COLÉGIO PEDRO II

Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura

Mestrado Profissional em Matemática em Rede Nacional

Rafael Mendonça dos Anjos

INTRODUZINDO NOÇÕES SOBRE CRIPTOGRAFIA NO ENSINO DE JOVENS E ADULTOS: RELACIONANDO BASE BINÁRIA E FUNÇÕES À CRIPTOGRAFIA

Rio de Janeiro

2020

Rafael Mendonça dos Anjos

INTRODUZINDO NOÇÕES SOBRE CRIPTOGRAFIA NO ENSINO DE JOVENS E ADULTOS: RELACIONANDO BASE BINÁRIA E FUNÇÕES À CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, vinculado à Pró-reitoria de Pós-graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador(a): Profª. Dra. Maria de Lourdes Rocha de Assis Jeanrenaud

Rio de Janeiro

2020

COLÉGIO PEDRO II

PRÓ-REITORIA DE PÓS-GRADUAÇÃO, PESQUISA, EXTENSÃO E CULTURA

BIBLIOTECA PROFESSORA SILVIA BECHER

CATALOGAÇÃO NA FONTE

A599 Anjos, Rafael Mendonça dos

Introduzindo noções sobre criptografia no ensino de jovens e adultos: relacionando base binária e funções à criptografia / Rafael Mendonça dos Anjos. - Rio de Janeiro: Colégio Pedro II, 2020.

148 f.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Colégio Pedro II, Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura.

Orientador: Maria de Lourdes Rocha de Assis Jeanrenaud.

1. Matemática – Estudo e ensino. 2. Numeração. 3. Criptografia. 4. Educação de jovens e adultos (EJA). I. Jeanrenaud, Maria de Lourdes Rocha de Assis. II. Colégio Pedro II. III Título.

CDD 510

Ficha catalográfica elaborada pela Bibliotecária Simone Alves – CRB7 5692.

Rafael Mendonça dos Anjos

INTRODUZINDO NOÇÕES SOBRE CRIPTOGRAFIA NO ENSINO DE JOVENS E ADULTOS: RELACIONANDO BASE BINÁRIA E FUNÇÕES À CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, vinculado à Pró-reitoria de Pós-graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador(a): Profª. Dra. Maria de Lourdes Rocha de Assis Jeanrenaud

Aprovado em: 03/12/2020

Banca Examinadora:

_____

Profª. Dra. Maria de Lourdes Rocha de Assis Jeanrenaud (Orientadora)
PROFMAT - Colégio Pedro II

_____

Profª. Dra. Patrícia Erthal de Moraes
PROFMAT - Colégio Pedro II

_____

Profª. Dra. Aline de Lima Guedes Machado
IME - UERJ

Rio de Janeiro

2020

À minha esposa Juliana e a meu filho Matheus que iluminam meus dias e transbordam de amor a minha vida.

AGRADECIMENTOS

Agradeço ao Conclave Universal que rege a toda existência, em especial ao Pai Maior e ao Mestre Jesus.

À minha esposa Juliana, revisora de meus textos, que me motivou a iniciar no curso de mestrado e me apoiou incondicionalmente, sem nunca reclamar das minhas obrigações e sempre ouvindo minhas reclamações e dificuldades, além de me dar forças e amor para continuar. Sem você, eu não conseguiria.

Ao meu filho Matheus, luz em minha vida, que me deu o prazer de seu nascimento um dia após o ENQ (qualificação do mestrado) e me alegra com seus sorrisos, sua energia e sua alegria todos os dias.

À minha orientadora Maria de Lourdes, pelas conversas e dicas preciosas para o direcionamento desse trabalho, sem as quais não seria possível chegar a sua forma final.

A meus familiares que, mesmo indiretamente, se preocuparam com meus estudos e me apoiaram quando necessário.

Aos amigos Luis Felipe e Nauana, que sempre se preocuparam e ouviram minhas queixas e lamúrias sobre o Mestrado, além de me apoiarem desde o primeiro momento perguntando e oferecendo seu tempo precioso.

Aos meus amigos fantásticos da turma de 2018 do PROFMAT – CPII, em especial a Diego Rangel meu companheiro de trabalhos e estudos desde os tempos de Universidade Federal Fluminense.

Aos meus professores do PROFMAT – CPII que me mostraram que, mesmo após muitos anos, ainda é possível buscar novos ares e conhecimentos acadêmicos, e me presentearam com aulas maravilhosas e inesquecíveis.

Aos meus alunos do Ensino de Jovens e Adultos (EJA) por me motivarem a sempre melhorar e modificar minhas convicções sobre os saberes e conhecimentos existentes.

RESUMO

ANJOS, Rafael Mendonça dos. **Introduzindo noções sobre criptografia no ensino de jovens e adultos:** relacionando base binária e funções à criptografia. 2020. Dissertação (Mestrado Profissional em Rede Nacional – PROFMAT) – Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura, Colégio Pedro II, Rio de Janeiro, 2020.

O Ensino de Jovens e Adultos - EJA é uma modalidade de ensino muito frequente em nossa realidade como cidade e país. Considerada uma "segunda chance" para aqueles que não conseguiram se formar por variados motivos, desde a falta de oportunidades até mesmo a necessidade de começar a trabalhar cedo para a garantia do sustento familiar, tem como objetivo fundamental alcançar esses jovens e adultos que tiveram dificuldade em concluir o Ensino Fundamental ou Médio na idade regular. Porém, para concretizar de fato tal objetivo é preciso perceber a necessidade de novas abordagens focadas nas características próprias dessa categoria de estudante. Basta refletirmos acerca dos múltiplos papéis que uma pessoa adulta desempenha – na família, na comunidade, na organização em que trabalha -, e nas experiências que acumula com esse desempenho, além de conhecimentos e informações adquiridas em outras situações de formação e/ou capacitação para percebermos que são detentores muitas vezes de conhecimentos válidos, porém não explícitos. Assim, o estudante adulto deve participar ao máximo na obtenção dos resultados do seu processo de ensino e aprendizagem. Ao contrário de uma relação verticalizada entre docente e aprendiz, ou de uma mera importação do sistema tradicional de ensino para a EJA, o ensino do adulto requer uma perspectiva diferente, mais voltada para o estímulo à aprendizagem. Para tanto, compreendemos que a aprendizagem ao longo da vida está diretamente relacionada com sua aplicabilidade no cotidiano do estudante adulto. Em outras palavras, de que forma ele utilizará o conhecimento adquirido em seu dia a dia. Um dos motivos de desinteresse visto nos estudantes desta modalidade de ensino é, em grande parte, oriundo dessa "falta de relação aparente" com o cotidiano. A pesquisa explora o tema *Criptografia*, onipresente em nosso dia a dia voltado de muitas formas para o uso da tecnologia, porém de pouca percepção para o cidadão comum. A Criptografia está presente no nosso dia a dia de forma permanente, seja ao efetuarmos uma transação bancária ou enviarmos um e-mail ou mensagem pelo celular, aqui mencionados como aplicações mais simples; seja na linguagem falada ou escrita, seja nas caracterizações matemáticas que podem ser interpretadas ou apropriadas. As atividades propostas, de caráter introdutório aos métodos da criptografia, são relacionadas aos conceitos de base numérica e funções. Assim, professores atuantes na EJA – Fundamental podem utilizá-las como auxílio no processo de ensino e aprendizagem inicial voltado para tais conceitos e ainda como base para futuras atividades e desdobramentos da pesquisa em si. Foi feito um compilado para a construção e elaboração das atividades adaptando-as de forma a se adequarem a realidade do público-alvo, de forma sequencial e lógica. As atividades elaboradas ou adaptadas contemplam os dois ciclos do EJA. Cabe destacar que é viável a utilização de tais atividades no 2º segmento do Ensino Fundamental, bastando ajustar ao início do 6º ano ou do 9º nono ano.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Palavras-chave: Educação de Jovens e Adultos; Criptografia; Sistemas de Numeração; Funções; Resolução de Problemas.

ABSTRACT

ANJOS, Rafael Mendonça dos. **Introduzindo noções sobre criptografia no ensino de jovens e adultos:** relacionando base binária e funções à criptografia. 2020. Dissertação (Mestrado Profissional em Rede Nacional – PROFMAT) – Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura, Colégio Pedro II, Rio de Janeiro, 2020.

Youth and Adult Education - EJA is a very common teaching modality in our reality as a city and country. Considered a "second chance" for those who failed to graduate for a variety of reasons, from the lack of opportunities to the need to start working early to guarantee family livelihood, it has the fundamental objective of reaching these young people and adults who had difficulties completing elementary or high school at the regular age. However, to actually achieve such an objective, it is necessary to realize the need for new approaches focused on the characteristics of this category of student. It is enough to reflect on the multiple roles that an adult person plays - in the family, in the community, in the organization in which he works -, and in the experiences he accumulates with this performance, in addition to the knowledge and information acquired in other situations of education and / or training for we realize that they are often holders of valid but not explicit knowledge. Thus, the adult student must participate as much as possible in obtaining the results of his teaching and learning process. Unlike a vertical relationship between teacher and apprentice, or a mere importation of the traditional teaching system into EJA, adult education requires a different perspective, more focused on stimulating learning. Therefore, we understand that lifelong learning is directly related to its applicability in the daily life of adult students. In other words, how he will use the knowledge acquired in his daily life. One of the reasons for the lack of interest seen in students in this type of teaching is, in large part, due to this "lack of apparent relationship" with daily life. The research explores the subject of Cryptography, which is ubiquitous in our daily lives, in many ways turned to the use of technology, but with little perception for ordinary people. Cryptography is present in our daily lives permanently, whether when making a bank transaction or sending an e-mail or message by cell phone, mentioned here as simpler applications; either in spoken or written language, or in mathematical characterizations that can be interpreted or appropriated. The proposed activities, of an introductory nature to cryptography methods, are related to the concepts of numerical basis and functions. Thus, teachers working in EJA – elementary school can use them as an aid in the teaching and initial learning process focused on such concepts and also as a basis for future activities and developments of the research itself. A compilation was made for the construction and elaboration of activities, adapting them to suit the reality of the target audience, in a sequential and logical way. The activities designed or adapted include the two cycles of the EJA. It should be noted that it is feasible to use such activities in the 2nd segment of Elementary Education, just adjusting to the beginning of the 6th year or the 9th year.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001"

Keywords: Youth and Adult Education; Cryptography; Numbering Systems; Functions; Problems Solving.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A finalidade da escola, além de apresentar as questões teóricas, é tornar seus estudantes cidadãos esclarecidos e capazes de relacionar os conceitos teóricos a situações na sociedade em que vive.

Nesse sentido, de acordo com a Base Nacional Comum Curricular (BNCC), podemos destacar duas das competências gerais da Educação Básica.

A primeira nos orienta a:

> [...] valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva. (BRASIL, 2017, p. 09)

Ou seja, há a necessidade de um embasamento histórico, filosófico e cultural, bem como a utilização de tecnologias vigentes para ambientar os estudantes e facilitar a relação entre o mundo teórico de sala de aula e o mundo "prático" da sociedade onde vive.

Essa relação entre os saberes, teórico e prático é mais evidente na segunda competência que acrescenta:

> [...] exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas. (BRASIL, 2017, p. 9)

Diante do cenário atual, cada vez mais frequente em todos os segmentos da educação, onde a rejeição à Matemática é a maior possível, faz-se necessária uma melhor abordagem aos tópicos e conteúdos trabalhados de forma teórica, visando relacioná-los de maneira clara e concisa ao cotidiano dos alunos. A aplicação de técnicas da criptografia para a introdução ou fixação de conceitos da matemática atinge esse objetivo.

No presente trabalho, procuramos desenvolver atividades voltadas para a sala de aula direcionadas à Educação de Jovens e Adultos (EJA- Ensino Fundamental), mas que podem, porém, serem aproveitadas em todos os anos do Ensino Fundamental II (6º ao 9º ano).

Quanto a esta modalidade de ensino, o artigo 37 da Lei de Diretrizes e Bases da Educação[1] nos diz que "A educação de jovens e adultos será destinada àqueles que não tiveram acesso ou continuidade de estudos nos ensinos fundamental e médio na idade própria e constituirá instrumento para a educação e a aprendizagem ao longo da vida."

Algumas questões precisam ser levadas em consideração quando se trata da EJA:

- Como a trajetória dos estudantes deve ser levada em consideração dentro da prática pedagógica do professor?
- Como o professor deve atender a esse segmento utilizando o contexto em que vivem para dar significado às suas aulas?
- Que estratégias utilizar para se apropriar das experiências individuais com o objetivo de enriquecer o processo de ensino-aprendizagem e criar uma ponte entre os temas abordados e o dia a dia de cada um?

De acordo com Feitosa (1999, p.17), "vivemos numa sociedade globalizada, altamente tecnológica que aponta para sucessivas mudanças e para a construção de um novo tempo que, por sua vez, exige a construção de novos paradigmas educacionais."

Assim, o professor atuante na EJA precisa ter a consciência de que os seus alunos esperam conquistar espaços que muitas vezes lhes foram negados pela falta de escolarização. Porém, essa educação não se constitui de forma mecânica, sistemática, uma vez que esses alunos querem ter consciência crítica do que acontece a sua volta e já se encontram moldados pelas experiências de vida que possuem.

Então o que se espera dessas aulas?

Já de início, o professor deve estar consciente de que não vai construir um saber, ele vai reconstruir um saber a partir das vivências dos seus estudantes, educandos, se atentando para as perspectivas deles.

Assim, seguindo esta linha de pensamento, com as atividades sugeridas temos o propósito de fomentar discussões sobre as relações matemáticas ligadas à criptografia e presentes em situações cotidianas e relações interpessoais. A ideia central foi de investigar cenários diversos com atividades ora objetivas ora subjetivas atreladas a questões práticas e operatórias, com a intenção de discussões e comparações.

---

[01] Lei de Diretrizes e Bases da Educação – Disponível em: <https://www.jusbrasil.com.br/topicos/11689869/artigo-37-da-lei-n-9394-de-20-de-dezembro-de-1996>. Acesso em 25/08/2020.

Nosso texto foi estruturado em 11 capítulos dos quais este é o primeiro.

Nos Capítulos 2 e 3, apresentamos a *Justificativ*a que nos cabe acerca da temática escolhida, como continuação do já mencionado nesta introdução e, os *Objetivos* a serem alcançados. O Capítulo 4 foi destinado a um esboço sobre o desenvolvimento da *Educação de Jovens e Adultos* em nosso país, tendo em vista o público-alvo a que se destinam prioritariamente as atividades propostas.

Já no Capítulo 5, apresentamos uma *Introdução à Criptografia* com aspectos históricos e principais métodos. Além disso, nos capítulos 6,7 e 8, tendo como base a Criptografia, caminhamos brevemente pela História da Matemática, pontuando alguns temas que serviram de suporte aos tópicos escolhidos, passando pelos *Sistemas d*e *Numeração* e finalizando com *Funções.* Procuramos assim perpassar dois grandes temas que trazem dúvidas e dificuldades aos estudantes.

No Capítulo 9, apresentamos uma breve descrição da *Metodologia* empregada para realizar esta pesquisa e das dificuldades encontradas.

Ponto central deste trabalho, no Capítulo 10 fazemos a descrição das *Atividade*s *Propostas* para aplicação em sala de aula, com indicação de objetivos, público-alvo, referências e sugestões de leitura.

Para finalizar, no Capítulo 11 seguem as *Considerações Finais* acerca do trabalho, na qual enfatizamos que aprender um tópico ou apropriar-se de um conteúdo e conseguir aplicá-lo em algum segmento do dia a dia mostra a importância da relação entre sala de aula e vida cotidiana, além de contribuir para o interesse e diminuir a rejeição à Matemática na sociedade.

Seguem ainda, as *Referências Bibliográficas* utilizadas como base para este trabalho, o Apêndice A - *Atividades Propostas* e o Apêndice B – *Resolução das Atividades Propostas*.

2 JUSTIFICATIVA

A presente pesquisa foi motivada por um olhar voltado a Educação de Jovens e Adultos - EJA levando em consideração suas barreiras, tanto culturais quanto estruturais.

Como professor da Rede Municipal de Ensino do Estado do Rio de Janeiro, o pesquisador optou por dar segmento a uma pesquisa transformadora de sua prática e que visa relacionar alguns tópicos e conceitos que norteiam o primeiro e último ciclos da EJA.

