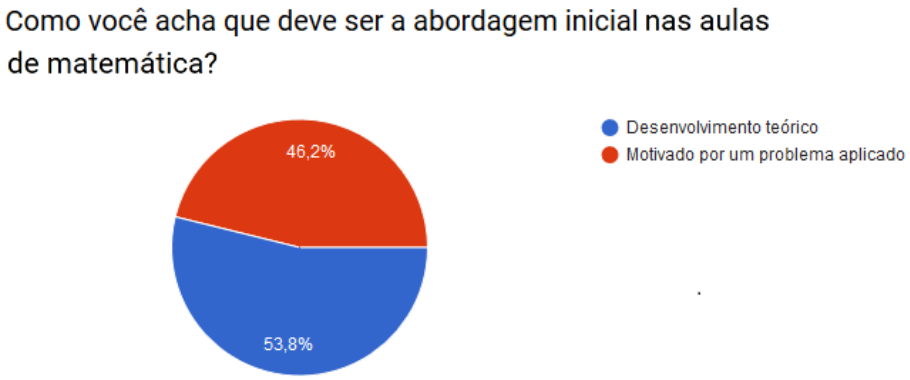
(b) Segunda aplicação

Figura 14 – Comparação entre a quantidade de alunos que afirmavam já ter experienciado uso de tecnologias educacionais antes e depois das atividades propostas.

Sobre como deve ser **a abordagem inicial de um conteúdo**, não houve diferença significativa em relação às respostas antes e depois da atividade ser aplicada. 62,5% (antes) contra 53,8% (depois) demonstraram acreditar que primeiramente a teoria deve ser desenvolvida e 37,5% (antes) contra 46,2% (depois) preferiram uma motivação inicial através da problematização. Pode-se especular que a explicação seja devida à possibilidade dos alunos se sentirem inseguros em abordagens que proponham experimentações baseadas na intuição antes da formalização teórica.



(a) Primeira aplicação



(b) Segunda aplicação

Figura 15 – A teoria como abordagem inicial teve um declínio de 10% dentre os alunos entrevistados.

Antes das atividades serem desenvolvidas, quando perguntados sobre **o que mais chama a atenção** nas aulas de matemática (figura 16), a maioria dos alunos respondeu que os problemas eram a parte mais interessante (43,8%), seguido dos exercícios de repetição (31,3%) e por último ficou o desenvolvimento teórico (25%).

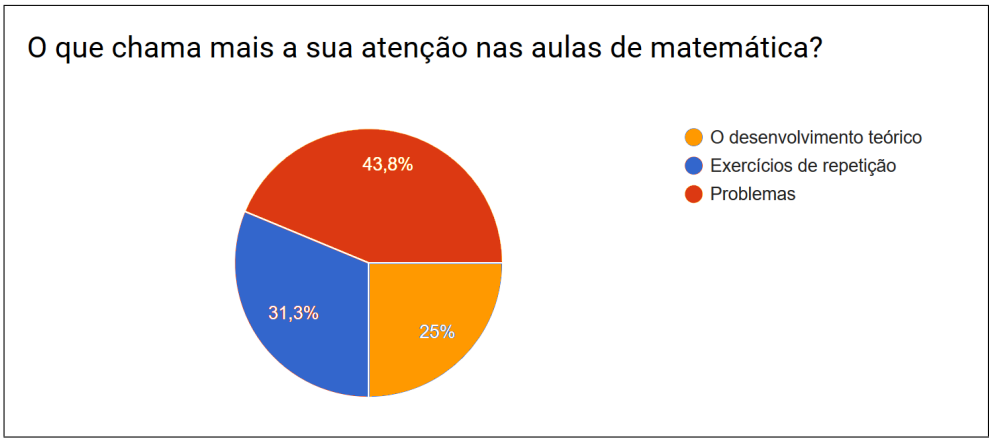


Figura 16 – Maior parte dos alunos acredita que os problemas são a parte mais atrativa nas aulas de matemática.

Os resultados foram similares quando lhes foi perguntado sobre o que **os ajuda mais a entender** os conceitos de matemática. A maioria acha que o aprendizado se dá através da resolução de problemas (40,6%), seguido pela resolução de exercícios repetitivos (37,5%). Os alunos constatam que não se aprende matemática passivamente.

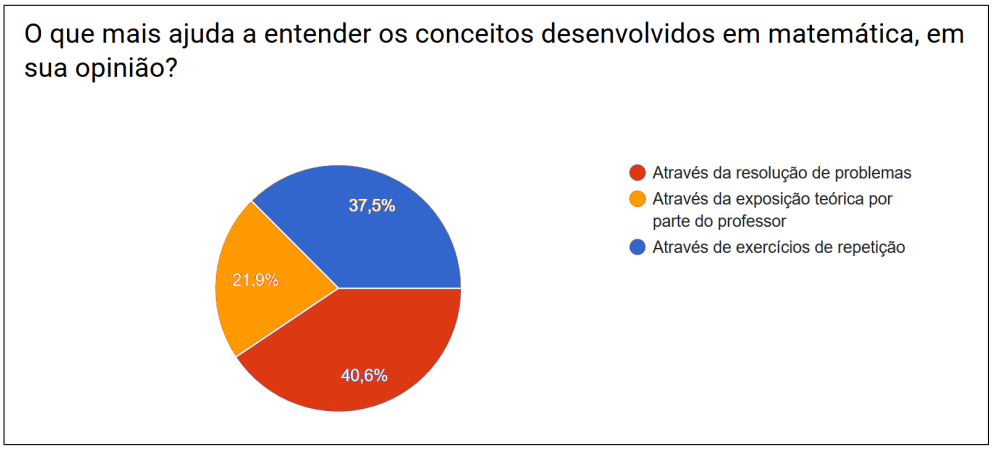


Figura 17 – Envolvimento ativo dos alunos é visto como primordial como paradigma ensino-aprendizagem.

Após a aplicação da atividade houve um aumento significativo em relação ao interesse em exercícios repetitivos. 61,5% dos alunos disse que a parte que **mais chama a atenção** nas aulas de matemática são exercícios que repetem procedimentos e 23,1% os problemas aplicados. 65,4% dizem que o que **os ajuda mais a entender** os conceitos desenvolvidos em sala de aula são exercícios procedimentais repetitivos, enquanto que apenas 19,2% dão esse crédito à resolução de problemas, como mostram os gráficos da imagem 18. Este resultado, embora surpreendente, explica-se pelo da abordagem ter motivado os alunos a fazer exercícios repetitivos - afinal os exercícios se tornam interessantes após os alunos descobrirem reais aplicações.