A observação do caráter introdutório tem a pretensão de facilitar a prática pedagógica de outros professores ao abordarem os referidos assuntos. O que se deseja é evitar a padronização de conteúdos e atividades, permitindo ao professor em si a autonomia e liberdade que tanto pleiteamos nas salas de aula de nosso país.

Além disso, pode-se notar a dificuldade que a maioria dos alunos possui, ao lidar com conteúdos e métodos abstratos, principalmente os da EJA. Há claramente um certo distanciamento por parte desses estudantes.

Um dos objetivos da presente pesquisa é tornar esse distanciamento menor, além de criar um fator de atração maior aos conteúdos que por vezes acabam se tornando subjetivos e fora da realidade.

A criptografia é um assunto importante e que tem despertado o interesse no contexto atual. A rotina diária das pessoas passa pelo uso contínuo de computadores, tablets e principalmente celulares para fazerem quase tudo, de pagamentos de compras a marcação de encontros. Mas tal comodidade tem seus perigos, por conta da transmissão de informações dos mais diversos tipos. Daí a preocupação com a transmissão segura de informações, garantida pelas mais diversas técnicas criptográficas.

Acreditamos que seu uso possa despertar um algo a mais nos alunos, motivando-os e ajudando o professor a contornar dificuldades ao tentar estimular seus alunos, no aprendizado e conceitos relacionados com o ensino da Matemática.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Elaborar um conjunto de atividades que envolvam criptografia e temas da matemática básica (sistemas de numeração, funções, porcentagem) para serem aplicadas em sala de aula em turmas de Educação de Jovens e Adultos, como estratégias para o ensino de Matemática nesta modalidade de ensino.

3.2 OBJETIVOS ESPECÍFICOS

- Auxiliar ao professor na obtenção de ferramentas e artifícios no processo ensino-aprendizagem.
- Auxiliar os estudantes da Educação de Jovens e Adultos na compreensão de conteúdos da Matemática que, por vezes, parecem “desconectados” da realidade, tanto do professor, quanto do aluno.
- Propiciar ao estudante da Educação de Jovens e Adultos ser o protagonista de algumas ações relativas ao seu processo de ensino aprendizagem, contribuindo ativamente para o seu próprio desenvolvimento.

4 A EDUCAÇÃO DE JOVENS E ADULTOS – EJA

A Educação de Jovens e Adultos é uma modalidade voltada para alunos de diversas faixas etárias que por algum motivo não conseguiram concluir o ensino básico. Há de se observar a complexidade dessa modalidade, pois o professor deve avaliar uma grande quantidade de variáveis (tais como tempo longe dos estudos básicos, motivação pessoal, necessidade de aprimoramento e qualificação para o trabalho e os "saberes cotidianos" relacionados ao dia a dia, além das habilidades requeridas) para que possa analisar, preparar e gerir tanto as aulas como o plano de curso que será abordado em uma determinada turma.

Historicamente, o índice de analfabetismo muitas vezes foi utilizado para meios e fins políticos, ora para impulsionar através de projetos voltados à redução dos números e consequente redução da parcela da população que não possuía apenas o ensino básico, ora para impulsionar candidaturas e intenções (verídicas ou não) na melhoria do ensino de base em nosso país. Isso se traduz nos dados referentes a quantidade de pessoas analfabetas no país.

Tabela 1- Analfabetismo na faixa de 15 anos ou mais – Brasil – 1900/2000

Ano	População de 15 anos ou mais		
	Total(1)	Analfabeta(1)	Taxa de Analfabetismo
1900	9.728	6.348	65,3
1920	17.564	11.409	65,0
1940	23.648	13.269	56,1
1950	30.188	15.272	50,6
1960	40.233	15.964	39,7
1970	53.633	18.100	33,7
1980	74.600	19.356	25,9
1991	94.891	18.682	19,7
2000	119.533	16.295	13,6

Nota: (1) Em milhares

Fonte: Disponível em: <http://portal.inep.gov.br/documents>. Acesso em 29/08/2020

Observe que, pela tabela, tem-se a sensação de uma redução nas taxas de analfabetismo. O que não necessariamente se configura como uma verdade quando se trata de números absolutos. A seguir, um comparativo entre os anos 2000 e 2010, datas dos últimos censos feitos até o momento em relação aos jovens e adultos a partir dos 15 anos, foco da pesquisa.

Tabela 2 - Taxa de analfabetismo da população de 15 anos ou mais de idade.

2000/2010

Unidades da Federação e municípios das capitais	Taxa de analfabetismo da população de 15 anos ou mais de idade, por grupos de idade (%)							
	Total		Grupos de idade					
			15 a 24 anos		25 a 59 anos		60 anos ou mais	
	2000	2010	2000	2010	2000	2010	2000	2010
Brasil	**13,6**	**9,6**	**5,8**	**2,5**	**13,0**	**8,5**	**35,2**	**26,5**

Fonte: Disponível em: < http://www.educacao.df.gov.br>. Acesso em 29/08/2020

A partir dos dados, deve-se analisar as questões qualitativas e quantitativas referentes a situação populacional dos censos e sua comparação. Ou seja, embora o percentual de analfabetos tenha diminuído em dez anos (2000 – 2010), note que a população era de 169.590.693 pessoas (2000) e passou a ser de 190.732.694 (2010). Esses números caracterizam que nos anos 2000, havia aproximadamente 23.064.334 pessoas analfabetas (maiores de 15 anos), enquanto em 2010, haviam aproximadamente 18.310.338 pessoas analfabetas (maiores de 15 anos). Vale salientar a quantidade de projetos e incentivos à educação impostos durante os governos na década citada que, mesmo assim, conseguiram apenas reduzir em menos de 5 milhões a quantidade de pessoas analfabetas maiores de 15 anos. Essa análise leva em conta um dos pilares da educação que é a universalização da educação básica. Ou seja, independente de etnia, credo, gênero, é dever do Estado que todo brasileiro tenha acesso a educação pública e de qualidade, de acordo com os artigos 3º e 4º da Lei de Diretrizes e Bases da Educação (1996).

Para uma compreensão mais ampla sobre a Educação de Jovens e Adultos e as taxas de analfabetismo no Brasil, bem como as teorias e práticas associadas, é necessário um olhar pregresso ante a história de tal modalidade em nosso país.

Um breve histórico sobre o EJA e seu desenvolvimento ao longo do Século XX

O início do século XX foi marcado por um período de grande preconceito e poucas possibilidades àqueles que não eram letrados. Além da distinção aberta às pessoas com menores

rendas, foram anexadas a essas, todas as pessoas analfabetas. Ou seja, de forma retrógrada, por não assegurar o direito à educação primária e gratuita a todos, a constituição de 1891, além de negar esse direito, ainda condicionou o voto à alfabetização.

Em 1915 foi criada a *Liga Brasileira contra o Analfabetismo*, que visava acabar com o analfabetismo, a essa altura considerado uma praga para a sociedade. Nesse ponto, deve-se notar que a educação não era o foco principal, e sim projetos de educação para jovens e adultos, tendo em vista o fato que a grande maioria da população não tinha qualquer formação acadêmica. Nas duas décadas que se seguiram (20 e 30), não houve desenvolvimento ou avanço significativo no tocante a Educação de Jovens e Adultos. Porem cabe aqui citar a criação do Ministério da Educação (MEC) em 1930, que buscou organizar e elaborar um programa de política educacional, através de um manifesto (1932) assinado por Anísio Teixeira, entre outros educadores à época (BRASIL, © 2018).

Segundo Viegas e Moraes (2017), a partir da década de 40 até o fim da década de 50, houve uma mudança no olhar dado a Educação de Jovens e Adultos, com a criação do *Plano Nacional da Educação* que continha como uma das diretrizes, o ensino primário obrigatório e gratuito a pessoas adultas. Com isso, o ensino para jovens e adultos começou a se afigurar como uma das prioridades no enfrentamento ao analfabetismo que havia chegado a 72% da população nas décadas anteriores. A criação do Instituto Nacional de Estudos Pedagógicos (INEP) em 1938 serviu como um início a esse movimento de mudança dos paradigmas.

Devido às pesquisas na área, foi criado um fundo monetário visando o desenvolvimento da educação e contemplando também o ensino supletivo para jovens e adultos. Regulamentado em 945, estabelecia que 25% dos recursos fossem gastos na Educação de Jovens e Adultos.

Na mesma época, foram criados a *Lei Orgânica do Ensino Primário* (1946), que inseria no contexto da educação o ensino supletivo, o *Serviço de Educação de Adultos* (SEA) (1947) e, a *Campanha de Educação Rural* (1952). Esse movimento pró Educação de Jovens e Adultos, durou até o fim dos anos 50 e ficou conhecido como a *Primeira Campanha Nacional de Jovens e Adultos.*

Ainda em 1958, aconteceu o *Congresso Nacional de Educação de Jovens e Adultos* no qual Paulo Freire, responsável por um grupo de educadores de Pernambuco, compartilha sua perspectiva sobre o processo de ensino-aprendizagem que envolve a proposta de um processo educativo pautado na construção juntamente com os educandos. Tal construção traz luz à inclusão dos saberes cotidianos e das múltiplas inteligências na educação básica. O trabalho de

Paulo Freire[2] passou a ser uma referência em âmbito nacional, e inspirou a maioria dos educadores que ensinavam para jovens e adultos (VIEGAS; MORAES, 2017).

O início da década de 60 foi marcado por uma mobilização da sociedade em relação a essa modalidade de ensino, quando inúmeros movimentos sociais deram o tom de como a educação para adultos poderia seguir e valorizar a cultura única de cada indivíduo, permitindo assim, uma heterogeneização do ensino e uma pluralização dos saberes.

Em janeiro de 1964, foi criado o *Programa Nacional de Alfabetização* que acabou sendo uma culminância dos projetos elencados e idealizados nos anos de 1961 e 1962. Em março de 1964, Paulo Freire foi nomeado para coordenar todo o programa, visto que o método de alfabetização utilizado pelo programa era de sua autoria. No entanto, com o golpe militar de 31 de março de 1964, o programa acabou extinto em 14 de abril do mesmo ano (STRELHOW, 2010, p. 54).

Da ditadura aos anos 90

A tomada de poder pelos militares teve um impacto em todos os setores da sociedade, principalmente a educação. O golpe militar de 1964 desencadeou um processo de repressão aos movimentos educacionais e culturais, e consequente perseguição e censura a seus idealizadores. O Programa Nacional de Alfabetização foi extinto, com dirigentes perseguidos e materiais apreendidos (HADDAD; DI PIERRO, 2000).

Porém, alguns movimentos resistiram e continuaram reafirmando os interesses populares:

[2] Paulo Freire (1921 – 1997). Formou-se em direito, mas não seguiu carreira, encaminhando a vida profissional para o magistério. Suas ideias pedagógicas se formaram da observação da cultura dos alunos - em particular o uso da linguagem - e do papel elitista da escola. Em 1963, em Angicos (RN), chefiou um programa que alfabetizou 300 pessoas em um mês. No ano seguinte, o golpe militar o surpreendeu em Brasília, onde coordenava o Plano Nacional de Alfabetização do presidente João Goulart. Freire passou 70 dias na prisão antes de se exilar. Em 1968, no Chile, escreveu seu livro mais conhecido, Pedagogia do Oprimido. Também deu aulas nos Estados Unidos e na Suíça e organizou planos de alfabetização em países africanos. Com a anistia, em 1979, voltou ao Brasil, integrando-se à vida universitária. Filiou-se ao Partido dos Trabalhadores e, entre 1989 e 1991, foi secretário municipal de Educação de São Paulo. Freire foi casado duas vezes e teve cinco filhos. Foi nomeado doutor honoris causa de 28 universidades em vários países e teve obras traduzidas em mais de 20 idiomas.

Disponível em: <https://novaescola.org.br/conteudo/460/mentor-educacao-consciencia>. Acesso em 04/09/2020.

> Sob a denominação de "educação popular", entretanto, diversas práticas educativas de reconstituição e reafirmação dos interesses populares inspiradas pelo mesmo ideário das experiências anteriores persistiram sendo desenvolvidas de modo disperso e quase que clandestino no âmbito da sociedade civil. Algumas delas tiveram previsível vida curta; outras subsistiram durante o período autoritário. (HADDAD; DI PIERRO, 2000, p. 113).

Ao longo desse período, destacaram-se algumas tentativas oficiais de programas voltados para a educação de adultos como o *MOBRAL – Movimento Brasileiro de Alfabetização* (1967) e a implantação do Ensino Supletivo em 1971, quando houve a promulgação da Lei Federal 5.692 reformulando as diretrizes de ensino de primeiro e segundos graus.

De acordo com Di Pierro e Haddad (2000), a criação do MOBRAL visava a implantação de uma política de controle de massa com ideais doutrinadores tais como: descentralização da estrutura com uma base conservadora para maior amplitude do trabalho e centralização de objetivos e visões políticas, além de um controle vertical pelos supervisores. O projeto acabou sofrendo algumas adaptações ao final dos anos 70, visando sua sobrevivência ante ao fracasso dos objetivos iniciais para superar o analfabetismo no Brasil.

Por outro lado, nesse período, as reformas educacionais promoveram a ampliação de ofertas e do alcance da Educação de Jovens e Adultos, de maneira formal, aos níveis de ensino básico como o nível fundamental e o nível médio. Tal fato permitiu o aumento do acesso à formação profissional.

O projeto MOBRAL durou até 1985, sendo duramente criticado pois visava conduzir a pessoa a adquirir as técnicas de escrita, leitura e cálculo como meio de integração a comunidade, sem levar em consideração a preocupação com a real formação do ser humano e sua cultura cotidiana, além da ausência de pensamento crítico. Acabou sendo substituído pelo projeto *Fundação Educar*.

O Ensino Supletivo foi apresentado como um projeto de escola do futuro em que a profissionalização era compatível a com a modernização socioeconômica ao final dos anos 70. A aprendizagem nesses moldes ficou a cargo do *SENAI – Serviço Nacional de Aprendizagem Industrial* (1942) – e do *SENAC – Serviço Nacional de Aprendizagem Comercial* (1946). Essa qualificação foi uma medida pretendida pelo governo para, prioritariamente, formar mão de obra barata visando o mercado de trabalho, modelo executado até os dias atuais.

Os anos 90

Segundo Viegas e Moraes (2017) com o processo de redemocratização política, a volta a liberdade de expressão e a organização de movimentos sociais urbanos e rurais permitiram a experimentação e a inovação pedagógica na Educação de Jovens e Adultos. Esse processo de mudança e revitalização espelhou-se na *Assembleia Nacional Constituinte* por meio da conquista do direito universal ao Ensino Fundamental público e gratuito, independente de idade, legitimado pelo artigo 208 da Constituição de 1988. Além disso, a Carta Magna estabelecia um prazo de dez anos para que tanto o governo quanto a sociedade civil concentrassem esforço conjunto para a erradicação do analfabetismo e a universalização do Ensino Fundamental, de maneira que 50% dos recursos vinculados à educação dos três níveis de governo deveriam ser dedicados a esses objetivos.

Nos anos 90, algumas ações do governo modificaram a estrutura que estava sendo criada, o que acabou atrasando todo o projeto proposto anteriormente. Uma dessas medidas foi a extinção da Fundação Educar; Com a opção do governo em negação por políticas públicas concretas, o plano educacional priorizou a Educação Básica, voltada para crianças de 7 a 14 anos, o que culminou com poucos avanços das iniciativas em erradicar o analfabetismo entre jovens e adultos. À época, pesquisas realizadas pelo Instituto Brasileiro de Geografia e Estatística (IBGE), apontaram que no ano de 1991, 20,1% da população brasileira com 15 anos ou mais era analfabeta.

Alguns movimentos surgiram logo no início da década com a motivação em remodelar o processo de ensino e aprendizagem na Educação de Jovens e Adultos. Dentre eles estava o *Movimento de Alfabetização* (Mova), que tratava a alfabetização segundo o contexto socioeconômico das pessoas alfabetizadas, inserindo-os no processo de aprendizagem como coparticipantes.

Em 1996, há o surgimento de um programa nacional promovido pelo Governo Federal: o *Programa de Alfabetização Solidária* (PAS), que se assemelhava aos programas referentes às campanhas das décadas de 40 e 50.