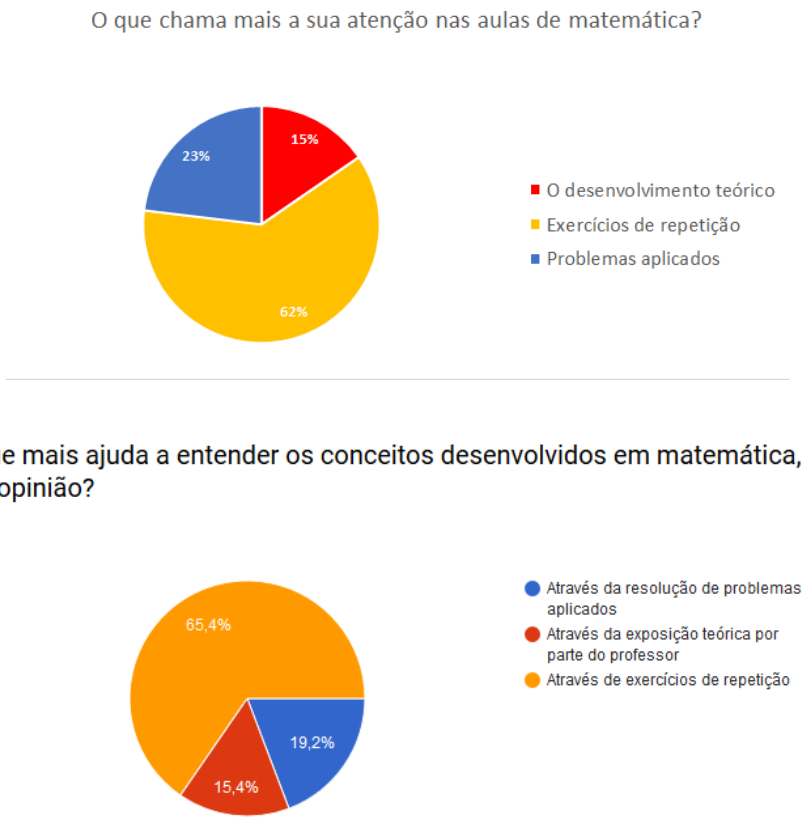


Figura 18 – Os exercícios de repetição ainda representam parte importante na aprendizagem de matemática.

No segundo questionário, quando perguntados sobre qual o papel que a resolução de problemas apresentados na forma de *WebQuest* deve desempenhar, 61,5% dos entrevistados opinaram que deveria servir como paradigma para o desenvolvimento teórico, enquanto que 38,5% acredita que os problemas deveriam apenas ilustrar a teoria aprendida e 0% responderam que o desenvolvimento puramente teórico se basta em si. O que corrobora a tese de que a atividade foi bem sucedida em problematizar o conteúdo e motivar a apresentação teórica e prática de exercícios repetitivos.

No primeiro questionário 84,4% dos alunos responderam que a tecnologia é uma ferramenta útil ao ensino e 59,4% acham que a tecnologia deve desempenhar papel ativo na aprendizagem. No segundo questionário esses números passaram para 100%. Além disso, no segundo questionário, 100% dos alunos deram preferência a aulas no laboratório de informática, explorando recursos computacionais e resolvendo problemas como motivação para que a teoria seja desenvolvida. Esses dados apontam para uma perspectiva de sucesso da atividade.

Reconhecemos a importância da formalização teórica e dos exercícios repetitivos na aprendizagem de conceitos da matemática. A abordagem proposta não pretende contestar

isso, e, pelo contrário, ao motivar a prática através do lúdico e ao criar a necessidade do emprego de conceitos matemáticos, incentiva o estudo teórico e a prática regular das técnicas aprendidas.

Foi observado ainda haver insegurança por parte dos alunos, o que podemos atribuir desde à ordem teoria-exercícios ser o *modus operandi* do ensino de matemática por anos, o que é reforçado pelo fato que de que 76,9% dos alunos não terem experimentado qualquer tipo de abordagem parecida em precedente, até possíveis falhas na condução das atividades por parte do professor, e mesmo uma limitação no entendimento do cenário completo por parte dos instrumentos de medição empregados. Além disso, os resultados reafirmam a tese elaborada inicialmente de que, apesar de ainda haver o problema supracitado, os alunos reconhecem a necessidade de uma abordagem com enfase na aplicação dos conceitos estudados, da geração da autonomia e da participação direta em seu processo de construção da aprendizagem.

Considerações Finais

O objetivo desse trabalho foi utilizar a criptografia como motivação e forma de problematização de temas do currículo de matemática do ensino fundamental e médio, tais como, funções, matrizes, matemática combinatória, MMC e MDC. Buscou-se utilizar desde métodos criptográficos antigos, como a cifra de César, até um dos mais populares atualmente, o RSA.

Foi escolhido o formato *WebQuest* de modo a reforçar o caráter investigativo das atividades. Evitou-se trilhar o caminho mais popular do uso de tecnologia em sala de aula, como uma ilustração dos assuntos abordados, ou como reprodução do que já é tradicionalmente feito, através de videoaulas. Procurou-se reforçar a autonomia dos alunos, romper com os paradigmas tradicionais e centrar a educação na descoberta e exploração.

A abordagem proposta foi bem sucedida. O uso de tecnologias e resolução de problemas através do formato *WebQuest* se mostrou eficaz no sentido de envolver o aluno na construção de seu conhecimento, desenvolvendo sua autonomia e autogestão, aguçar a curiosidade dos alunos em relação ao objeto de estudo. Além disso, surpreendentemente, fez aumentar também a necessidade e interesse por parte da turma no desenvolvimento teórico e na prática das técnicas aprendidas através de exercícios que envolvem repetição de procedimentos. Os alunos solicitaram que a abordagem fosse continuada em todas as aulas de matemática do ano.

O tema escolhido e a ênfase na resolução de problemas foi capaz de revelar a insegurança em usar a intuição e a falta de autonomia por parte dos alunos acostumados com a repetição de formatos inflexíveis de aula. Em contrapartida, utilizar a criptografia para problematizar os conteúdos se mostrou eficiente no sentido de despertar a curiosidade dos alunos, auxiliando a superação desses problemas.

Um ponto que merece especial destaque é como as atividades apresentadas serviu bem em complementar as abordagens mais tradicionais. O esforço de mudar o paradigma educacional para uma apresentação dos conteúdos através da problematização e da experimentação, foi capaz de fazer os alunos desenvolverem autonomia dentro de sua própria aprendizagem, buscando os conceitos necessários para o desenvolvimento da tarefa e, mais importante, criou a necessidade da formalização desses conceitos. Ao fim, uma abordagem tradicional, iniciando pela exposição teórica seguida pelos exercícios, não só pareceu mais promissora, mas foi demandada pelos alunos. Isso deixa claro o potencial da abordagem em motivar o desenvolvimento dos conteúdos e em desenvolver ajudar os alunos a desenvolverem sua autonomia, os fazendo capazes de identificar e demandar, claramente,

o que necessitavam para dar continuidade na aprendizagem dos tópicos abordados.

Como desdobramento dos estudos aqui desenvolvidos, foi aprovado em edital de extensão tecnológica do IFF a criação de um curso, no formato *WebQuest*, de revisão dos tópicos mais críticos do ensino fundamental a ser disponibilizado *online* gratuitamente.

Referências

BRASIL. **Parâmetros Curriculares Nacionais**: Matemática. Brasília, 1997.

BRASIL. **Parâmetros Curriculares Nacionais do Ensino Médio**. Brasília, 1999.

DODGE, B. Webquests: A technique for internet-based learning. **Distance Educator**, v. 1, n. 2, p. 10–13, 1995.

FIGUEIREDO, L. M. **Números Primos e Criptografia de Chave Pública**. 2009.

FIGUEIREDO, L. M. **Introdução à Criptografia**. 2012.

FIGUEIREDO, L. M. **Criptografia Geral I**. 2013.

FREIRE, P. **Pedagogia da Autonomia**: Saberes necessários à prátivca educativa. 31. ed. São Paulo: Paz e Terra, 2005.

GOMES, F. C. L. **Uma Proposta de Abordagem no Ensino Médio da Criptografia RSA e sua Estrutura Matemática**. Dissertação (Mestrado) — Universidade Federal do Tocantins, Gurupi, 2014.

HEFEZ, A. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: SBM, 2011.

MORTIMER, E. F. Construtivismo, mudança conceitual e ensino de ciências: Para onde vamos? **Investigações em Ensino de Ciências**, n. 1, p. 20–39, 1996.

MOTTA, C. E. M. Ouroboros: o fracasso das disciplnas de matemática básica e pré-cálculo nas universidades brasileiras. **Jornal Dá Licença**, UFF, n. 58, p. 3–5, 2014.

ZATTI, S. B.; BELTRAME, A. M. A presença da álgebra linear e teoria dos números na criptografia. **Jornada da Educação**, p. 1–10, 2006. Disponível em: <http://www.unifra-.br/>.

ZATTI, V. **Autonomia e Educação em Immanuel Kant e Paulo Freire**: Volume 1. Porto Alegre: ediPUCRS, 2007.

WebQuests

Constam aqui as *WebQuest* utilizadas nas atividades realizadas na produção deste material. Note que, como não se trata de um formato de aula totalmente fechado, há seções que constam em algumas aulas e que não constam em outras.

Cifra de César

Figura 19 – Capa da tarefa sobre cifras de substituição.

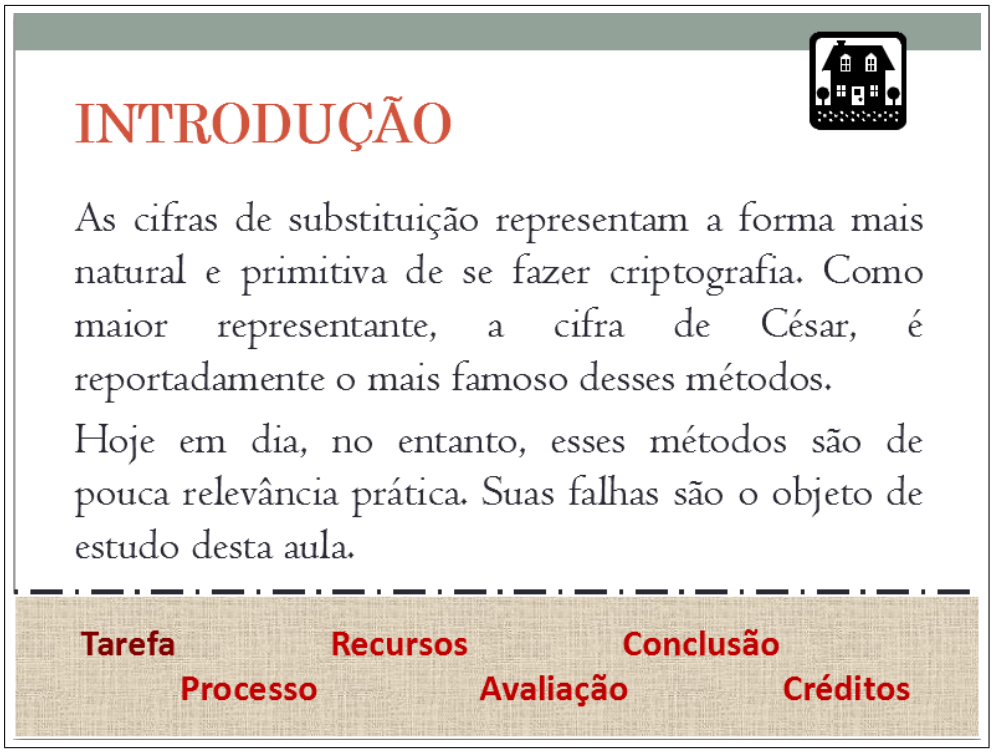


Figura 20 – Introdução da tarefa sobre cifras de substituição.

Figura 21 – Atividades propostas colocadas como objetivos a cumprir.

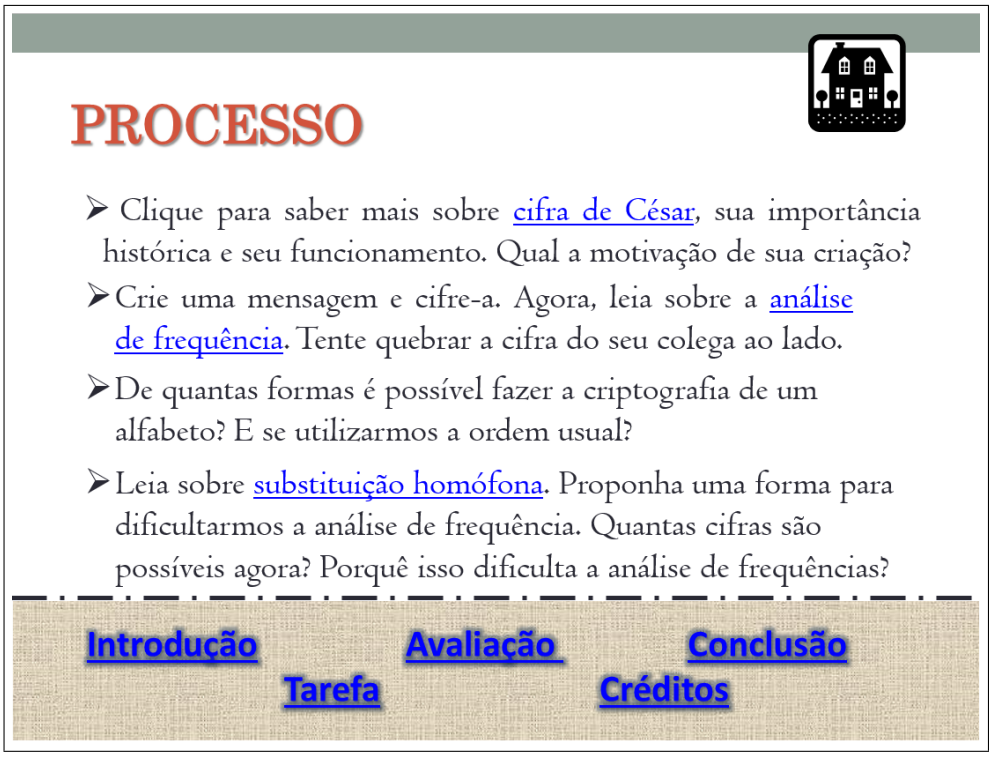


Figura 22 – O processo inclui orientações gerais de conduta para o aluno.

Figura 23 – Avaliação proposta.