A promulgação da Lei de Diretrizes e Bases da Educação – LDB (1996) trouxe poucas mudanças no que se refere à Educação de Jovens e Adultos, com apenas dois artigos que acabam por reafirmar o direito de jovens e adultos trabalhadores ao ensino básico adequado às suas condições de estudo e o dever do poder público em oferecê-lo gratuitamente na forma de cursos e exames supletivos. Como única novidade dessa seção da lei, é apresentado o rebaixamento

das idades mínimas para a submissão dos candidatos aos exames supletivos em 15 anos para o Ensino Fundamental e 18 anos para o Ensino Médio. Porém, ainda em 1996, uma emenda constitucional alterou, dentre outros, o Art. 208 da constituição de 1988, retirando a obrigação do Estado em oferecer o Ensino Fundamental aos alunos que não o cursaram em idade própria, mantendo apenas o compromisso a gratuidade. Como principal consequência ao retrocesso, foi criado o *Fundo de Manutenção e Desenvolvimento do Ensino Fundamental e Valorização do Magistério* (FUNDEF), com a educação primária de jovens e adultos sendo excluída de tal orçamento (VIEGAS e MORAES, 2017, p. 468).

Em 1998, se destaca o *Programa Nacional de Educação na Reforma Agrária* cujo objetivo era atender às populações situadas nas áreas de assentamento. O programa era coordenado pelo *Instituto Nacional de Colonização Agrária* (INCRA).

Novo século, mudanças de base

O século XXI trouxe algumas tentativas em mudar o analfabetismo a nível nacional.

Segundo Viegas e Moraes (2017), em maio de 2000, foi aprovado o parecer CNE/CEB 11/2000. Com grande relevância, versa sobre as Diretrizes Curriculares Nacionais (DCNs) para a EJA sendo o documento oficial, até o momento, que rege as ações educativas nessa modalidade de ensino. Com uma visão crítica de especialistas no campo da EJA e contribuições da comunidade escolar, sua elaboração é um trabalho mais elaborado e que leva em conta as especificidades próprias dessa modalidade de ensino.

Ainda em 2000, houve a aprovação do Plano Nacional da Educação (sancionado no ano seguinte – Lei n. 10.172/2001), que visava a modificação geral em todos os níveis de ensino da Educação Básica. Nesse ponto, a diagnose da Educação de Jovens e Adultos é uma ferramenta importante para o entendimento de suas dificuldades, além das abordagens diversificadas devido ao seu caráter heterogêneo:

> Para atender a essa clientela, numerosa e heterogênea no que se refere a interesses e competências adquiridas na prática social, há que se diversificar os programas. Neste sentido, é fundamental a participação solidária de toda a comunidade, com o envolvimento das organizações da sociedade civil diretamente envolvidas na temática. É necessária, ainda, a produção de materiais didáticos e técnicas pedagógicas apropriadas, além da especialização do corpo docente (BRASIL, PNE, p. 41).

Já no governo de Luís Inácio da Silva, houve várias iniciativas e projetos no âmbito da EJA, além de uma mudança no olhar sobre essa modalidade. Inicialmente destacam-se aspectos positivos:

> É possível distinguir dois traços principais nas políticas de EJA do governo federal nesse período. O primeiro, essencialmente positivo e distintivo do governo anterior, foi a mudança da posição relativa da EJA na política educacional, atribuindo-se maior importância a esse campo, tanto no discurso quanto no organograma do governo e em suas ações. Embora a EJA continue a ocupar lugar secundário na agenda da política educacional do governo, houve um incremento na colaboração da União com os estados e municípios, por meio da institucionalização da modalidade no sistema de ensino básico, com sua inclusão nos mecanismos de financiamento e nos programas de assistência aos estudantes (alimentação, transporte escolar e livro didático) (DI PIERRO, 2010, p. 945).

Destacamos ainda a criação do *Fundo de Desenvolvimento da Educação Básica* - (FUNDEB) em substituição ao FUNDEF. A Lei n. 11.497/2009 regulamentou o direito à alimentação escolar e a inclusão da modalidade no *Programa Dinheiro Direto Na Escola*, além das resoluções do FUNDEB que incluíram a modalidade, entre 2004 e 2009, no Programa Nacional do Livro Didático, de Alimentação e de Transporte Escolar.

De 2009 a 2010, O Brasil participou da *VI Conferência Internacional de Educação de Adultos* – CONFINTEA, realizada em Belém (PA) e organizada pela UNESCO, na qual se promoveu a discussão de questões específicas visando a |EJA.

Já no Plano Nacional de Educação – PNE (2011- 2020) foram estipuladas vinte metas, entre as quais as 9ª e 10ª tratam da abordagem a ser dada a Educação de Jovens e Adultos.

> Meta 9: Elevar a taxa de alfabetização da população com 15 anos ou mais para 93,5% até 2015 e erradicar, até o final da década, o analfabetismo absoluto e reduzir em 50% a taxa de analfabetismo funcional até o final da década (BRASIL, PNE, 2010).

> Meta 10: Oferecer, no mínimo, 25% das matrículas de educação de jovens e adultos na forma integrada à educação profissional nos anos finais do ensino fundamental e no ensino médio (BRASIL, PNE, 2010).

Embora, o PNE gozasse de um certo nível de consenso entre todas as partes que o discutiram, por motivos internos ao Governo Federal, foi deixado de lado e retornou com força em 2014, quando foi sancionado pela Lei 13.005/2014 em um plano de dez anos (2014 – 2024). Em tese, não houve mudanças sensíveis, com a quantidade de metas sendo mantidas, principalmente no que se refere à Educação de Jovens e Adultos.

Em 2017, ocorreu a promulgação da *Base Nacional Comum Curricular* - BNCC que visa renovar os parâmetros educacionais. Destaca-se, porém, a ausência de parâmetros claros referentes à Educação de Jovens e Adultos e suas demandas. Dessa maneira, há a inexistência de discussões específicas levando em conta as características pautadas na diversidade e heterogeneidade presentes na EJA, pois a BNCC possui caráter unificador e homogêneo. Ao desconsiderar as especificidades dessa modalidade, deve haver uma "adaptação" das instituições escolares sem levar em conta as condições diferenciadas características da EJA. (FERREIRA, 2019, p. 11).

Analisando os dados e a história abordados até o momento, desde o século XX, é seguro afirmar que o Brasil ainda está longe de erradicar o analfabetismo, seja por políticas públicas mal estruturadas ou mal formuladas, seja pela ausência de discussão em todas as esferas do ensino. É evidente a invisibilidade sofrida pela EJA na elaboração e aplicação de projetos e processos voltados ao ensino. Nesse ponto, cabe citar Paulo Freire que, com sua pedagogia de inclusão do sujeito no processo de aprendizagem, exemplifica o porquê e a importância das discussões a respeito das peculiaridades da EJA:

> Nosso papel não é falar ao povo sobre a nossa visão do mundo, ou tentar impô-la a ele, mas dialogar com ele sobre a sua e a nossa. Temos de estar convencidos de que a sua visão do mundo, que se manifesta nas várias formas de sua ação, reflete a sua situação no mundo, em que se constitui (FREIRE, 2020, p. 120).

Organização

A **EJA** é ofertada tanto no ensino presencial, como à distância. Hoje, o programa é dividido em etapas, com abrangência do Ensino Fundamental ao Médio.

EJA - Ensino Fundamental: destinada a jovens a partir de 15 anos que não completaram a etapa entre o 1º e o 9° ano. Tem duração média de 2 anos para a conclusão.

EJA - Ensino Médio: destinada a alunos maiores de 18 anos que não completaram o Ensino Médio, que completa a Educação Básica no Brasil. Ao concluir essa etapa, o aluno estará apto a realizar provas de vestibular e Enem, para ingressar em universidades. O tempo médio de conclusão é de 18 meses.

No âmbito do Município do Rio de Janeiro, região de atuação do pesquisador, o Programa de Educação de Jovens e Adultos – PEJA para o Ensino Fundamental, segue a seguinte distribuição:

PEJA I – 1º ao 5º ano

A. Bloco I – Alfabetização de Jovens e Adultos.
B. Bloco II – 4º e 5º anos.

PEJA II – 6º ao 9º ano

A. Bloco I – 6º e 7º anos.
B. Bloco II – 4º e 5º anos.

ENCCEJA[3] - Exame Nacional para Certificação de Competências de Jovens e Adultos

O Exame Nacional para Certificação de Competências de Jovens e Adultos (Encceja) foi realizado pela primeira vez em 2002 para aferir competências, habilidades e saberes de jovens e adultos que não concluíram o Ensino Fundamental ou Ensino Médio na idade adequada. É realizado pelo Inep em colaboração com as secretarias estaduais e municipais de educação. O Exame é aplicado pelo Inep, mas a emissão do certificado e declaração de proficiência é responsabilidade das Secretarias Estaduais de Educação e Institutos Federais de Educação, Ciência e Tecnologia, que firmam Termo de Adesão ao Encceja.

O Encceja é direcionado aos jovens e adultos residentes no Brasil ou no exterior que não tiveram a oportunidade de concluir seus estudos em idade própria e que atendam ao art. 38, §1º e §2º da Lei de Diretrizes e Base (LDB), a Lei 9.394 de 20 de dezembro de 1996: tenham, no mínimo, 15 anos completos na data de realização do Exame, para quem busca a certificação do ensino fundamental; ou tenham, no mínimo, 18 anos completos na data de realização do Exame, para quem busca a certificação do ensino médio.

[3] Disponível em: < https://www.gov.br/inep/pt-br/areas-de-atuacao/avaliacao-e-exames-educacionais/encceja>. Acesso em 12/10/2020

5 INTRODUÇÃO À CRIPTOGRAFIA

Ao longo da história, o ser humano buscou formas eficientes de comunicação. Uma dessas formas, a criptografia, sempre foi uma ferramenta importante para as nações e reinos do mundo, seja para a transmissão de uma ordem de um general a seus exércitos, para um serviço de contraespionagem utilizado por reis e rainhas, ou ainda, para simples jogos mentais de lógica. Sua importância veio da necessidade de se manter em segredo estratégias de guerra, o que gerou a necessidade de se criar símbolos, códigos e técnicas para codificar e decodificar mensagens.

Por conta disso, grupos e departamentos foram criados para a elaboração de códigos[4] e cifras e, ao mesmo tempo, para a decodificação de qualquer mensagem que fosse interceptada, criando assim uma disputa intelectual entre os reinos e nações.

O desenvolvimento e os desdobramentos de técnicas alternativas para se criar ou decifrar um código propiciou a evolução da criptografia pautada cada vez mais na matemática praticada em cada época. Ao ser revelada a fraqueza de um código, este torna-se inútil e imediatamente provoca o desenvolvimento de um novo código, que vigorará até que outros consigam decifrar seus pontos fracos e assim sucessivamente.

Há vários relatos históricos de episódios que envolvem criação e manipulação de códigos em motins, batalhas e, até mesmo, guerras. Tal tática servia para confundir os "inimigos" de forma a obter informações privilegiadas e mais importantes para o planejamento de ataque ou defesa a um território pré-determinado.

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante, se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2003, p.13)

[04]Código e Cifra têm diferentes significados. Um código secreto é um sistema no qual toda palavra ou frase da sua mensagem é trocada por outra palavra, frase ou símbolos, alterando o sentido da mensagem. Uma cifra é um sistema onde cada letra da sua mensagem é substituída por outra letra ou símbolo. A cifra envolve uma chave criptográfica, enquanto o código não. Os códigos podem ser usados em conjunto com as cifras para que a mensagem fique ainda mais difícil de ser decifrada. Como exemplo de código, temos os familiares códigos de barras que se encontram vulgarmente na maioria dos produtos à venda.

Durante as guerras mundiais, havia a necessidade em desenvolver tecnologia para fins militares. Duas dessas tecnologias eram referentes a comunicação em geral, tanto para a informação enviada como para a informação interceptada: o rádio transmissor e os radares.

Tais dispositivos foram associados a máquinas cifradoras, cuja representante mais importante foi a Máquina *Enigma* incorporada para uso pelos militares alemães ainda na década de 1920 e da qual daremos mais detalhes à frente.

5.1 ESTEGANOGRAFIA X CRIPTOGRAFIA

A base para uma comunicação secreta é a ocultação da mensagem.

Assim, temos duas vertentes a considerar: a *Esteganografia* e a *Criptografia.* No primeiro caso, a mensagem é ocultada de alguma forma, mas sem transformação. No segundo, a mensagem é transformada por algum tipo de técnica (cifragem[5]) como forma de ocultá-la.

Esteganografia é uma palavra de origem grega[6] que tem por definição a arte da escrita escondida. O primeiro uso registrado da palavra data do ano de 1499, no livro *Steganographia*, de Johannes Trithemius[7], porém sua prática vem de mais longe.

Em "As Histórias", Heródoto narra os conflitos entre Grécia e Pérsia (século V a.C.). Em uma das histórias, Histaeu que queria encorajar Aristágora de Mileto a revoltar-se contra o rei Persa, transmite suas instruções raspando a cabeça de um mensageiro e escrevendo a mensagem em seu couro cabeludo. Histaeu aguardou que o cabelo crescesse, protegendo assim

---

[05] A cifra é um ou mais algoritmos que cifram e decifram um texto. A operação do algoritmo costuma ter como parâmetro uma chave criptográfica. Cifragem é o processo de conversão de um texto claro para um código cifrado e decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado. Uma chave criptográfica é um valor secreto que interage com o algoritmo de encriptação. A fechadura da porta da frente da sua casa tem uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave na fechadura, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não. Disponível em: <https://pt.wikipedia.org/wiki/Criptografia#Chave_Criptogr%C3%A1fica>. Acesso em 15/05/2020.

[06] *Estegano* = esconder + *graphein* = escrita.

[07] **Johannes Trithemius** (1462 - 1516), também conhecido em obras portuguesas como João Tritêmio, é o pseudônimo de Johann Heidenberg, que foi um polímata e monge beneditino alemão ilustre na Renascença Alemã como lexicógrafo, cronista, criptógrafo e ocultista, e que influiu consideravelmente no desenvolvimento do ocultismo moderno e tardio. Foi, também, mestre dos igualmente ilustres Henrique Cornélio Agrippa e Paracelso.

O pseudônimo Tritêmio é uma lusitanização de *Trithemius*, demônimo e exônimo alatinado da sua terra-natal: a então aldeia alemã de Trittenheim. Disponível em:< https://pt.wikipedia.org/wiki/Johannes_Trithemius >. Acesso em 18/08/2020.

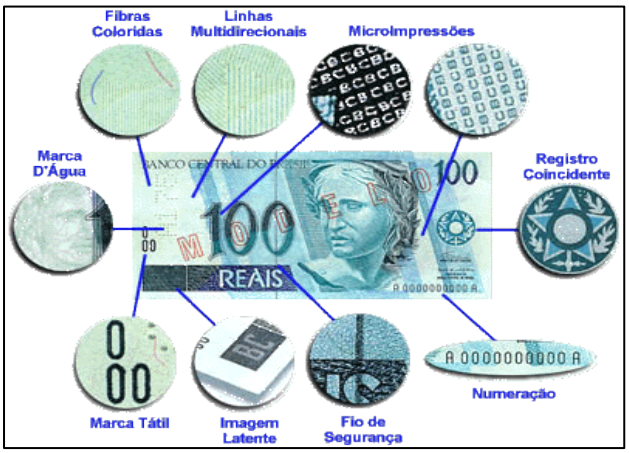
a mensagem enviada. O mensageiro, como não portava nada que o comprometesse, viajou sem ser importunado. Ao chegar a seu destino, o mensageiro raspou sua cabeça evidenciando a mensagem encaminhada. Há o fato que à época, a lentidão na transmissão era compreensível. Esse método, porém, tinha um ponto fraco: caso o mensageiro fosse revistado, o conteúdo da comunicação seria revelado.

Ainda atualmente, a Esteganografia inclui um amplo conjunto de métodos e técnicas podem ser empregadas em diversos meios, digitais ou não, tais como textos, imagens, áudios, vídeos, e espalhamento de espectro.

Destacam-se algumas aplicações práticas interessantes. Ela é uma das técnicas utilizadas para implementar mecanismos de verificação de direitos autorais em imagens e outras mídias. Além disso, pode ser utilizada para a divulgação de mensagens sem o conhecimento da existência dessas mensagens por parte de outros interessados.

Um exemplo interessante e atual pode ser verificado em cédulas, por exemplo, de 100 reais que possui diversos dispositivos de segurança contra fraudes:

Figura 1 – Dispositivos de segurança em cédulas de R$100,00



Fonte: Disponível em: <http://www.fraudes.org/>. Acesso em: 15/04/2020

Paralelamente ao desenvolvimento da Esteganografia e por conta de sua pouca eficácia em alguns casos, houve a evolução da *Criptografia*[8].

[8] Cripto vem do grego kryptos e significa esconder, ocultar. Grafia também vem do grego graphein, e significa escrever. Criptografia, portanto, significa escrita oculta ou escrita secreta. (TKOTZ, 2005, p.13)

Os primeiros registros obtidos da utilização de técnicas criptográficas datam de 2.000 a.C. na civilização egípcia.

A utilização, por escribas hebreus, de uma cifra de substituição[9] para a confecção do Livro de Jeremias por volta do séc. VI a.C., é um exemplo de como já se utilizavam técnicas criptográficas de modo sistemático.

César, no séc. I a.C., com uma cifra de transposição[10], simples mas eficiente à sua época (a cifra de César), marca a utilização do que viria a ser, nos anos que se seguiram e até a nossa época, uma das mais importantes aplicações de uso militar.

Mas, ao contrário da Esteganografia, a Criptografia tem como objetivo ocultar o significado da mensagem e não a mensagem em si.

Um exemplo de cifragem é a brincadeira infantil, onde crianças codificam bilhetes e enviam a outras crianças. Suponha que se deseja enviar a mensagem "Vamos estudar matemática hoje?". Intercala-se então as letras do nome do remetente, por exemplo, MATHEUS (chave), escondendo seu significado. Desta maneira, tem-se:

"**MVAATMHOESUS MEASTTUHDEAURS MMAATTEHEMAUTSICA MHATOTHJEEUS**?",

que será a mensagem a ser enviada sem precisar de ocultação.

A Criptografia leva grande vantagem sobre a Esteganografia pois torna o conteúdo da mensagem, em princípio, ilegível ao interceptador.

Devemos destacar ainda que existem dois tipos básicos de criptografia: as de chave simétrica (Figura 2) e as de chave assimétrica (Figura 3).

O primeiro utiliza uma única chave para cifrar e decifrar a mensagem; o segundo adota um par de chaves, uma para cifrar (chave pública) e outra para decifrar (chave privada) a mensagem.

---

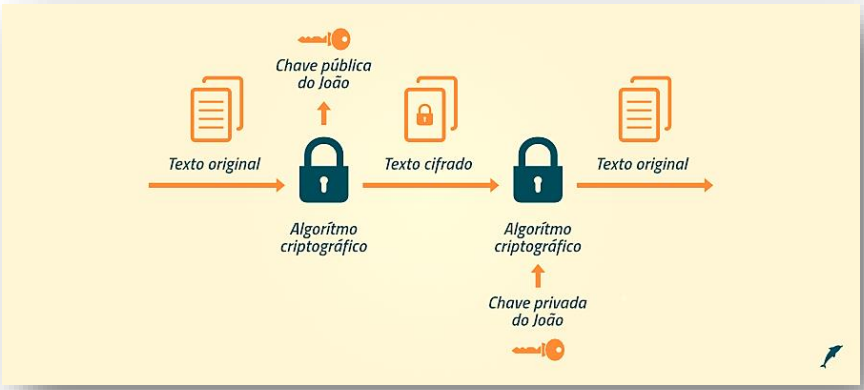
[9] Método de criptografia que opera de acordo com um sistema pré-definido de substituição alfabética. Para criptografar uma mensagem, unidades do texto - que podem ser letras isoladas, pares ou outros grupos de letras - são substituídas para formar a cifra.

[10] Método que procede à mudança de cada letra (ou outro qualquer símbolo) no texto a cifrar para outra (sendo a decifração efetuada simplesmente invertendo o processo).

Figura 2 – Esquema de Criptografia de Chave Simétrica

Fonte: Disponível em: <https://cryptoid.com.br>. Acesso em 15/04/2020.

Figura 3 – Esquema de Criptografia de Chave Assimétrica



Fonte: Disponível em: <https://cryptoid.com.br>. Acesso em 15/04/2020.

A partir daí, começa a ser desenvolvida a *Criptoanálise*, arte de tentar descobrir o texto cifrado e a lógica do processo utilizado em sua encriptação (chave).

O registro mais antigo que se tem notícia a respeito de um trabalho publicado sobre Criptoanálise vem dos árabes que eram matemáticos muito respeitados e desenvolveram estudos nessa área. Abu *Yusuf Ya 'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi*, conhecido como o filósofo dos árabes, foi autor de 290 livros sobre medicina, astronomia,

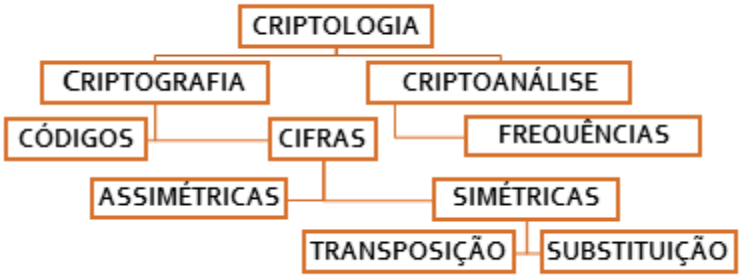
matemática, linguística e música. Seu maior tratado, contudo, foi redescoberto apenas em 1987 no Arquivo *Sulaimaniyyah Ottoman* em Istambul, na Turquia, e é intitulado "Um Manuscrito sobre Decifração de Mensagens Criptográficas" e versava sobre a análise de freqüências em textos encriptados.[11]

Tem-se por fim, a *Criptologia*, disciplina científica que reúne e estuda os conhecimentos e técnicas necessários à Criptoanálise e à Criptografia.

De acordo com Singh (2003), faremos alguns comentários sobre os métodos criptográficos mais importantes ao longo da história, cujo caráter mais simples nos permite fácil aplicabilidade em temas voltados para a Educação Básica: as cifras de transposição e substituição.

O esquema a seguir mostra o caráter de nossa exposição até aqui e o que se seguirá:

Figura 4 - Organograma - Criptologia



Fonte: O autor, 2020.

[11]Disponível em: <https://pt.wikipedia.org/wiki/Criptoan%C3%A1lise>. Acesso em 15/04/2020

5.2 CIFRAS DE SUBSTITUIÇÃO[12]

Neste tipo de cifra, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição alfabética. Historicamente, as principais cifras de substituição podem ser subdivididas em monoalfabéticas ou polialfabéticas.

5.2.1 **Cifra de substituição monoalfabética**

Em meados do séc. X, os árabes já usavam a Criptografia para codificar informações sobre impostos, bem como alguns segredos de Estado. Em geral, o alfabeto cifrado era uma permutação das letras do alfabeto original, rearranjadas de forma pré-determinada. Havia também auxílio de alfabetos que continham símbolos diferentes às letras originais. Esse tipo de cifra é chamado de Cifra de substituição monoalfabética, onde cada letra é substituída por um símbolo ou letra de acordo com um pré-arranjo do alfabeto considerado. O mais comum era o deslocamento linear das letras do alfabeto, conhecida por *Cifra de César*.[13]

Figura 5 - Cifra de César

Fonte: Disponível em: <http://clubedosgeeks.com.br>. Acesso em: 15/04/2020.

[12]As cifras de substituição podem ser de substituição simples, de substituição polialfabética, de polígramos, onde se utiliza um grupo de letras ao invés de uma única letra para a substituição da mensagem, por exemplo, “RAF” pode corresponder a “MAT”; e ainda, de substituição por deslocamento: ao contrário da cifra de César, não usa um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra "LUZIA" utilizando o critério de rotação "035", seria substituir "L" pela letra que está 0(zero) posições a frente no alfabeto, o "U" pela letra que está 3 (três) posições a frente, e assim por diante, repetindo-se o critério se necessário. Esses dois últimos casos, não serão abordados neste texto.

[13]Conta a história que Júlio César, Imperador romano, utilizava um código nas mensagens enviadas a seus generais, um sistema simples de substituição, no qual cada letra da mensagem original era trocada pela letra que se situa três posições à sua frente. Ficando da seguinte forma: Cada letra “A” era substituída pela Letra “D”, “B” por “E” e assim sucessivamente. Qualquer cifra que tenha esse padrão é considerada uma cifra de César. O alfabeto possui 26 letras, dessa forma pode-se cifrar o texto de 26 formas diferentes. (Tkotz, 2005)

Vejamos um exemplo no quadro a seguir, com deslocamento linear de 9 letras e início na letra J:

Quadro 1 - Alfabeto cifrado – Cifra de César

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

Fonte: O autor, 2020.

Desta maneira, a mensagem:

HÁ ESPIÕES ENTRE OS ADMINISTRADORES DO ESTADO

após a codificação se torna:

QJ NBYRXNB NWCAN XB JMVRWRBCAJMXANB MX NBCJMX.

Vale destacar que os espaços entre palavras e pontuações podem ser representados por símbolos ou números.

5.2.2 **Cifra de substituição polialfabética**

Em alguns momentos da História, a balança da guerra entre criptoanalistas e criptógrafos estava pendendo ora para o lado dos primeiros, ora para o lado dos últimos, com uma ligeira vantagem para os criptoanalistas que acabavam por decifrar os novos códigos inventados de tempos em tempos. Esse fato levou os criptógrafos a procurarem uma cifra mais forte que pudesse equilibrar novamente a "batalha", ou até mesmo vencê-la.

Em 1466, o italiano Leon Battista Alberti[14] publicou um ensaio denominado *De Cifris* em que apresentava o que acreditava ser uma nova forma de cifra. Há época, todas as cifras de

[14] **Leon Battista Alberti** (1404 — 1472) foi um arquiteto, teórico de arte e humanista italiano. Ao estilo do ideal renascentista, foi filósofo da arquitetura e do urbanismo, pintor, músico e escultor. Sua vida é descrita em *Vite*, de Giorgio Vasari. Personificou o ideal renascentista do «*uomo universale*». Disponível em: < https://pt.wikipedia.org/wiki/Leon_Battista_Alberti>. Acessado em 18/08/20.

substituição necessitavam de apenas um único alfabeto cifrado para codificar uma mensagem. Alberti propôs o uso de, pelo menos, dois alfabetos cifrados de forma alternada, de modo a confundir os criptoanalistas. Assim, seu dispositivo consistia em um disco com dois anéis concêntricos, dos quais o exterior era fixo e o interior móvel. No exterior encontravam-se os algarismos de 1 a 4 e o alfabeto latino com exclusão das letras H, J, Q, W e Y, de baixa frequência na língua italiana. No anel interior móvel estava gravado o mesmo alfabeto em minúsculas com acréscimo de “&”, “y”, “k” e “h” ' em ordem aleatória. A grande vantagem desse tipo de cifra é que a mesma letra do texto original não necessariamente aparece como uma única letra no texto cifrado.

Figura 6 - Disco de Alberti

Fonte: Disponível em: <https://www.creativeescaperooms.com> Acessado em: 15/05/2020.

A proposta de Alberti foi aprimorada por alguns estudiosos, entre eles o alemão Johannes Trithemius[15], o italiano Giovanni Porta[16]e por fim, o francês Blaise de Vigenère[17]. Este último examinou detalhadamente as ideias de Alberti, Trithemius e Porta adaptando-as de

[15]**Johannes Trithemius** (1462 - 1516), também conhecido em obras portuguesas como **João Tritêmio**,[1] é o pseudônimo de **Johann Heidenberg**, que foi um polímata e monge beneditino alemão ilustre na Renascença Alemã como lexicógrafo, cronista, criptógrafo e ocultista, e que influiu consideravelmente no desenvolvimento do ocultismo moderno e tardio. Disponível em: <https://pt.wikipedia.org/wiki/Johannes_Trithemius>. Acesso em 26/08/2020.

[16]**Giovanni Battista Della Porta** (1535 – 1615), italiano nascido em Vico Equense foi criptógrafo, matemático, físico, artista, química(o), inventor, dramaturgo, astrólogo, filósofo, médico, astrônomo. Seus principais interesses eram filosofia, cosmologia, alquimia e dramaturgia. Em 1563 publicou uma obra de criptografia, o *De Furtivis Literarum Notis*, na qual descreve o primeiro exemplo de substituição poligráfica cifrada, acenando para o conceito de substituição polialfabética.[1] Por esta obra é considerado o maior criptógrafo do Renascimento. Disponível em: <https://pt.wikipedia.org/wiki/Giovanni_Battista_della_Porta>. Acesso em 26/08/2020.

[17]**Blaise de Vigenère** (1523 - 1596) foi criptógrafo, matemático, diplomata, escritor, astrólogo francês. Autor de várias obras, incluindo o *Traicte de Chiffres* (1585). Neste descreve a cifra de autochave que inventara, a primeira cifra deste tipo não quebrável trivialmente. Disponível em: <https://pt.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re>. Acesso em 26/08/2020.

forma a criar uma cifra, mais coerente, coesa e poderosa. A cifra ficou conhecida como *Cifra de Vigenère*.

Quadro 2 - Quadrado de Vigenère

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

Fonte: O autor, 2020.

Esta cifra especial é formada por até vinte e seis alfabetos distintos para criar a mensagem cifrada. Primeiramente, monta-se o quadrado de Vigenère, um alfabeto normal seguido de vinte e seis alfabetos cifrados, com um deslocamento de uma letra em relação ao anterior. Como exemplo, uma pessoa pode cifrar a primeira letra de acordo com a linha 1, a segunda letra de acordo com a linha 10, a terceira de acordo com a linha 26, e assim por diante.

Para decifrar a mensagem, é necessário saber que linha do quadrado de Vigenère foi usada para a cifragem de cada letra, por isso deve existir um sistema previamente conhecido para a alternância entre as linhas. Em geral, utilizava-se uma palavra-chave no início da mensagem, que determinava a ordem a ser cifrada para o restante das letras componentes da mensagem.

Por exemplo, a mensagem “FIQUEM EM CASA”, será codificada tendo em vista a palavra-chave “SAÚDE” onde serão utilizados cinco alfabetos dos vinte e seis, e a primeira letra é codificada pelo alfabeto que se inicia com a letra S, a segunda letra com o alfabeto que se inicia com a letra A, e assim sucessivamente, mantendo sempre o ciclo dos cinco alfabetos.

Quadro 3 - Mensagem cifrada – Cifra de Vigenère

Mensagem	**F**	**I**	**Q**	**U**	**E**	**M**	**E**	**M**	**C**	**A**	**S**	**A**
Chave	S	A	U	D	E	S	A	U	D	E	S	A

Fonte: O autor, 2020.

Assim, as letras F, M e S da mensagem original serão codificadas com o alfabeto que se inicia pela letra S. As letras I, E e A, pelo alfabeto que se inicia por A; Q e M pelo alfabeto que se inicia por U; U e C pelo alfabeto que se inicia por D; e, finalmente, E e A, pelo alfabeto que se inicia por E.

A mensagem cifrada será: “XIKXIEEGFEKA”

5.2.2.1 A Máquina ENIGMA

A importância do uso de cifras polialfabéticas pode ser avaliada quando sabemos que foi a base da mais famosa máquina de encriptação de mensagens: a *Enigma*.

Desenvolvida ao final da Primeira Guerra Mundial, em 1918, pelo alemão Arthur Sherbius[18], esta máquina cifrante era basicamente uma versão elétrica do disco de Alberti. Tinha a aparência de uma máquina de escrever e o modelo mais antigo tinha três elementos básicos: um teclado para introduzir a mensagem que se quereria cifrar, um roteador para cifrar cada letra da mensagem e um mostrador para visualizar a mensagem cifrada. Todo esse aparato contido numa caixa de dimensões relativamente reduzidas.

Para ser utilizada, era preciso um cuidado extremo, seja na configuração da chave de acionamento da máquina ou no uso manual de seus códigos. Além disso, a chave de configuração deveria ser trocada diariamente, sob o risco de ser rastreada e seus códigos decifrados por tecnologias equivalentes à própria máquina.

[18]**Arthur Sherbius** (1878 – 1929), foi um engenheiro electrotécnico alemão que inventou e patenteou (*Sch 52638 IX/42n*) em 1918 a Máquina Enigma para cifrar mensagens e de uso comercial. Ao constatar que na Alemanha o uso de sistemas de criptografia se encontrava bastante atrasado, decidiu construir uma máquina que permitisse fazer a codificação de mensagens de modo automático, através de rotores. A Marinha alemã interessou-se pelas potencialidades para uso militar do dispositivo, mas considerava a máquina pouco prática. Só mais tarde, graças a melhorias na máquina, conseguiu alguma receptividade dos militares. Disponível em: <https://pt.wikipedia.org/wiki/Arthur_Scherbius>. Acesso em 26/08/2020.