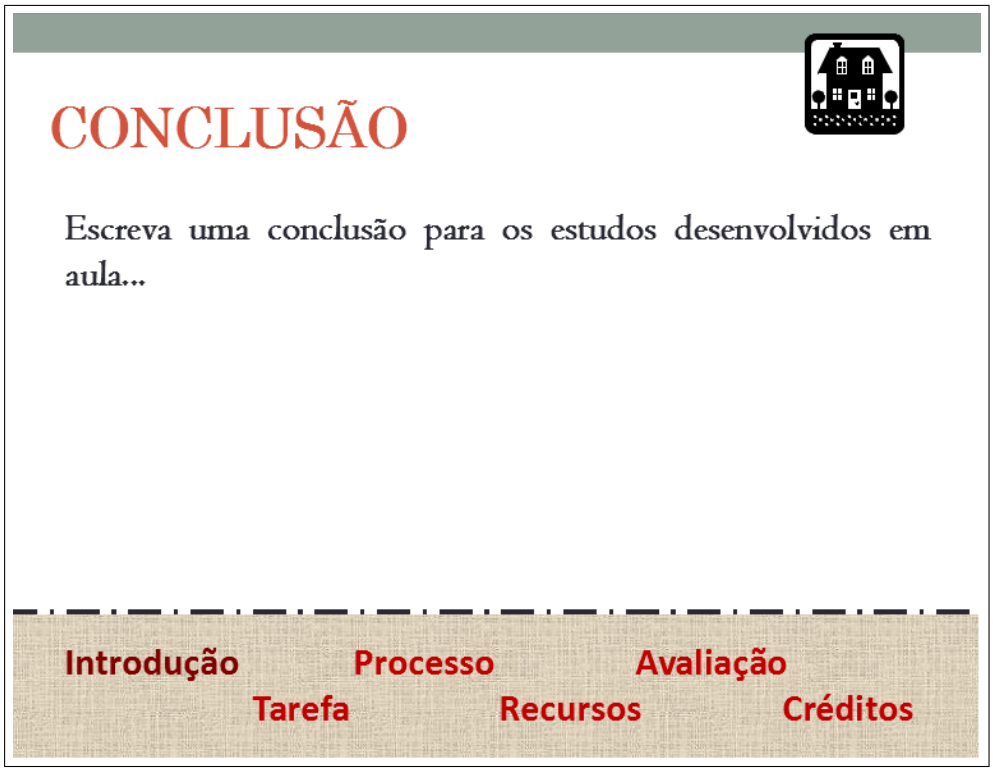


Figura 24 – Conclusão deixada a cargo do aluno.

Links Utilizados

http:www.mcsesolution.comSeguran%C3%A7aa-matematica-da-cifra-de-cesar.html

http:www.mat.uc.pt pedrolectivosCodigosCriptografia1011interTIC07pqap.pdf

http:pt.wikipedia.orgwikiCifra_de_substitui%C3%A7%C3%A3o#Substitui.C3.A7.C3.A3o_hom.C3.B3fona

Cifra de Hill

Figura 25 – Capa da tarefa sobre cifras de Hill.

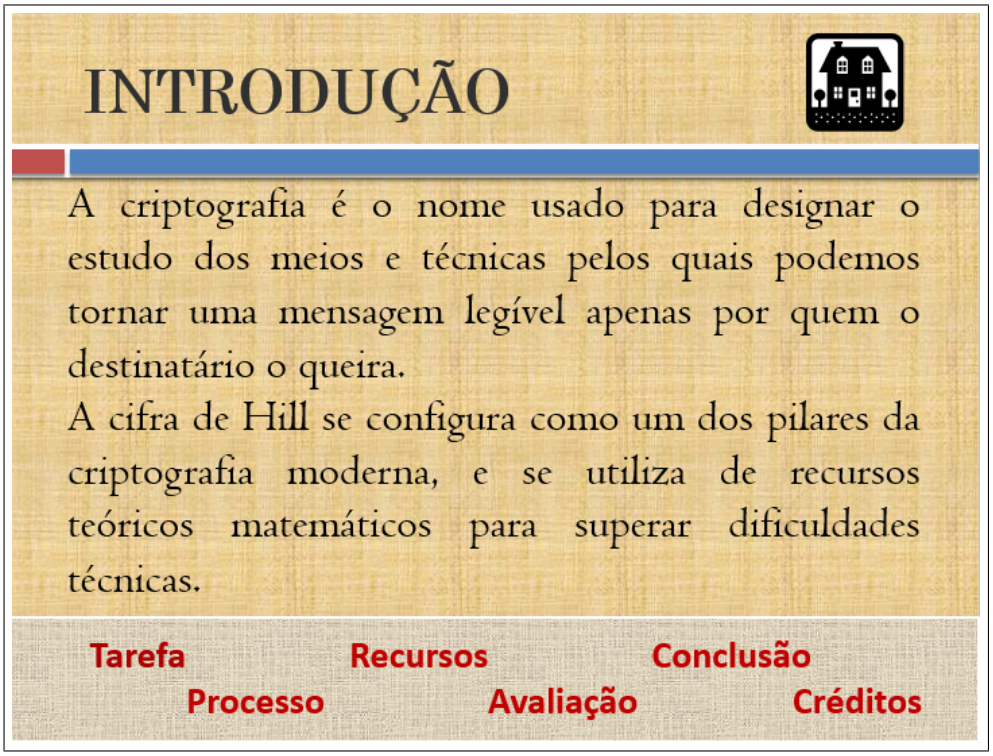


Figura 26 – Introdução da tarefa sobre cifras de Hill.

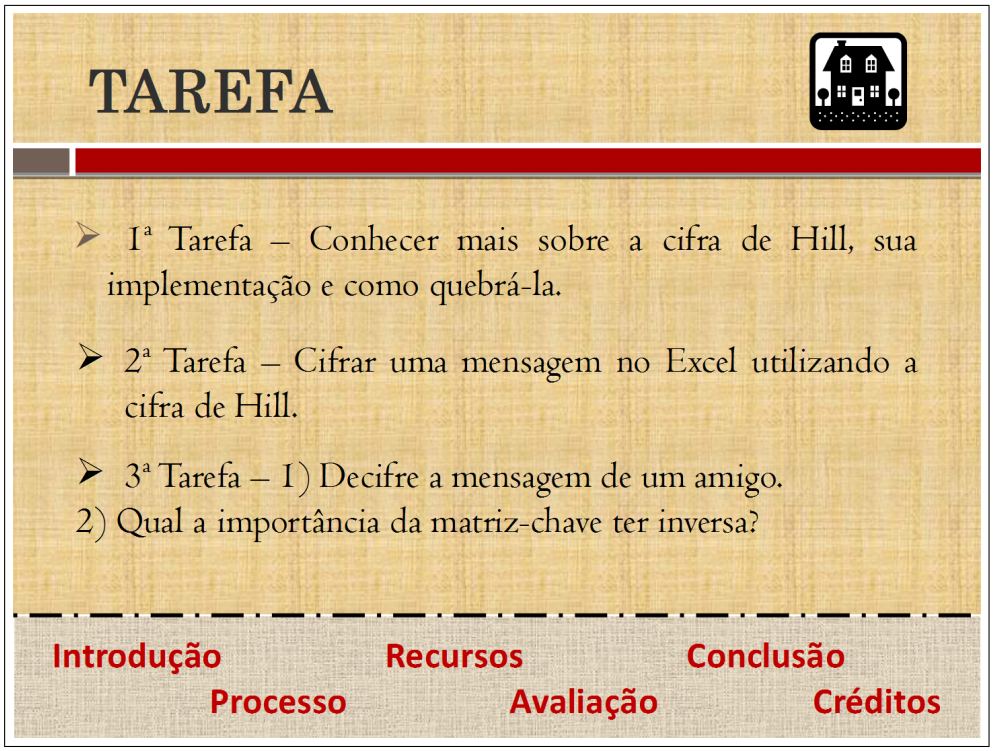


Figura 27 – Atividades propostas subjetivas valorizam autonomia.

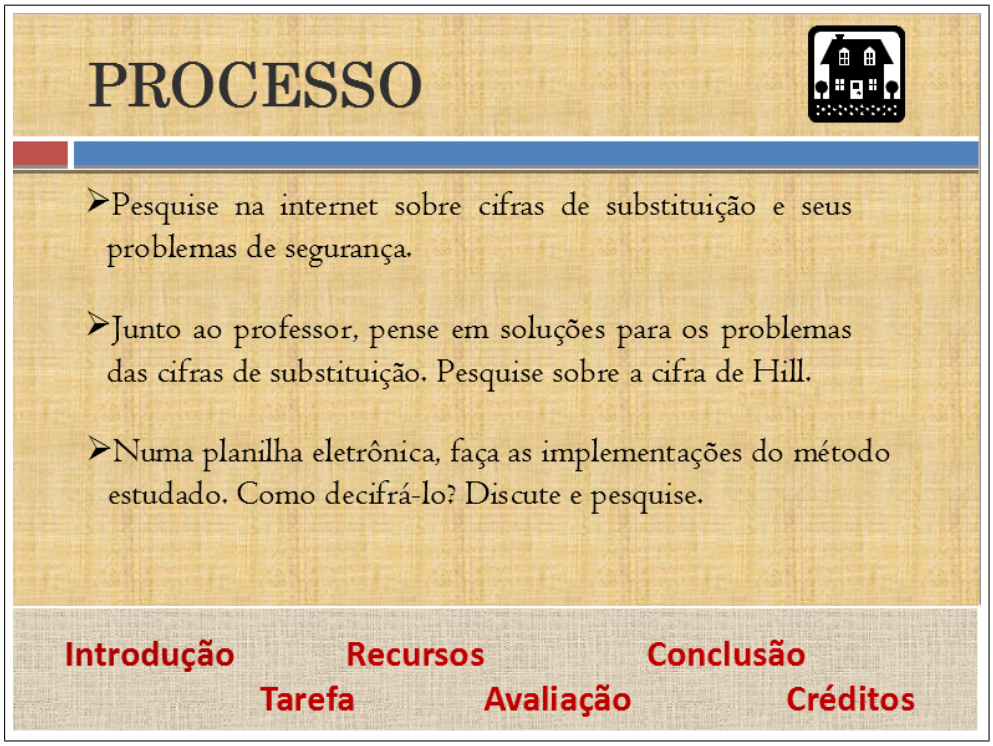


Figura 28 – Na própria *WebQuest* havia as fontes a serem consultadas pelo alunos.

Figura 29 – Avaliação proposta.

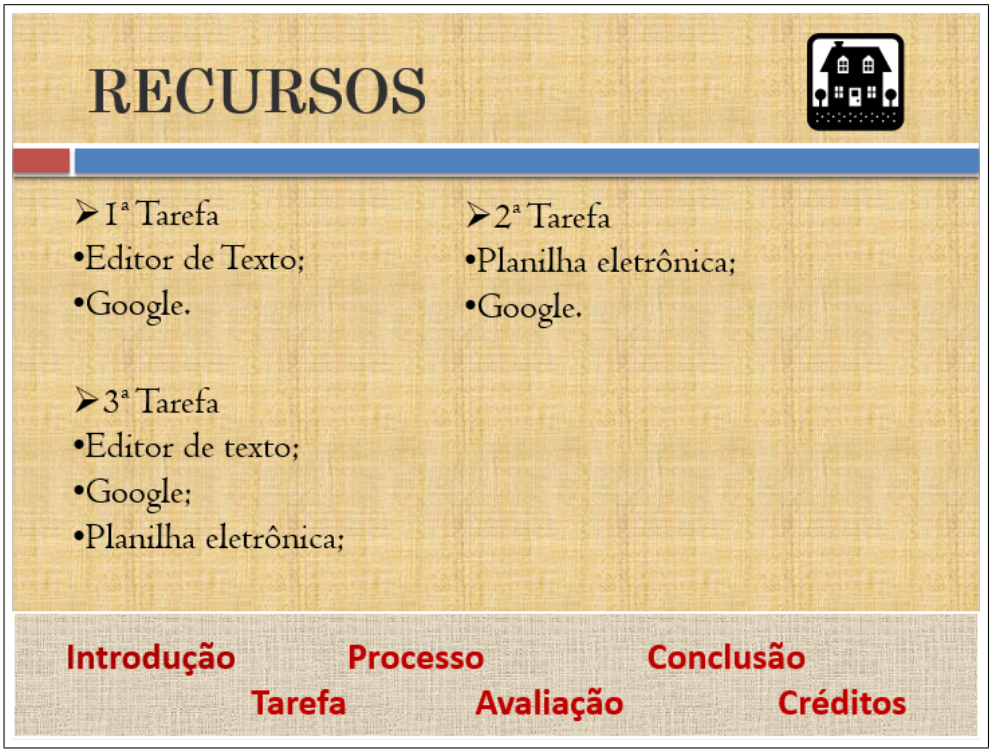


Figura 30 – Recursos utilizados na tarefa.

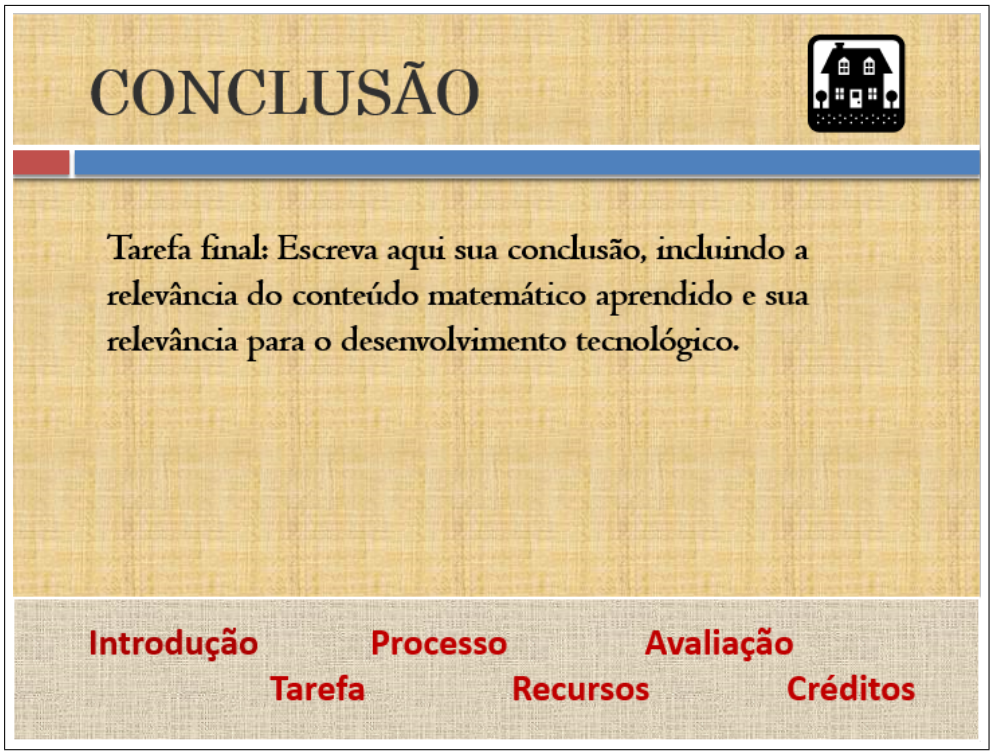


Figura 31 – Conclusão deixada a cargo dos alunos.