Na máquina havia três rotores, cada um com vinte e seis possíveis posições, a posição inicial dos misturadores formava a chave da cifra. (TKOTZ, 2005)

Vamos calcular o total de cifras possíveis:

- Total de posições possíveis dos três rotores simultaneamente:

$$26 \times 26 \times 26 = 17.576$$

- Sequência dos três rotores: $3! = 6$
- Total de possibilidades de substituição de 6 pares de letras: $\frac{26!}{2^6 \times 6! \times 14!} = 100.391.791.500$
- Total de cifras possíveis:

$$17.576 \times 6 \times 100.391.791.500 = 10.586.916.764.424.000$$

Este quantitativo de cifras possíveis é responsável pelo sucesso da Enigma, já que seria humanamente impossível decifrar as mensagens por tentativas de uso de cada cifra possível.

A facilidade de uso e a suposta indecifrabilidade do código empregado foram as principais razões para a sua popularidade e amplo uso durante a Segunda Guerra Mundial.

O código foi, no entanto, quebrado em 1933 por matemáticos da Polónia com a ajuda de meios eletromecânicos. Versões aperfeiçoadas de tais meios criadas pelos britânicos em Bletchley Park[19], sob a liderança do matemático Alan Turing[20], aceleraram o processo de decodificação das Enigmas usadas pela Marinha alemã.

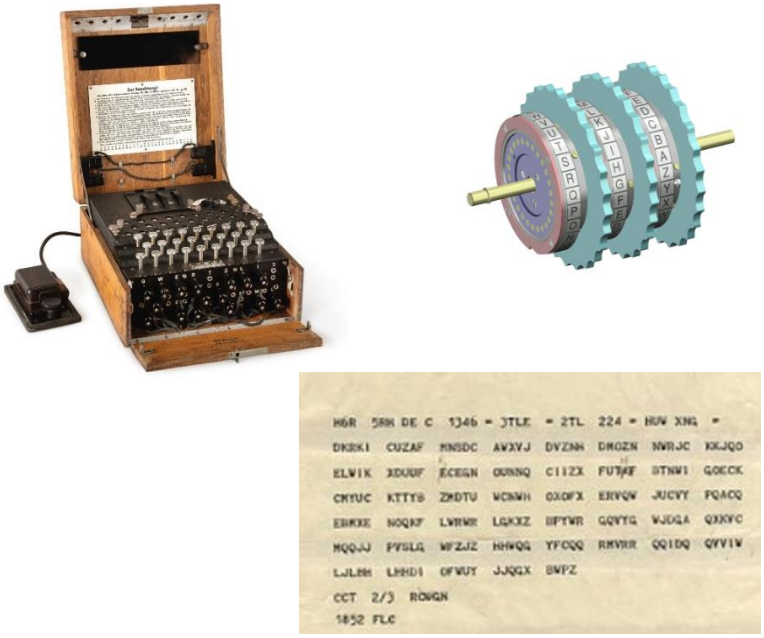
A descoberta de informações contidas nas mensagens que o código da Enigma não protegeu é geralmente tida como responsável pelo fim da Segunda Guerra Mundial pelo menos um ano antes do que seria de prever.

---

[19]**Bletchley Park foi** uma antiga instalação militar secreta localizada em Bletchley na Inglaterra, onde funcionou a Government Code and Cypher School (GC&CS), na qual se realizaram os trabalhos de decifração de códigos alemães durante a Segunda Guerra Mundial, sendo um dos mais conhecidos a decifração da Enigma. De acordo com o historiador oficial da inteligência britânica, a "ultra" inteligência produzida em Bletchley reduziu a guerra de quatro para dois anos e que, sem ela, o resultado da guerra teria sido incerto. Disponível em: <https://pt.wikipedia.org/wiki/Bletchley_Park>. Acesso em 15/04/2020.

[20]**Alan Turing** (1912 – 1954), foi um matemático, lógico, criptoanalista e cientista da computação britânico. Foi influente no desenvolvimento da ciência da computação e na formalização do conceito de algoritmo e computação com a máquina de Turing, desempenhando um papel importante na criação do computador moderno. Foi também pioneiro na inteligência artificial e na ciência da computação. É conhecido como o pai da computação. Disponível em: <https://pt.wikipedia.org/wiki/Alan_Turing>. Acesso em 26/08/2020.

Figura 7 - Máquina ENIGMA, rotores e mensagem cifrada



Fonte: Disponível em: <https://www.invaluable.com>. Acesso em 15/04/2020.

5.3 CIFRAS DE TRANSPOSIÇÃO

Transpor significa alterar a posição inicial de algo sem acrescentar novos elementos. Desta forma, quando um texto é alvo de uma transposição, os caracteres originais são preservados, permutando-se apenas suas posições relativas ao texto em questão.

Podemos, a título de exemplo, destacar duas cifras de transposição: o Bastão de Licurgo e a Viagem do Cavaleiro.

A primeira revela uma "máquina" de criptografia, a mais antiga já conhecida: um bastão de madeira fornecido a Almirantes e Generais que, quando em missões, portavam-no para cifrar mensagens. Esse bastão era conhecido como *scytalae* ou Bastão de Licurgo.

Tratava-se de uma tira de tecido, usualmente de couro, enrolada no bastão. Após escrever uma frase ou texto, desenrolava-se a tira de forma a rearranjar as letras, codificando a mensagem escrita. Podendo ser disfarçada de cinto, essa mesma tira era entregue ao destinatário que possuía um bastão semelhante ao primeiro, para que a mensagem enviada fosse decodificada, revelando a frase ou texto original.

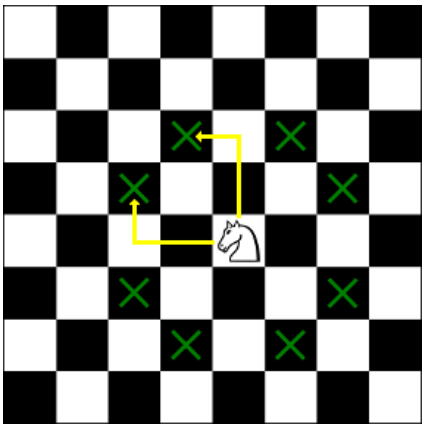
Figura 8 - *Scytalae*

Fonte: Disponível em <http://mathcenter.oxford.emory.edu/site/math125/transpositionCiphers>. Acesso em 23/07/2020.

A segunda das cifras citadas, a Viagem do Cavaleiro, faz alusão ao tabuleiro de xadrez, constituído por uma grade quadrada de 64 casas dispostas em 8 linhas e 8 colunas. A sequência a ser considerada é sempre dada por movimentos possíveis do cavalo, cujas trajetórias se assemelha à letra L.

De fato, o movimento leva em consideração retângulos de 3 x 2 casas, na vizinhança onde o cavalo se situa, de maneira que só é permitida a ocupação dos extremos das diagonais desses retângulos mais distantes da posição do cavalo.

Figura 9 - Movimentos possíveis do cavalo no tabuleiro de xadrez



Fonte: Disponível em: < https://docs.kde.org/trunk5/pt_BR/kdegames/knights/piece-movement.html>.Acesso em 23/07/2020.

Ao fixar o ponto de partida em uma casa específica, pode-se fazer com que o cavalo ocupe todas as 64 casas sem passar duas vezes pela mesma casa. Existem inúmeras soluções

possíveis para tal fato, bastando escolher uma delas para iniciar uma sequência obtendo uma transposição difícil de se identificar.

Quadro 4 - Exemplo de possibilidade para a Viagem do Cavaleiro

26	49	12	61	24	47	10	59
13	62	25	48	11	60	23	46
50	27	40	29	36	33	58	9
63	14	35	32	41	30	45	22
16	51	28	39	34	37	8	57
3	64	15	54	31	42	21	44
52	17	2	5	38	19	56	7
1	4	53	18	55	6	43	20

Fonte: O autor, 2020.

Nesse caso, o movimento se inicia pela casa inferior esquerda e segue de acordo com a numeração indicada.

Considere a mensagem a ser cifrada: **O ataque será à meia noite**

Utilizando a solução anterior proposta no Quadro 4, tem-se:

Quadro 5 - Viagem do Cavaleiro - Cifragem de "O ataque será à meia noite"

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

Fonte: O autor, 2020.

Observe-se que mesmo com as letras destacadas, ainda sim é difícil decodificar a frase sem saber onde começa e onde termina. Portanto, ao seguirmos a sequência apresentada anteriormente, conseguiremos decodificar e obter a frase original.

5.4 ANÁLISE DE FREQUÊNCIAS

Por conta da necessidade de decifrar mensagens, alguns estudiosos árabes, passaram a observar certos padrões e recorrências e começaram a desenvolver a criptoanálise, obtendo algum sucesso na descoberta de métodos para quebrar a cifra de substituição monoalfabética.

Destaca-se Al-Kindi, famoso cientista árabe que respondia pela alcunha de “o filósofo dos árabes”, que se utilizou de técnicas empregadas por teólogos para examinarem revelações contidas no Corão e desenvolveu uma técnica que lhe permitisse estudar a frequência com que as letras apareciam nas palavras do alfabeto. O sistema consistia em, conhecendo o idioma da mensagem, pesquisar um outro texto na mesma língua, longo o suficiente para preencher uma página. Depois disso, contar a frequência com que cada letra apareceria.

Em seguida, seria preciso examinar o criptograma e classificar seus símbolos de acordo com a frequência em que aparecessem. Por fim, relacionar as letras e símbolos mais frequentes selecionados, buscando uma relação entre ambos.

Figura 10 - Primeira página do Guia em Decifração de Mensagens de Al-Kindi

Fonte: Disponível em:< https://pt.wikipedia.org/wiki/Criptoan%C3%A1lise>. Acesso em: 15/05/2020.

Em relação à língua portuguesa, a tabela a seguir apresenta a frequência em que as letras de nosso alfabeto aparecem quando consideramos um texto de 100 letras:[21]

Tabela 3 - Frequência de letras do alfabeto português – Texto com 100 letras

Letra	Frequência (%)	Letra	Frequência (%)
A	14.63	N	5,05
B	1,04	O	10,73
C	3,88	P	2,52
D	4,99	Q	1,20
E	12,57	R	6,53
F	1,02	S	7,81
G	1,30	T	4,34
H	1,28	U	4,63
I	6,18	V	1,67
J	0,40	W	0,01
K	0,02	X	0,21
L	2,78	Y	0,01
M	4,74	Z	0,47

Fonte: Disponível em: < https://www.gta.ufrj.br>. Acesso em 20/05/2020.

Além disso:

- O comprimento médio das palavras em português do Brasil é de 4.53 letras.
- As vogais A, E, I, O, U e as consoantes S, R, N, D, M formam mais de 3/4 dos textos em português.
- A média de vogais a cada 10 letras é de 4.88.

Estatísticas mais complexas poderiam ser usadas, como considerar os pares de letras ou mesmo trios. Isto se faz para proporcionar mais informação ao criptoanalista. Por exemplo, as letras q e u vão quase sempre juntas em português, enquanto a q isolada é muito rara.

Mas por algum tempo ainda, os criptógrafos ficaram em vantagem ante os criptoanalistas. A cifra de Vigenère, por exemplo, tem por principal vantagem sua infalibilidade em relação à análise de frequência. Além disso, a a cifra possui um número enorme de chaves. Basta tomar o número de possibilidades que é de 26^{26}. A cifra de Vigenère era considerada indecifrável e tornou-se conhecida pela alcunha de *Le chiffre indéchiffable*.

[21]Nesta referência também se encontra um exemplo completo de criptoanálise por meio da análise de frequências.

5.5 CIFRAGEM MISTA – A SUPERCIFRA ADFGVX

A cifra ADFGVX[22] é um método que combina as técnicas de substituição e de transposição, além do quadrado de Políbio[23] 6 x 6 que inclui as 26 letras do alfabeto e os 10 algarismos. O método foi desenvolvido em 1918 pelo coronel Fritz Nebel do exército alemão no final da Primeira Guerra Mundial, a partir de uma versão menos complexa, a cifra ADFGX. A chave é constituída pelas letras A – D – F – G – V - X, escolhidas por serem muito distintas em código Morse evitando assim erros de transcrição nas comunicações via telégrafo.

Na época, a cifra ADFGVX prometia segurança máxima e foi posta em prática pela primeira vez no dia 5 de março de 1918, nas semanas que antecederam a ofensiva da Primavera (segunda batalha do Somme) iniciada a 21 de março.

Porém, as mensagens cifradas foram interceptadas pelo exército francês que, para desvendar esta cifra, recrutou o tenente Georges Painvin, um especialista em criptoanálise militar. Painvain atirou-se ao trabalho dia e noite, utilizando técnicas de análise de frequência estatística, baseado nas mensagens interceptadas todos os dias.

No início de junho de 1918, o exército alemão já se encontrava a 100 km de Paris e a situação estava desesperada. Painvain conseguiu, no entanto, decifrar a primeira mensagem às primeiras horas do dia 2 de junho. A mensagem decifrada era um pedido urgente de munições para uma dada localização. Com esta informação, os franceses perceberam quais eram os planos do inimigo e conseguiram conter a investida alemã.

A solução geral para esta cifra foi encontrada apenas em 1933.

Para exemplificar, considere o seguinte quadrado de Políbio 6 x 6:

---

[22]Veja SINGH, 2003, p. 410.

[23]Método criptográfico dos gregos, o **Quadrado de Políbio** funciona como um sistema de tabela de correlação e tem muitos derivados até o dia de hoje. Seus derivados revolucionaram a comunicação à distância nos dias. No quadrado a seguir poderíamos escrever a palavra DEFESA como 141521154311.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Disponível em: <https://www.segdigital.com.br/blog/criptografia-um-pouco-de-historia/>. Acesso em 14/08/2020.

Quadro 6 - Exemplo de Quadrado de Políbio – Cifra ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A	1	7	A	N	T	I
D	C	U	H	2	O	D
F	L	0	S	E	Y	9
G	P	B	V	K	4	Z
V	3	J	W	M	X	6
X	G	R	5	F	8	Q

Fonte: O autor, 2020.

Para criptografar uma dada frase com este diagrama, as letras que compõem a mensagem são substituídas pelos seus equivalentes da chave ADFGVX utilizada, considerando linha/coluna nesta ordem. Considere a mensagem:

LAVE SUAS MÃOS

Mensagem Original	L	A	V	E	S	U	A	S	M	A	O	S
Mensagem Cifrada	FA	AF	GF	FG	FF	DD	AF	FF	VG	AF	DV	FF

A mensagem cifrada é então organizada por linhas numa tabela baseada numa chave de tamanho variável de acordo com a dimensão da mensagem.

Supondo que a chave criptográfica é a palavra **MEDO,** obtém-se:

M	**E**	**D**	**O**
F	A	A	F
G	F	F	G
F	F	D	D
A	F	F	F
V	G	A	F
D	V	F	F

O passo seguinte é ordenar a chave por ordem alfabética e transpor a mensagem cifrada por colunas:

D	**E**	**M**	**O**
A	A	F	F
F	F	G	G
D	F	F	D
F	F	A	F
A	G	V	F
F	V	D	F

A mensagem final, a ser transmitida via rádio seria:

AFDFAFAFFFGVFGFAVDFGDFFF

5.6 A CRIPTOGRAFIA NOS DIAS ATUAIS

A possibilidade e velocidade na comunicação atualmente trouxe novos desafios à Criptografia. Em uma troca de mensagens em uma rede social, ou em uma operação bancária, é grande necessidade em proteger os dados enviados pelo remetente e recebidos pelo destinatário. Com a internet desbravando novos horizontes, com trocas de informações em microssegundos, há o aparecimento constante de novos desafios.

Imagine - se numa situação presente no cotidiano da maioria da população como uma compra online utilizando o cartão de crédito.

A loja virtual envia uma solicitação com seus dados ao banco e este responde a essa situação, aprovando ou não a compra. Aí surgem os problemas. Um deles é que seus dados podem ser interceptados por algum *hacker* dando – lhe assim acesso a todos os seus dados e informações bancárias. Outro desses problemas é que o banco tem que ter certeza se a loja que enviou as informações é de fato ou suspeita com possibilidades de um crime virtual.

Este é apenas um exemplo de como foi premente a necessidade de se produzirem métodos e códigos que, mesmo com a ajuda de um computador avançado, fossem difíceis de serem quebrados.

De acordo com Singh (2003), em meados da década de 70, na Califórnia, Whitfield Diffie[24] idealizou a cifra assimétrica, onde saber codificar não significava saber decodificar.

[24]**Bailey Whitfield 'Whit' Diffie** (Washington, D.C., 5 de junho de 1944) é um matemático e criptógrafo estadunidense. Pioneiro em criptografia de chave pública. Formado pelo Instituto de Tecnologia de Massachusetts (MIT) e entusiasta da contracultura, ele se interessava muito pela criptografia. Junto com Martin Hellman e Ralph Merkle criou o conceito de criptografia de chave pública. Disponível em: <https://pt.wikipedia.org/wiki/Whitfield_Diffie>. Acesso em 26/08/2020.

De forma a desenvolver essa ideia de criptografia, o método consistia em buscar funções únicas que fossem irreversíveis. Em uma analogia, pode-se pensar em quebrar uma lâmpada: quebrar é fácil, mas é impossível fazer com que volte a sua condição inicial. Diffie publicou sua ideia em 1975, e a partir daí, alguns cientistas se uniram para a busca dessas funções especiais que validassem a ideia da cifra assimétrica. No início, o otimismo era grande devido à nova grande ideia ser plausível e interessante. Mas com o passar dos meses, parecia improvável que essas funções existissem.

Em 1978, na costa leste dos Estados Unidos, Ronald Rivest[25], Adi Shamir[26] e Leonard Adleman[27], encontraram uma função capaz de tornar a ideia do trio anterior real e prática. Surge assim, no Massachusetts Institute of Technology (M.I.T.), a criptografia RSA.

De acordo com Coutinho (2014):

> Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachusetts Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no Netscape, o mais popular dos softwares de navegação da internet. (COUTINHO, 2014, p.3).

No RSA, a chave de encriptação é pública e é diferente da chave de decriptação que é secreta (privada). Esta assimetria é baseada na dificuldade prática da fatoração do produto de dois números primos grandes. É considerado um dos métodos mais seguros, já que até a presente data não foi possível quebrá-lo.

Um usuário do RSA cria e publica uma chave (pública) baseada em dois números primos grandes, que devem ser mantidos secretos. Qualquer um pode usar a chave pública para encriptar a mensagem, mas com métodos atualmente publicados, e se a chave pública for muito

---

[25]**Ronald Linn Rivest** (Schenectady, 6 de maio de 1947) é um matemático e criptologista estadunidense. Foi laureado com o Prêmio Turing de 2002, juntamente com Adi Shamir e Leonard Adleman, pelo algoritmo RSA. Disponível em: <https://pt.wikipedia.org/wiki/Ronald_Rivest>. Acesso em 26/08/2020.

[26]**Adi Shamir** (Tel Aviv, 6 de julho de 1952) é um criptógrafo israelita. Foi um dos inventores do algoritmo RSA e da criptoanálise diferencial. Disponível em: <https://pt.wikipedia.org/wiki/Adi_Shamir>. Acesso em 26/08/2020.

[27]**Leonard Max Adleman** (São Francisco, 31 de dezembro de 1945) é formado em ciência da computação e biologia molecular. É professor da Universidade do Sul da Califórnia. Foi laureado com o Prêmio Turing de 2002, juntamente com Ronald Rivest e Adi Shamir, pelo desenvolvimento do algoritmo RSA. Disponível em: <https://pt.wikipedia.org/wiki/Leonard_Adleman>. Acesso em 26/08/2020.

grande, apenas alguém com o conhecimento dos números primos pode decodificar a mensagem de forma viável.

Trata-se de uma das mais importantes aplicações da teoria dos números, em particular, as propriedades de congruências lineares e dos números primos.

No RSA, as chaves são geradas da seguinte forma:

1. Escolhe-se de forma aleatória dois números primos grandes, p e q, da ordem de 10^{100} pelo menos.
2. Calcula-se n = p.q.
3. Calcula-se a função *totiente*[28] em n: $\emptyset$ (n) = (p-1).(q-1).
4. Escolhe-se um inteiro e coprimo com n e tal que $1 < e < \emptyset$ (n).
5. Calcula-se d de forma que $d.e \equiv 1 \pmod{\emptyset (n)}$, ou seja, d é o inverso multiplicativo de e (mod $\emptyset$ (n)).

Desta forma tem-se as chaves pública (n,e) e privada (d,n).

A cifragem c da mensagem m será dada por $c \equiv m^e \pmod{n}$.

A decifragem m da mensagem c será dada por $m \equiv c^d \pmod{n}$.

Tomemos como exemplo a codificação da mensagem m = HELLO[29].

Considere-se os primos p = 29 e q = 37.

Temos a seguir: n = p.q = 1073, $\emptyset$ (n) = 28.36 = 1008 e escolhemos e = 71 < n =1073, MDC (71,1073) = 1.

A chave pública será dada então por (e,n) = (71,1073)

Para obtermos a chave privada será preciso calcular d tal que $71.d \equiv 1 \pmod{1008}$. Omitindo os respectivos cálculos, obtém-se d = 1079.

A chave privada será dada então por (d,n) = (1079,1073)

---

[28]Trata-se da função de Euler definida por $\emptyset (n) = \#\{x \in IN / x \leq n \text{ e MDC } (n,x) = 1\}$.

[29]Disponível em: <https://br.ccm.net/faq/9951-exemplo-de-algoritmo-assimetrico-rsa>. Acessado em 13/08/2020.

Para codificar uma mensagem, devemos identificar cada um de seus caracteres pelo código ASCII.[30]

Assim, no código ASCII, a mensagem HELLO será escrita como m = 7269767679.

A mensagem deve a seguir ser recortada em blocos contendo menos dígitos que n, ou seja, no caso em tela, blocos com 3 dígitos, da esquerda para a direita. Caso algum bloco tenha menos que 3 dígitos, deve ser completado com zeros.

Assim chega-se a

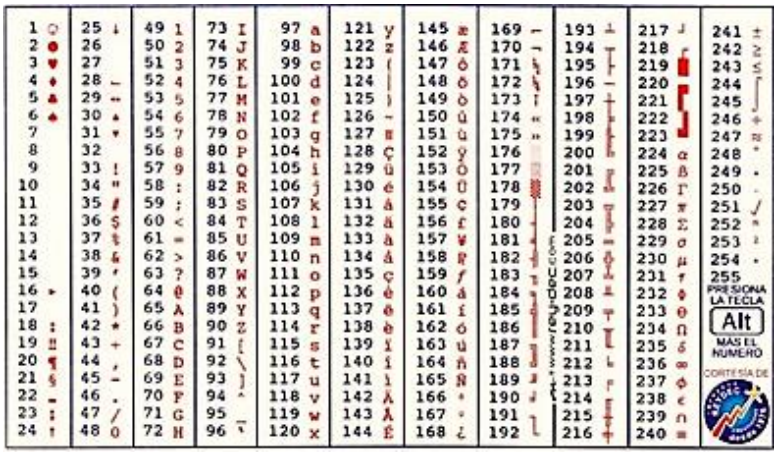
726 976 767 900

e podemos efetuar a cifragem por blocos por meio de $c \equiv m^e \pmod{n}$, n = 1073.

$$726^{71} \equiv 436 - 976^{71} \equiv 822 - 767^{71} \equiv 825 - 900^{71} \equiv 552$$

Portanto, a mensagem cifrada será dada por: 436822825552. O procedimento inverso é similar.

Figura 11 - Caracteres do código ASCII – Sistema decimal



Fonte: Disponível em: <https://br.pinterest.com/pin/611645193126909560>.Acesso em 15/08/2020.

[30]**ASCII** (do inglês *American Standard Code for Information Interchange*; "Código Padrão Americano para o Intercâmbio de Informação") — geralmente pronunciado [áski] — é um código binário (cadeias de bits: 0s e 1s) que codifica um conjunto de 128 sinais: 95 sinais gráficos (letras do alfabeto latino, sinais de pontuação e sinais matemáticos) e 33 sinais de controle, utilizando 7 bits para representar todos os seus símbolos. Disponível em https://pt.wikipedia.org/wiki/ASCII. Acessado em 13/08/2020.

A criptografia RSA atua diretamente na internet, por exemplo, em mensagens de e-mails, em compras on-line e o que você imaginar; tudo isso é codificado e recodificado pelo sistema RSA.

Sem nos alongarmos por não estar em consonância com os nossos propósitos neste texto, podemos ainda mencionar outros sistemas criptográficos como a **criptografia quântica,** um afluente em desenvolvimento da criptografia que utiliza os princípios da Mecânica Quântica para garantir uma comunicação segura e a **criptografía de curvas elípticas**, uma aproximação para a criptografia de chave pública com base na estrutura algébrica de curvas elípticas sobre corpos finitos.

6 SISTEMAS DE NUMERAÇÃO

A arte de contar e registrar as quantidades se desenvolveu em diferentes culturas. De acordo com registros remotos, os números teriam surgido há mais de 25.00 anos para resolver problemas relacionados à contagem, ao pastoreio, à agricultura e até mesmo por necessidades de ordem espiritual.

No desenvolvimento histórico das civilizações, em um dado momento em que as contagens foram se tornando mais extensas e complexas, foi necessária a adoção de uma sistematização de contagem para viabilizar os processos.

De acordo com Eves (2004), iniciou-se uma organização numérica em grupos convenientes limitando-os à correspondência empregada entre eles. Dois aspectos comuns a quase todos os sistemas seriam a relação feita um a um e o princípio aditivo. Essas duas regras de formação eram usadas pela maioria dos povos, mostrando a sua importância na forma de contar de toda a humanidade.

De forma esquematizada, se escolhe um número b como base e se atribui símbolos e nomes para representar cada número 1, 2, 3, ..., b. Para os números maiores do que b, os nomes e símbolos seriam combinações dos já escolhidos.

Utilizando a ideia anterior, a seguir serão apresentados alguns tipos de sistemas de numeração já utilizados ou ainda em uso.

6.1 SISTEMAS DE AGRUPAMENTOS SIMPLES

> Talvez o mais antigo tipo de sistema de numeração a se desenvolver tenha sido aquele chamado sistema de agrupamentos simples. Nessa modalidade de sistema escolhe-se um número b como base e adota-se símbolos para 1, b, b^2, b^3 etc. Então, qualquer número se expressa pelo uso desses símbolos aditivamente, repetindo-se cada um deles o número necessário de vezes. (EVES, 2004 – p.30)

O sistema de numeração hieroglífico egípcio era baseado nesse tipo de agrupamento. Observemos a figura a seguir:

Figura 12 - Sistema de numeração Egípcio

Fonte: EVES, 2004, p.31.

Ou seja, qualquer número poderia se expresso pelo uso desses símbolos de forma aditiva. Por exemplo, 12 = 1(10) + 2(1) e seria representado por ∩ **II**.

O número acima foi escrito da esquerda para a direita, mas não era o padrão egípcio. O modo habitual era a escrita da direita para a esquerda.

Uma outra civilização a recorrer a esse tipo de agrupamento foi a babilônica. Por não possuírem papiros e com pouco acesso a pedras convenientes, o material utilizado para a escrita era basicamente feito de argila. As inscrições eram impressas em tábuas de argila úmidas com estilos próximos a triângulos de forma que ao mudar a posição, produzia-se duas formas de caracteres semelhantes a cunhas (daí a representação em escrita cuneiforme).

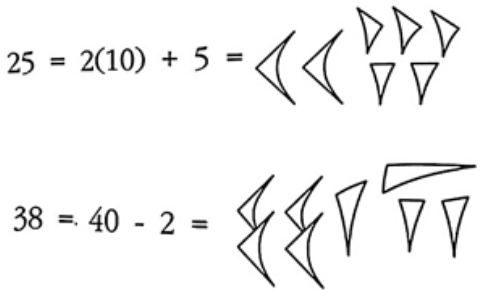
As tábuas, após marcação, eram cozidas em um forno até endurecer, de forma a obter um registro de forma permanente. Entre 2.000 a.C. a 200 a.C. os números menores que 60 eram representados por grupamentos simples de base 10.

Figura 13 - Símbolo subtrativo e os símbolos para 1 e 10

Fonte: Idem, p.32.

A figura a seguir nos mostra a construção dos números escritos com essa simbologia.

Figura 14 - Formação de números em escrita cuneiforme - Babilônia



Fonte: EVES, 2004, p.32.

Segundo Boyer (1996), dos vários sistemas de numeração usados pelos gregos, o sistema ático ou herodiânico é um dos dignos de serem mencionados. Foi chamado de ático porque os símbolos ocorriam com freqüência em inscrições atenienses e herodiânico por estar descrito num fragmento atribuído a Herodian, um gramático do segundo século.

Tratava-se de um sistema de numeração simples de base 10 formado pelas letras iniciais dos nomes atribuídos aos números.

Os símbolos para 1, 10, 10^2, 10^3, 10^4 eram I, Δ, H, X, M. O 5 possuía um símbolo especial uma forma antiga de π, a inicial da palavra grega pente (cinco). De forma que I, Δ, H, X, M eram as iniciais de *deka* (dez), *hekaton* (100), *Kilo* (mil), *Myriad* (dez milhares). Uma curiosidade é que o número cinco era utilizado com frequência sozinho ou em combinação com outros símbolos.

Figura 15 - Sistema ático ou herodiânico

Fonte: Idem

Por fim, há um exemplo final desse tipo de sistema de agrupamentos simples que utiliza a base 10: os numerais romanos cujos símbolos básicos são I, X, C, M para 1, 10, 100, 1000 que são acrescidos de V, L, D para 5, 50 e 500.

Nessa escrita, o princípio subtrativo era determinado pela posição entre dois símbolos de unidades distintas. Como a escrita é decrescente, um símbolo de unidade menor posicionado à esquerda de um símbolo de unidade maior significa a diferença entre as duas unidades. Essa simbologia, raramente era usada em tempos antigos, passando a ser utilizada em tempos mais modernos. Assim:

1944 = MDCCCCXXXXIIII	1944 = MCMXLIV
Medieval	Moderno

No uso do princípio subtrativo, seguem as regras: o I só pode preceder o V ou X, o X só pode preceder o L ou C e o C só pode preceder o D ou o M.

6.2 SISTEMAS DE AGRUPAMENTOS MULTIPLICATIVOS

O sistema de agrupamento simples evoluiu significativamente para um tipo de sistema que pode ser caracterizado como multiplicativo e que mescla símbolos alfanuméricos para representar um determinado número.

> Nesse tipo de sistema, após se escolher uma base b, adotam-se símbolos para 1, 2, ..., b - 1 e um segundo de símbolos para b, b^2, b^3, ... Empregam- se símbolos dos dois conjuntos multiplicativamente de maneira a mostrar quantas unidades dos grupos de ordem superior são necessárias. (EVES, 2004, p.33)

Como exemplo, suponha os nove primeiros números representados pelos símbolos habituais e as potências de 10 representadas pelas letras do alfabeto (a, b, c, ...) vejamos como seria a escrita do número 10917:

$$10917 = 1d9b1a7,$$

em que **1d** se refere a $1x10^4$ (10.000); **9b** se refere a $9x10^2$ (900); e, **1a** se refere a $1x10^1$ (10).

Um possível exemplo para esse tipo de sistema seria o sistema de numeração tradicional chinês-japonês.

Em Eves (2004), a explicação para o tipo de escrita ser dada na vertical é pelo fato de não haver material disponível para a escrita, como o papel. Os chineses e japoneses antigos eram obrigados a registrar seus achados em lâminas de bambu:

> A parte do caule do bambu situada entre dois nós era rachada longitudinalmente em tiras estreitas. Depois que essas tiras eram secas e raspadas, elas eram colocadas lado a lado e amarradas por quatro cordões transversais. A estreiteza das tiras fazia com que os caracteres fossem arranjados verticalmente, de cima para baixo, dando origem ao costume de escrever que perdurou até os tempos **mais** modernos, quando as lâminas de bambu foram substituídas pela tinta e o papel, materiais de escrita mais conveniente. (EVES, 2004, p. 34)

Figura 16 - Grupos básicos utilizados para a escrita no sistema chinês

Fonte: EVES, 2004, p.34.

6.3 SISTEMAS DE NUMERAÇÃO CIFRADOS

Em um sistema de numeração cifrado, há uma maior composição alfanumérica que nos demais.

Ao adotar uma base b, escolhem-se símbolos para 1, 2, ..., (b – 1); b, 2b, ..., (b – 1).b; b^2, $2b^2$, ..., (b – 1)b^2; e assim por diante.