Cifras Assimétricas e Inversão de Matrizes

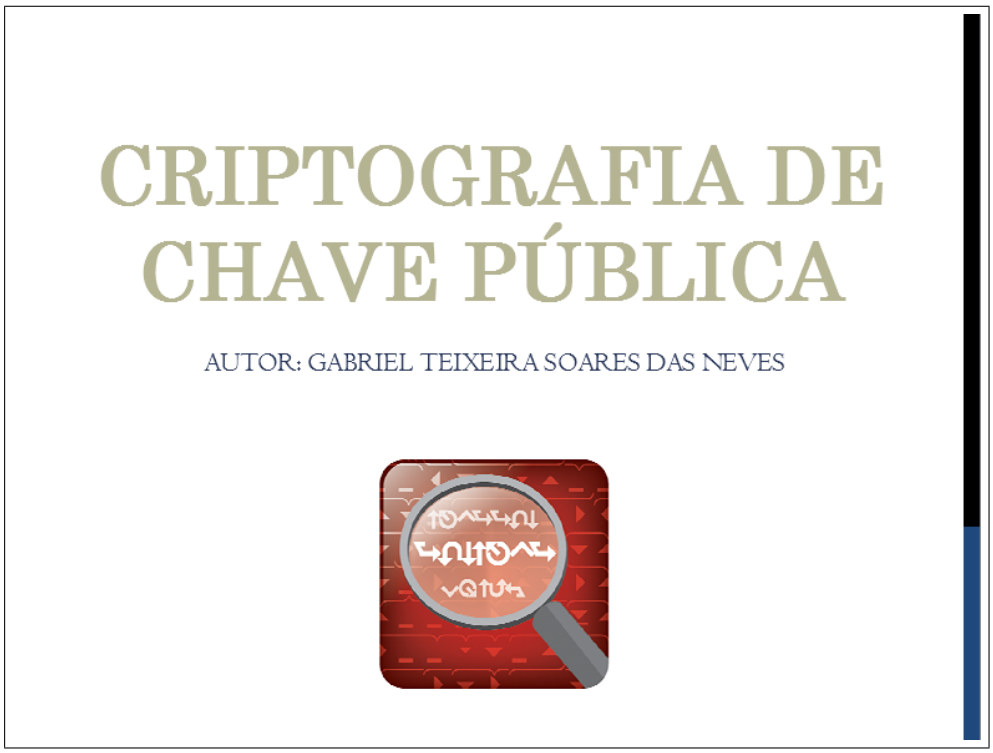


Figura 32 – Capa da tarefa sobre cifras assimétricas.

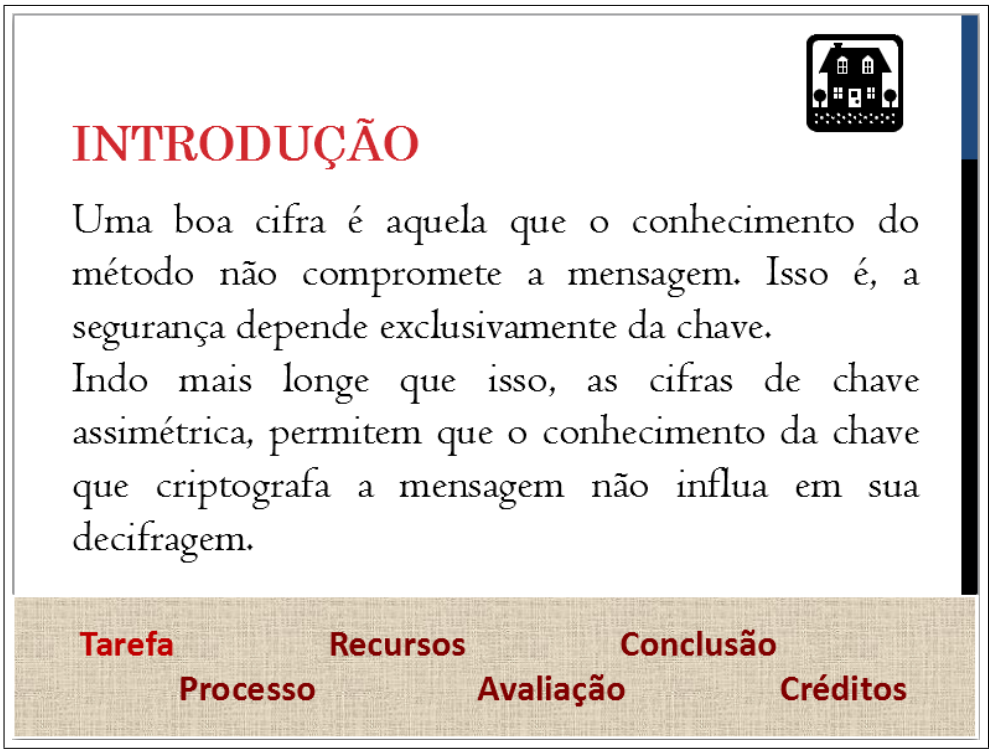


Figura 33 – Introdução da tarefa sobre cifras assimétricas.

Figura 34 – Tarefas da *WebQuest* sobre cifras assimétricas.

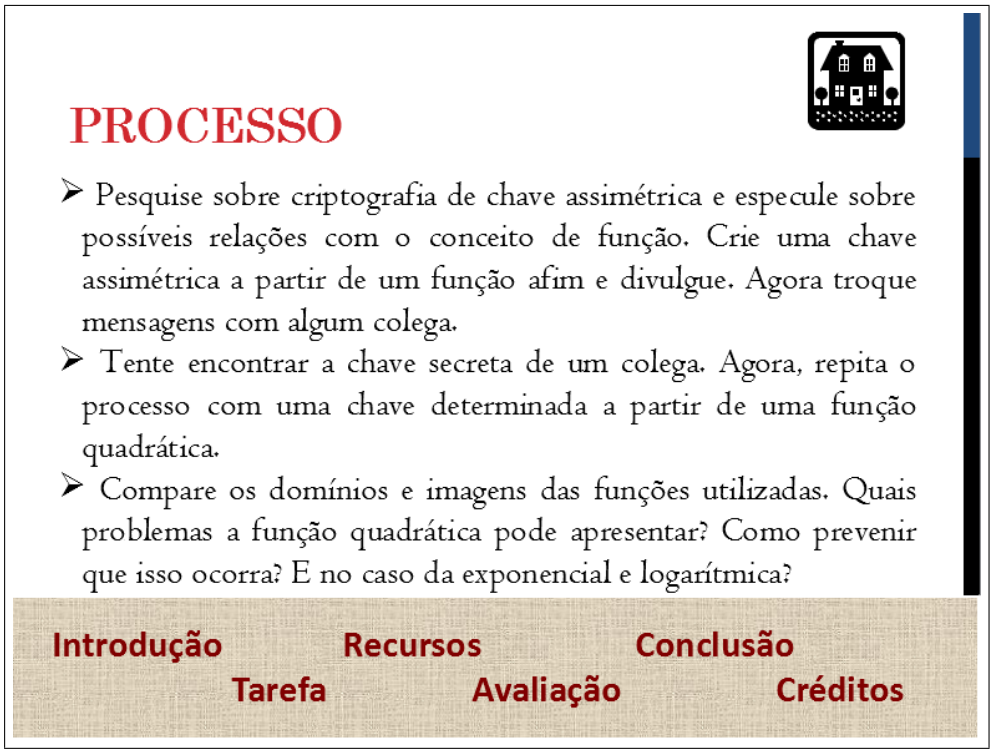


Figura 35 – Processo proposto.