A representação dos números acaba por ser compacta, embora a quantidade de memorização exigida seja enorme:

> O sistema de numeração grego, conhecido como jônico ou alfabético, cujas origens situam-se por volta do ano 450 a.C., é um exemplo desse sistema cifrado. Ele é decimal e emprega 27 caracteres – as 24 letras do alfabeto grego e três outras obsoletas: *digamma*, *koppa* e *sampi*. (EVES, 2004, p.35)

A figura a seguir ilustra o sistema jônico utilizando letras minúsculas (que só mais tarde vieram a substituir as maiúsculas). Tais equivalências tinham que ser memorizadas:

Figura 17 - Sistema de numeração Grego Jônico

1	α	alpha (alfa)	10	ι	iota	100	ρ	rho
2	β	beta	20	κ	kappa	200	σ	sigma
3	γ	gamma (gama)	30	λ	lambda	300	τ	tau
4	δ	delta	40	μ	mu	400	υ	upsilon
5	ε	epsilon	50	ν	nu	500	φ	phi
6	obsoleta	digamma	60	ξ	xi	600	χ	chi
7	ζ	zeta	70	ο	omicron	700	ψ	psi
8	η	eta	80	π	pi	800	ω	omega
9	θ	theta (teta)	90	obsoleta	koppa	900	obsoleta	sampi

Fonte: EVES, 2004, p.35.

Alguns exemplos desse uso, seriam: $31 = \lambda\alpha$ e $735 = \psi\lambda\varepsilon$.

Para números maiores, utilizavam-se barras ou acentos para acompanhar os símbolos.

Cabe mencionar outros sistemas de numeração cifrados como o egípcio (hierático e demótico), cóptico, hindu-bramante, hebreu, sírio e arábico antigo. Os três últimos eram sistemas de numeração alfabéticos.

6.4 SISTEMAS DE NUMERAÇÃO POSICIONAL

Segundo Eves (2004) neste sistema, define-se uma base e cada posição subsequente é determinada por uma potência consecutiva a essa base. À essas posições, são atrelados algarismos que representam cada uma dessas posições. Ou seja, ao se definir uma base b, são adotados símbolos para 0, 1, 2, ..., b – 1, de forma que o sistema será composto por b símbolos básicos (em nosso sistema, chamados com frequência de dígitos) tais que qualquer número possa ser escrito de maneira única na forma

$$N = a_n b^n + n_{a-1} b^{n-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0, \text{ onde } 0 \leq a_i < b,\ i = 0, 1, \ldots, n.$$

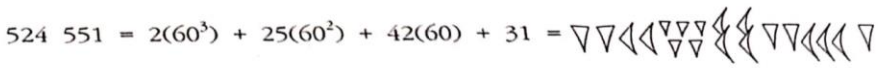
Dessa maneira, representa-se o número N na base b pela sequência de símbolos

$$a_n\, a_{n-1}\, a_{n-2} \ldots a_2\, a_1\, a_0$$

Assim, basta a utilização de um símbolo básico para representar potências da base pré-estabelecida, levando em conta que a ordem do símbolo representa a potência referente à posição na qual encontra-se o mesmo.

Os babilônios antigos, em algum momento entre 3000 a.C. e 2000 a.C., acabaram por desenvolver um sistema de numeração sexagesimal misto que empregava o sistema posicional.

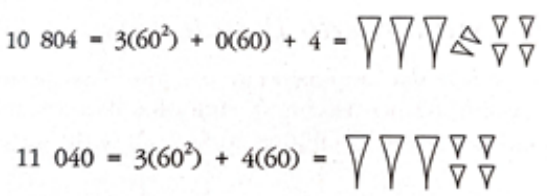
Figura 18 - Exemplo de base sexagesimal mista posicional dos Babilônios



Fonte: EVES, 2004, p. 36.

Havia, contudo, um grande problema com esse sistema de numeração: um símbolo referente ao zero na representação de potências ausentes de 60. Esse fato acabava por provocar uma confusão em algumas leituras de números. Posteriormente, foi introduzido um símbolo, representados por duas cunhas pequenas, inclinadas, porém essa representação era referente à potência ausente de 60 *entre algarismos*, nunca quando ela ocorria na extremidade final de um número. Esse símbolo poderia, portanto, ser considerado como um *zero parcial*, pois um zero de fato deve servir para indicar as potências ausentes da base tanto no meio, como no final de números (EVES, 2004, p. 36). Como exemplo, observe o caso dos números 10804 e 11040 (aqui, pode-se notar a confusão causada pelo zero) abaixo:

Figura 19 – Exemplos de *zeros parciais*



Fonte: Idem

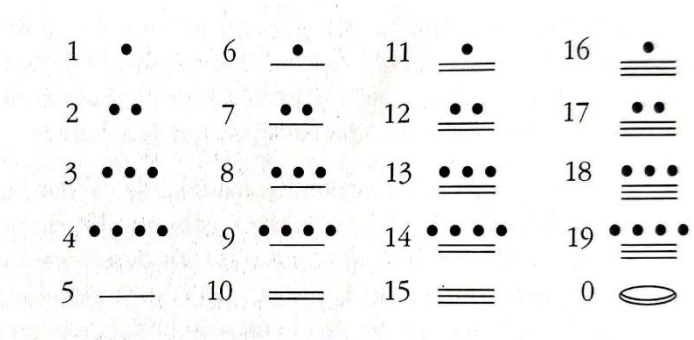
Note que 11040 tem uma representação que pode causar dúvidas acerca de seu valor real. Abaixo, uma possível representação, levando em conta o uso do símbolo, poderia ser:

Figura 20 - Possibilidade alternativa ao *zero parcial*

Fonte: EVES, 2004, p. 37.

Outro sistema que deve ser citado, com algumas caraterísticas bem interessantes, é o sistema de numeração maia. Nesse sistema de numeração com base mista, há o emprego de símbolos simples, por meio de pontos e traços, além de uma representação característica para o zero. Segundo Eves (2004), esse sistema possui origem remota e desconhecida, foi descoberto por expedições espanholas a Yucatán no início do século XVI. Essencialmente vigesimal, porém o segundo grupo vale (18)(20) = 360 em vez de $20^2 = 400$. Todos os grupos de ordem superior são da forma $(18)(20^n)$. Uma possível explicação para essa discrepância provavelmente reside no fato de o ano maia consistir em 360 dias. Os vinte números do grupo eram escritos de maneiras bem simples através de pontos e traços (seixos e gravetos) de acordo com o esquema de agrupamento a seguir:

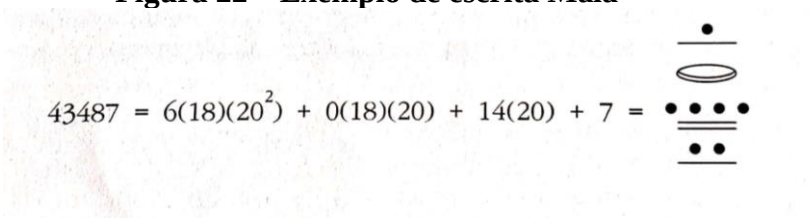
Figura 21 – Sistema de numeração Maia



Fonte: Idem

Como exemplo, o número 43487 escrito na forma vertical (à maneira maia):

Figura 22 – Exemplo de escrita Maia



Fonte: EVES, 2004, p. 37.

Ainda de acordo com Eves (2004), esse sistema era adotado pela classe sacerdotal, enquanto relatos de um sistema vigesimal puro popular eram recorrentes e, contudo, não sobreviveram em forma de escrita.

Nosso próprio sistema de numeração, constitui um exemplo de sistema de numeração posicional:

> Cada algarismo de um número possui um valor que é dado, na verdade, pelo valor do algarismo multiplicado pelo valor de sua posição no número. Assim, por exemplo, o algarismo mais à esquerda de 1965 é um 1, e está na quarta posição, por isso, seu valor é 1.10^3, ou mil. De maneira semelhante, o 9 tem o valor 9.10^2 (isto é, 900), o 6 tem valor de 6.10^1 (isto é, 60) e o 5 tem valor 5.10^0 (isto é, 5). (WALL, 2014, p.36)

Por exemplo:

$$3.576 = 3.000 + 500 + 70 + 6 = 3 \times 10^3 + 5 \times 10^2 + 7 \times 10^1 + 6 \times 10^0$$

Em um sistema de numeração posicional, qualquer número natural $b > 1$ pode servir de base numérica. A veracidade desta afirmação pauta-se na aplicação do algoritmo da divisão euclidiana.

TEOREMA: (Divisão Euclidiana)

Sejam a e b dois números naturais com $0 < b < a$. Existem dois números naturais q e r tais que $a = b.q + r$, com $0 \leq r < b$.

Demonstração

(Existência)

Sejam $a, b \in \mathbb{N}$, tais que $0 < b < a$.

Seja $S \subset \mathbb{N}$, tal que $S = \{a, a – b, a – 2b, a – 3b, ..., a – qb\}$, com $0 \leq q$.

Note que S é limitado inferiormente por 0. Pelo Princípio da Boa Ordem, $\exists\ r \in \mathbb{N}$, r elemento mínimo de S, tal que $a – bq = r$. Resta mostrar que $0 \leq r < b$.

Se b divide a então $r = 0$ e não há mais nada a se demonstrar. ■

Se b não é divisor de a, suponha por absurdo que $r > b$. Daí, $\exists\ c \in \mathbb{N}$ tal que $r = b + c$. Ou seja,

$$r = a – bq = b + c \Leftrightarrow c = a – bq – b \Leftrightarrow c = a – (q + 1)b$$

Logo, $c < r$ que configura um absurdo, pois r é elemento mínimo de S. ■

(Unicidade)

Sejam $q, q', r, r' \in \mathbb{N}$ tais que $a = bq + r$ e $a = bq' + r'$.

Daí, tem-se: $bq + r = bq' + r' \Leftrightarrow b(q – q') = r' – r$

Logo, b divide $r' – r$. Porém, b divide r' e b divide r, pois por hipótese $0 \leq r, r' < b$.

Portanto, $r' – r = 0 \therefore r' = r$. Isso implica que: $b(q – q') = 0 \therefore q = q'$. ■

Nas condições do teorema apresentado acima, q e r são chamados, respectivamente, de quociente e de resto da divisão de a por b. Cabe notar que o resto da divisão de a por b será zero se, e somente se, b divide a.

Assim, podemos com este resultado provar que qualquer número natural pode ser escrito de modo único, em uma base numérica qualquer.

TEOREMA

Dados os números naturais a e b, com $a > 0$ e $b > 1$, existem números naturais $n \geq 0$ e $0 \leq r_0, r_1, ..., r_{n-1}, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que:

$$a = r_0 + r_1 b + r_2 b^2 + ... + r_{n-1} b^{n-1} + r_n b^n.$$

Demonstração

Vamos mostrar, por indução completa, a validade da propriedade.

Para $a < b$, basta tomar $a = r_0$. Nada mais a mostrar.

Para $a \geq b$ e pelo Teorema da divisão euclidiana, existem $q, r' \in \mathbb{N}$ com $0 \leq r' < b$ e $0 < q < a$, tais que

$$a = bq + r'. \qquad (I)$$

Suponha a propriedade válida para todo natural menor que a. Vamos mostrar que a propriedade é válida para todos os naturais.

Tem-se, por hipótese de indução que existem naturais $n' \geq 0$ e $0 \leq r_1, r_2, ..., r_{n'+1} < b$, $r_{n'} \neq 0$, univocamente determinados tais que

$$a = r_1 + r_2b^1 + r_3b^2 + ... + r_{n'+1}b^n. \qquad (II)$$

De (I) e (II), segue que

$$a = b(r_1 + r_2b^1 + r_3b^2 + ... + r_{n'+1}b^n) + r' = r' + r_1b^1 + r_2b^2 + ... + r_{n'+1}b^{n'+1}.$$

Tomando $r' = r_0$ e $n'+1 = n$, tem-se a validade do teorema. ■

A representação dada é chamada de **Expansão relativa à base b**.

Quando b = 10 é conhecida por expansão decimal, quando b = 2, toma o nome de expansão binária, da qual falaremos em sequência.

A seguir, é dado um algoritmo para determinar a expansão de um número qualquer relativo à uma base fixada b, bastando aplicar sucessivamente a divisão euclidiana, como visto abaixo:

$$a = bq_0 + r_0,\ r_0 < b$$

$$q_0 = bq_1 + r_1,\ r_1 < b$$

$$q_1 = bq_2 + r_2,\ r_2 < b,$$

e assim em diante. Como $a > q_0 > q_1 > ...$, e em certo ponto, $q_{n-1} < b$, portanto,

$$q_{n-1} = bq_n + r_n\ ,$$

decorre $q_n = 0$, o que implica que $0 = q_n = q_{n+1} = q_{n+2} = ...$, e portanto, $0 = r_{n+1} = r_{n+2} = ...$.

Tem-se, então, que

$$a = r_0 + r_1 b + ... + r_n b_n.$$

A fim de evitar confusão, utilizaremos a notação

$$[a_n...a_1a_0]_b = a_0 + a_1 b + ... + a_n b^n.$$

Apenas no caso da base 10 (mais usual), a notação seguirá na forma

$$[a_n...a_1a_0]_{10} = a_n...a_1a_0$$

A seguir, três exemplos que servem para ilustrar o esquema de divisões sucessivas:

- Representar o número 10 na base 2.

Note que $10 = 5.2 + 0,$

$5 = 2.2 + 1,$

$2 = 1.2 + 0,$

$1 = 0.2 + 1,$

Logo, $10 = 0.1 + 1.2 + 0.2^2 + 1.2^3$

Ou seja: $10 = [1010]_2$.

- Representar o número 543 na base 5.

Tem-se $543 = 108.5 + 3,$

$108 = 21.5 + 3,$

$21 = 4.5 + 1,$

$4 = 0.5 + 4,$

Logo, $543 = 3.1 + 3.5 + 1.5^2 + 4.5^3$

Portanto, $543 = [4133]_5$.

- Representar o número 4967 na base 12.

Note que nesse caso, a base é maior do que 10. Com isso, utilizaremos símbolos α e β para a representação do 10 e do 11.

Tem-se $4967 = 413.12 + 11,$

$413 = 34.12 + 5,$

$34 = 2.12 + 10,$

$2 = 0.12 + 2,$

Logo, $4967 = 11.1 + 5.12 + 10.12^2 + 2.12^3$

Portanto, $4967 = [2\alpha 5\beta]_{12}$.

Há vários sistemas de numeração que possuem aplicações práticas, além do decimal. O sistema de numeração binário é utilizado em computadores. Além disso, muitos programadores utilizam sistemas de numeração de bases 8 e 16. Há também vestígios de base 5 (moedas de 5 e 10 centavos) e base 60 (aritmética do relógio, e medição de ângulos).

A seguir, daremos ênfase ao sistema binário, um dos objetos das atividades que fazem parte deste texto.

6.4.1 **Sistema Binário**

O sistema de numeração binário utiliza apenas os algarismos 0 e 1 já que são os únicos restos possíveis em uma divisão por 2.

Um número natural escrito na base binária será dado por:

$$N = a_n.2^n + a_{n-1}.2^{n-1} + ... + a_2.2^2 + a_1.2^1 + a_0.2^0$$

onde $0 \leq i \leq n$ e $a_n = 0$ ou 1.

Sua representação será: $(a_n a_{n-1} a_{n-2}.....a_2 a_1 a_0)_2$

A conversão de um número do sistema decimal para o binário dar-se-á como vimos anteriormente por divisões sucessivas onde o divisor é 2.

Como exemplo, vamos representar 45 na base binária, com a devida atenção aos restos obtidos:

45 = 2. 22 + **1**

22 = 2.11 + **0**

11 = 2 .5 + **1**

5 = 2.2 + **1**

2 = 2.2 + **0**

1 = 2. 0 + **1**

Assim:

$45 = 2 \,.\, 22 + 1 = 2 \,.\, (2.11 + 0) + 1 = 4 \,.\, 11 + 1 = 4 \,.\, (2 \,.5 + 1) + 1 =$

$= 8 \,.\, 5 + 4 + 1 = 8 \,.\, (2.2 + 1) + 4 + 1 = 32 + 8 + 4 + 1 = 2^5 + 2^3 + 2^2 + 2^0$

Ou seja: $45 = 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0$.

Quadro 7 - Representação de 45 na base 2

Base 10	Potências de base 2						**Base 2**
	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
45	1	0	1	1	0	1	101101

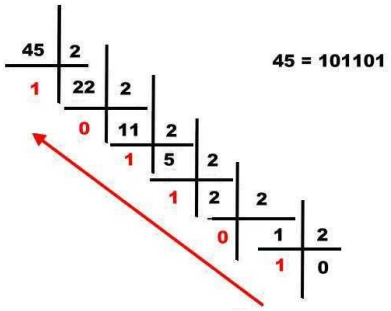
Fonte: O autor, 2020.

$$45 = (101101)_2$$

Cabe destacar que, neste caso, a “leitura” do número na base binária é feita do último resto para o primeiro, como indicado acima.