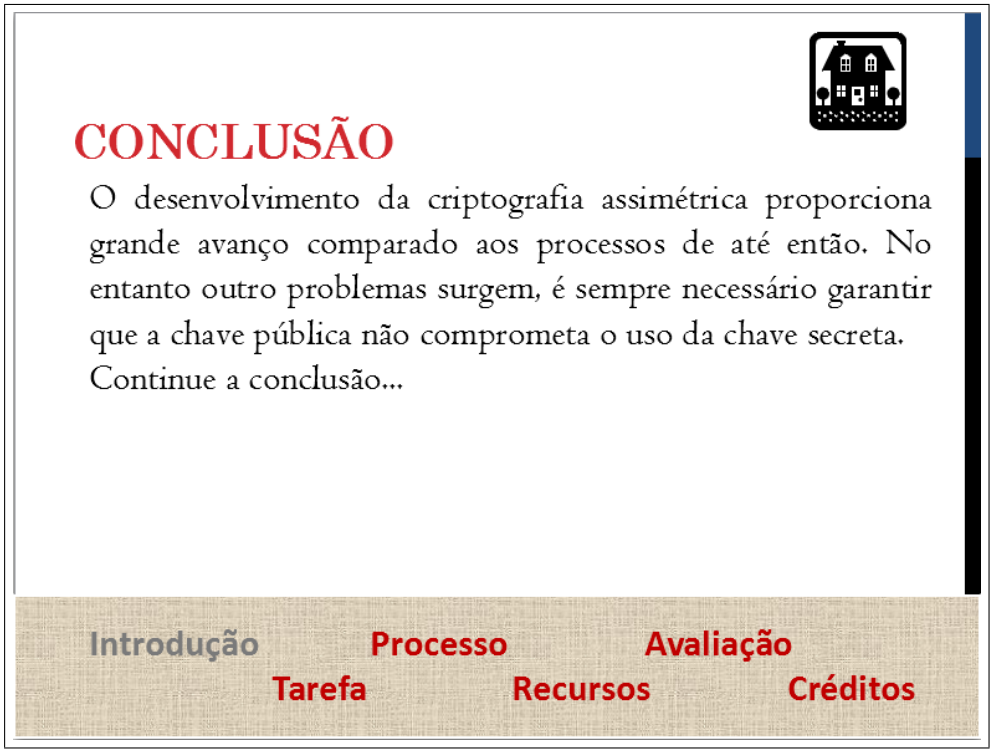


Figura 36 – Conclusão iniciada pelo autor, deve ser finalizada pelo aluno.

Figura 37 – Recursos utilizados na tarefa.

Link Utilizado

http:prof-ricardovianna.blogspot.com.br201105criptografia-parte-ii-criptografia-em.html

Criptografia RSA

Figura 38 – Capa da tarefa sobre criptografia RSA.

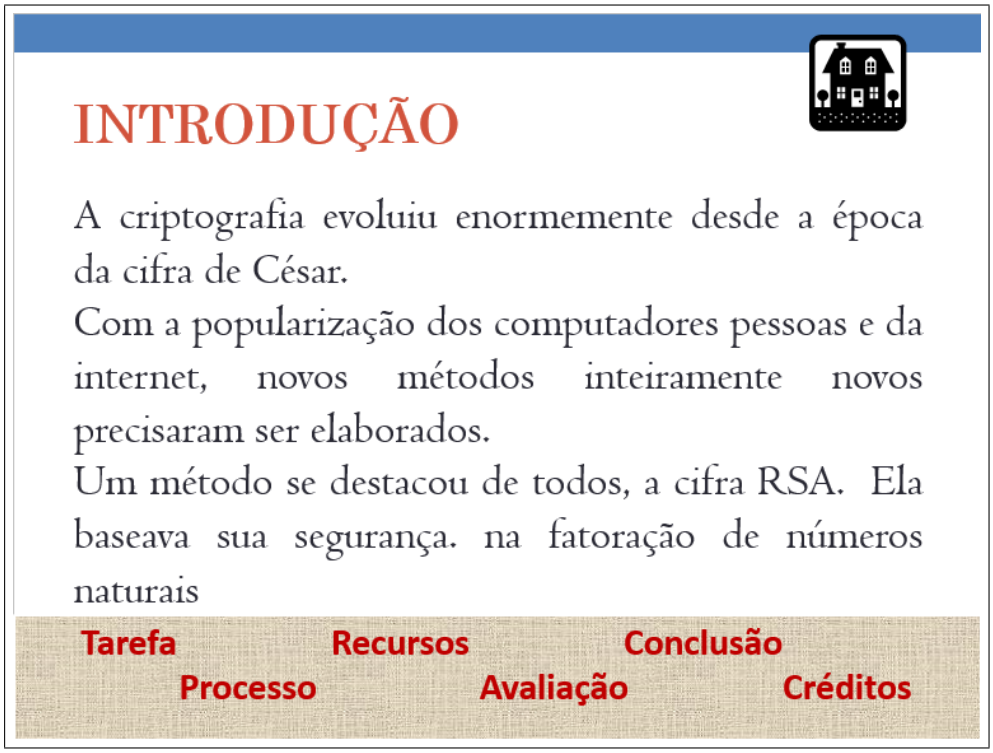


Figura 39 – Introdução da tarefa sobre criptografia RSA.

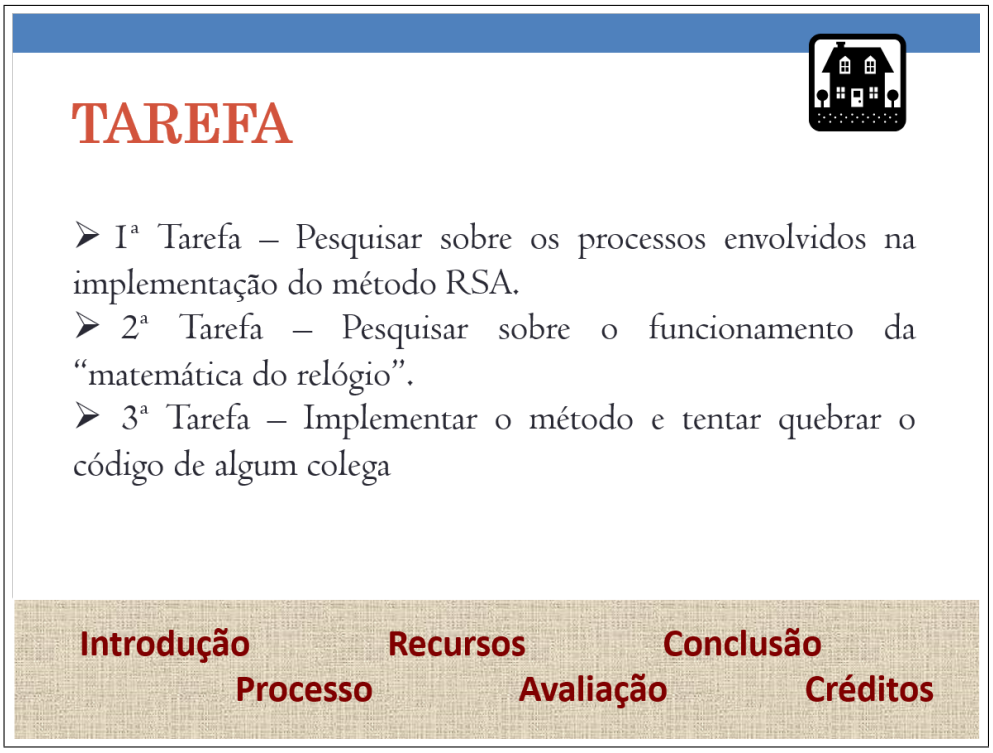


Figura 40 – Mais uma vez, a tarefa consiste basicamente da apresentação dos objetivos visados.

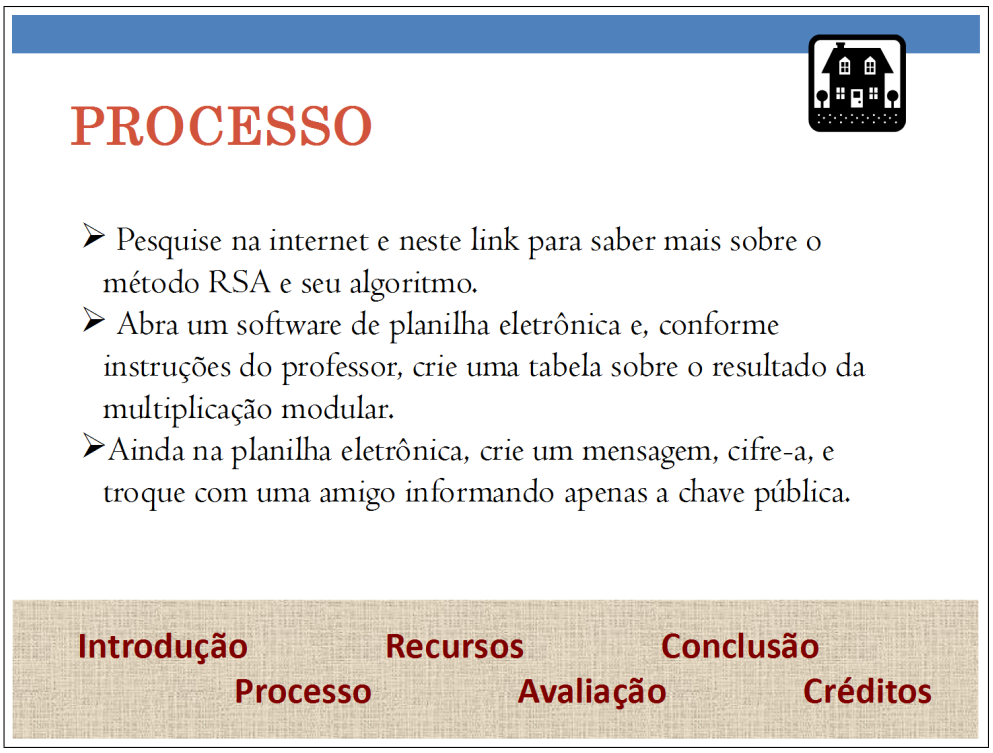


Figura 41 – No caso da RSA o professor precisa ir além da *WebQuest* e exercer um influência mais direta no processo.

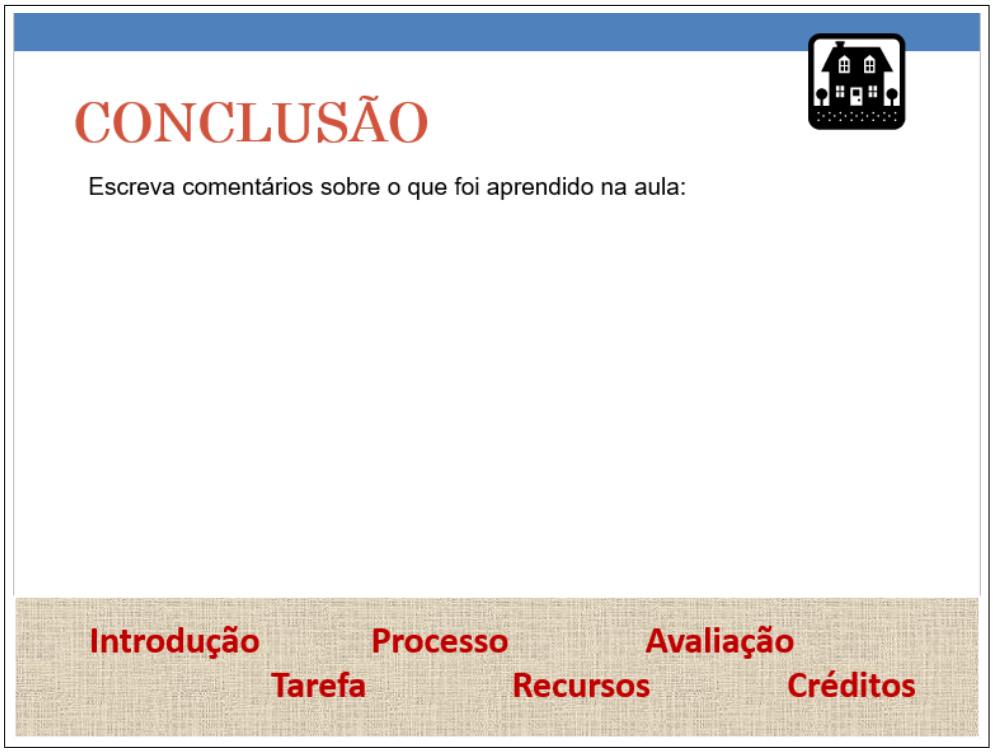


Figura 42 – Conclusão deve ser composta pelo aluno.

Questionários

Questionário Aplicado Antes das Atividades

1.Como você acha que deve ser a abordagem inicial na matemática?

a)Desenvolvimento teórico.

b)Motivado por um problema.

2.O que mais ajuda a entender os conceitos desenvolvidos em matemática, em sua opinião?

a)Através da resolução de problemas.

b)Através da exposição teórica por parte do professor.

c)Através de exercícios de repetição.

3.Você já teve professores de matemática que faziam uso de recursos computacionais?

a)Sim.

b)Não.

4.O que você acha do uso de tecnologias em sala de aula?

a)Só atrapalha.

b)Útil.

c)Dispensável.

5.Qual o papel você acha que tecnologias devem desempenhar em sala de aula?

a)Ferramenta ativa na aprendizagem.

b)Apenas ilustração da matéria.

c)Conteúdo direto no quadro é sempre melhor.

Questionário Aplicado Após as Atividades

1.Como você acha que deve ser a abordagem inicial na matemática?

a)Desenvolvimento teórico.

b)Motivado por um problema.

2.O que mais ajuda a entender os conceitos desenvolvidos em matemática, em sua opinião?

a)Através da resolução de problemas.

b)Através da exposição teórica por parte do professor.

c)Através de exercícios de repetição.

3.Você já teve professores de matemática que faziam uso de recursos computacionais?

a)Sim.

b)Não.

4.O que você acha do uso de tecnologias em sala de aula?

a)Só atrapalha.

b)Útil.

c)Dispensável.

5.Qual o papel você acha que tecnologias devem desempenhar em sala de aula?

a)Ferramenta ativa na aprendizagem.

b)Apenas ilustração da matéria.

c)Conteúdo direto no quadro é sempre melhor.

6.Como você gostaria que se dessem as aulas de matemática?

a)No laboratório de Informática, explorando recursos computacionais e resolvendo problemas

b)Em sala de aula, com exposição teórica seguida de exercícios de repetição

7.Que papel a resolução de problemas deve desempenhar na exposição do conteúdo?

a)Um motivador para a explicação teórica

b)Ilustração para o está sendo aprendido

c)Nenhum. O ideal são exercícios de repetição.