Para facilitar, se pode utilizar o esquema apresentado na figura a seguir:

Figura 23 - Transformação da base 10 para a base 2 por Divisão Euclidiana



Fonte: O autor, 2020.

Esse sistema se destaca pelo fato de ser largamente utilizado em computadores e foi fundamental para o desenvolvimento da tecnologia utilizada em larga escala atualmente.

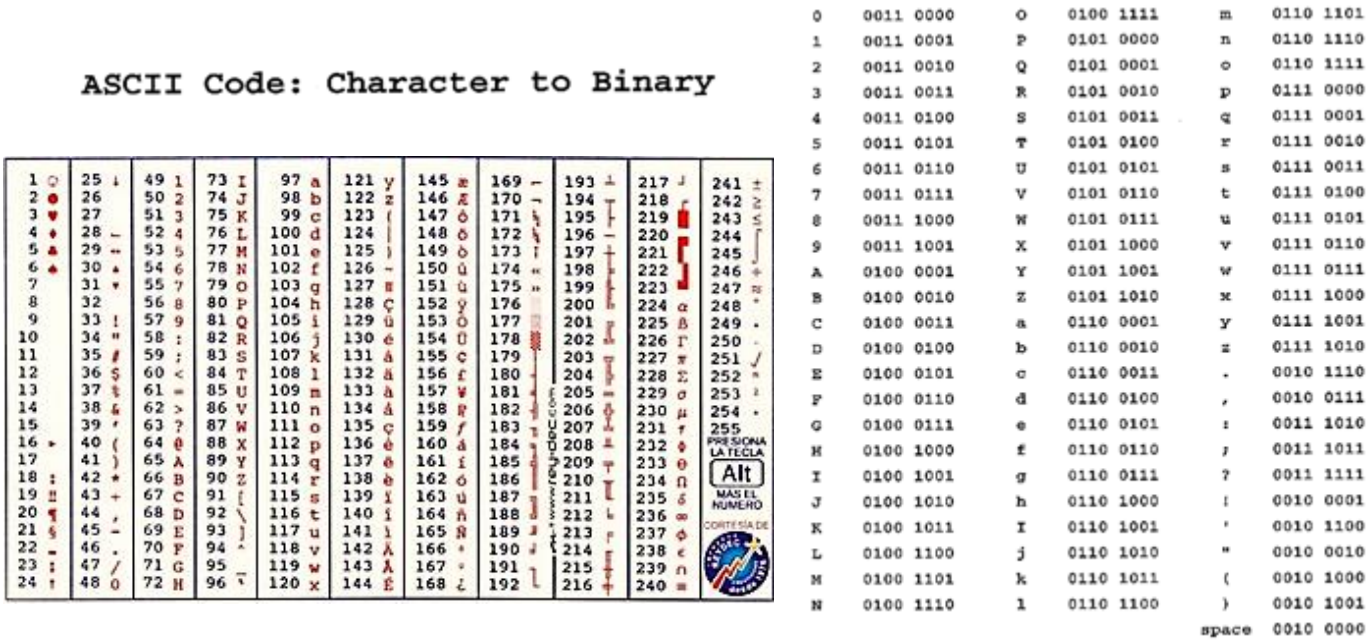
Internamente, a representação de números em circuitos elétricos usa uma série de chaves que possuem dois estados ou posições: “ligada” (passando energia elétrica) representado pelo algarismo binário 1 e “desligada” (não passando energia elétrica) representado pelo algarismo binário 0. Esta é a forma como o computador recebe as informações: um *bit* é a menor unidade de informação que pode ser armazenada ou transmitida. Assim, um bit pode assumir somente dois valores: 0 ou 1, corte ou passagem de energia, respectivamente.

Um *byte* é composto por 8 *bits*, compreendendo 256 caracteres e cada letra, número ou símbolo equivale a um número binário de 8 dígitos. Com isso, possibilita diversas combinações de dígito para representar diversas informações, como números, palavras, cálculos etc.

> Os computadores lidam apenas com números binários - seqüências de um e zero conhecidas como *digitos binários*, ou, abreviadamente, *bits* (de *binary digits*, em inglês). Esta conversão pode ser realizada de acordo com vários protocolos, tais como o American Standard Code for Information Interchange (Código Padrão Americano para Troca de Informações), conhecido pela sigla ASCII. (SINGH, 2003, p. 269).

Mas como são inseridas as informações? Por meio de um protocolo já mencionado anteriormente, o ASCII, onde cada letra, número e símbolos são representados por uma sequência de 8 dígitos que assumem o valor 0 ou 1.

Figura 24 - Protocolo ASCII – Binários



Fonte: Disponível em: https://www.ehow.com.br/escrever-numeros-binarios-como_290958/. Acesso em 16/08/2020.

As tabelas ASCII fornecem os números binários que correspondem ao sistema decimal, alfabeto e símbolos diversos, utilizados para entradas de textos que compreendam todas as representações utilizadas na comunicação e informação.

Por exemplo, a palavra **INFORMAÇÃO** em binário é codificada como (letras maiúsculas; sem considerar a cedilha):

01001001010011100100011001001111010100100100110101000001010000110100000101001111

Exemplos como este nos mostram como podemos unir codificação e bases na abordagem de sistemas numéricos.

O trabalho didático com o sistema binário e outros nos permite mais facilmente a abordagem do sistema decimal como uma extensão de técnica.

7 PORCENTAGEM

Segundo o dicionário Oxford, porcentagem significa “proporção de uma quantidade ou grandeza em relação a uma outra avaliada sobre a centena [símb.: %]; percentual”. De modo geral definimos porcentagem por meio do conceito de razão centesimal, ou seja, aquela cujo consequente é igual a 100, dita porcentagem.

Assim: $\frac{13}{100}$ = 13 % (treze por cento); $\frac{8}{100}$ = 8 % (oito por cento)

Presente no cotidiano do ser humano, a porcentagem é uma ferramenta de análise e aferição de dados, de forma qualitativa, para nortear parte ou partes de determinado nicho ou escopo em pesquisas. Tal ferramenta, propicia abordagens e tratamentos específicos às áreas de interesse contidos na pesquisa em si.

Como grande exemplo atual, as pesquisas de intenção de votos são feitas através de subgrupos específicos (e setorizados geograficamente), tomados de forma aleatória dentro de um espaço amostral maior, embora finito. É feita uma análise dos dados comparando o conjunto formado por esses subgrupos com a população total votante, culminado nos valores percentuais de intenções de votação no quadro a seguir:

Quadro 8 - Intenção de voto – Eleições municipais (RJ) - 2020

Candidato	(%) Intenção de voto
1	19,7
2	11,1
3	9,6
4	6,0
5	5,0
6	3,8
7	3,2
8	2,4
9	1,6
10	0,7
11	0,6
12	0,6
13	0,2
14	0,1
Outros	0,1
Branco/nulo	22,7
Não sabe	9,3

Fonte: Disponível em: < https://diariodorio.com/>. Adaptado. Acesso em 21/09/2020.

Assim, por exemplo, 6% dos entrevistados afirmaram ter intenção de voto no candidato 4. Ou seja, de um grupo de 100 entrevistados, 6 afirmaram ter essa intenção de voto.

Em nosso estudo, utilizaremos a análise de textos avaliando a contagem de letras em duas situações distintas. Tal fato, produzirá duas tabelas de percentuais que servem de base para analisar textos criptografados, pois o objetivo é relacionar a porcentagem à criptografia.

A seguir, será utilizada a porcentagem para a análise de frequência de letras em um texto em português e em outro texto em inglês. Os textos citados foram escolhidos por possuírem mais de mil letras em seu corpo, fato este que garante o caráter fidedigno à análise de quaisquer textos criptografados.

Texto 1 (3084 letras do alfabeto)

Mais de um milhão de pessoas infectadas e sistemas de saúde em colapso no mundo todo. Arrisco-me a dizer que nunca tínhamos enfrentado um vírus com uma capacidade de transmissão tão alta. E este é o grande trunfo do novo coronavírus, que apesar de não ter uma letalidade considerada elevada na população geral, tem a capacidade de provocar estragos sistêmicos – na saúde, na economia e nas relações interpessoais.

A Covid-19 chegou de forma avassaladora, destruindo tudo ao seu redor. Mas ao mesmo tempo, a capacidade de mobilização das pessoas se sobressaiu diante do caos. Os primeiros países acometidos pelo novo coronavírus subestimaram a sua capacidade de destruição. E é preciso ressaltar que que estamos falando de nações extremamente desenvolvidas e com surpreendente capacidade de articulação, como China, Coreia e Japão. Quando a doença chegou à Europa, o erro se repetiu. Desta vez, porém, em países como a Itália, envelhecidos e com uma política desgastada. A devastação foi ainda mais impressionante. Estamos falando de cerca de 600 novas mortes por dia, mais de 130 mil pessoas contaminadas.

No Brasil, apesar dos números crescentes de casos e mortes, estamos tendo a chance de aprender com os erros cometidos em outros países. Exaustivamente acompanhamos por meio de publicações científicas, estudos pontuais e imprensa, que dentre todas as medidas adotadas para o enfrentamento à Covid-19, o isolamento social é um dos métodos mais eficientes para redução do aparecimento de novos casos.

O nosso sistema de saúde tem um desafio enorme pela frente. O novo coronavírus chegou no país acometendo, num primeiro momento, pacientes do setor privado de saúde – que representa um quarto da população do país. A epidemia, no entanto, agora já está na comunidade e é uma realidade para o Sistema Único de Saúde (SUS), responsável pela atenção de mais 150 milhões de brasileiros. E grande parte dessas pessoas (48% da população do país) vive em locais que, sequer, têm coleta de esgoto; sendo a higiene um requisito primordial para o enfrentamento de qualquer epidemia.

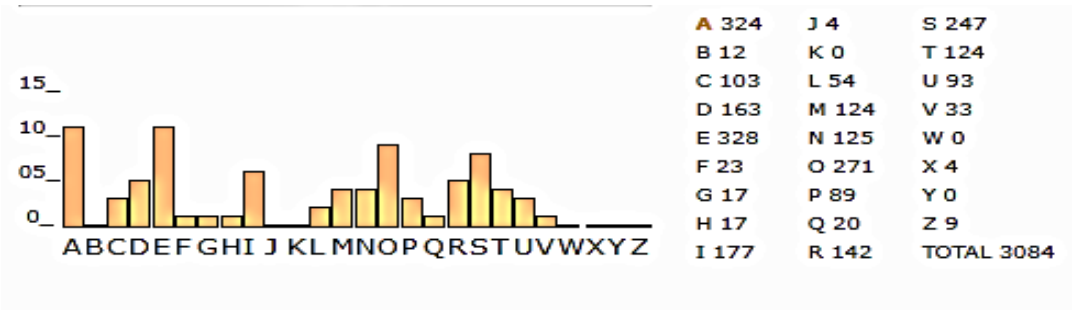
Onde vamos parar? O que eu posso dizer é que há um esforço visível do Ministério da Saúde em conduzir este momento da melhor forma possível. Todos os representantes da cadeia – hospitais, operadoras, indústria de materiais e medicamentos – estão sensibilizados com a grandiosidade do problema e juntos têm buscado soluções para outros desafios de ordem prática, como escassez de suprimentos, disponibilidade de leitos e UTIs equipadas, além da sustentabilidade financeira dos hospitais.

A mensagem que eu gostaria de deixar é que todos valorizem a vida e priorizem o coletivo. Há um grupo importante da economia, formado por serviços essenciais (saúde, alimentação, segurança e logística), indústria de materiais e medicamentos, entre outros, trabalhando exaustivamente para o enfrentamento da pandemia. Portanto, políticos, influenciadores, profissionais da saúde, peço que nos ajudem a passar por este momento, para que possamos sair dessa crise mais fortes como pessoas, como profissionais, como nação!

Fonte: (AMARO, 2020)

Em seguida ao texto, segue a análise de frequência das letras:

Figura 25 - Análise de Frequência do Texto 1



Fonte: Disponível em: <http://numaboa.com.br/criptografia/criptoanalise/309-Ferramenta-de-frequencia>. Acesso em: 21/09/2020.

Em termos percentuais:

Tabela 4 - Análise Percentual do texto I

LETRAS	FREQUÊNCIA (%)
A	10,5
B	0,4
C	3,3
D	5,3
E	10,6
F	0,7
G	0,6
H	0,6
I	5,7
J	0,1
K	0
L	1,7
M	4,0
N	4,0
O	8,8
P	2,9
Q	0,6
R	4,6
S	**8,0**
T	4,0
U	3,0
V	1,0
W	0,0
X	0,1
Y	0,0
Z	0,3

Fonte: o autor, 2020.

Observe-se, por exemplo que, das 3084 letras presentes, 247 são letras “S”. Percentualmente significa que em cada 100 letras, o “S” é encontrado 8 vezes (8%).

Texto 2 (2364 letras do alfabeto)

The UK is at a "critical point" in the coronavirus pandemic and "heading in the wrong direction", the government's chief medical adviser will warn.

Prof Chris Whitty believes the country is facing a "very challenging winter period" and is hold a televised briefing at 11:00 BST. It comes after the prime minister spent the weekend considering whether to introduce further measures in England.

On Sunday, a further 3,899 daily cases and 18 deaths were reported in the UK. The prime minister is understood to be considering a two-week mini lockdown in England - being referred to as a "circuit breaker" - in an effort to stem **widespread growth of the virus.** He held a meeting at Downing Street on Sunday, along with Prof Whitty, Chancellor Rishi Sunak and Health Secretary Matt Hancock, to discuss possible measures.

BBC political editor Laura Kuenssberg said the view from No 10 was that while doing nothing "was not an option", neither was a full national lockdown, and that whatever measures are imposed could be turned "off and on" throughout the winter. Asked about reports of disagreements among cabinet ministers about whether or not to impose a second lockdown, Transport Secretary Grant Shapps told BBC Breakfast: "A conversation, a debate, is quite proper and that is exactly what you'd expect.

"Everyone recognises there is a tension between the virus and the measures we need to take, and the economy and ensuring people's livelihoods are protected."

He added it was "very clear when you follow the data" that the UK is "at this tipping point where we may need to go further".

At the briefing later, Prof Whitty will be joined by the government's chief scientific adviser Sir Patrick Vallance, to present the latest data.

Prof Whitty is expected to say: "The trend in the UK is heading in the wrong direction and we are at a critical point in the pandemic.

"We are looking at the data to see how to manage the spread of the virus ahead of a very challenging winter period."

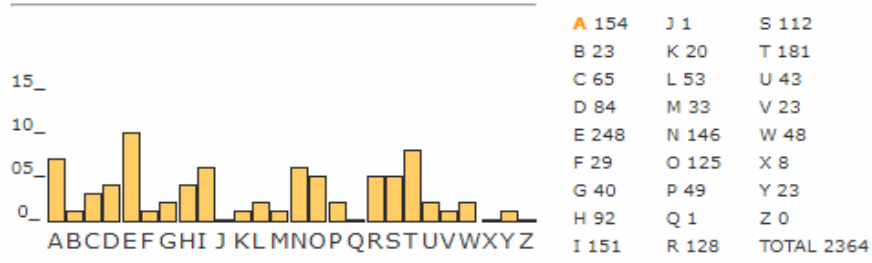
The two scientists are expected to explain how the virus is spreading and the potential scenarios as the winter approaches. They are also expected to share data on other countries who are experiencing a second wave, and explain how the UK could face similar situations.

Commenting on the upcoming announcement, Mr Shapps said: "I've heard their briefing and it is very stark”.

Fonte: BBC, 2020.

Em seguida ao texto, note a análise de frequência das letras:

Figura 26 - Análise de Frequência do texto II



Fonte: Disponível em: <http://numaboa.com.br/criptografia/criptoanalise/309-Ferramenta-de-frequencia>. Acesso em: 21/09/2020.

Em termos percentuais:

Tabela 5 - Análise Percentual do texto II

LETRAS	FREQUÊNCIA (%)
A	6,5
B	1,0
C	2,7
D	3,5
E	10,5
F	1,2
G	1,7
H	3,9
I	6,4
J	0 **(1 vez)**
K	0,8
L	2,2
M	1,4
N	6,2
O	5,3
P	2,1
Q	0 **(1 vez)**
R	5,4
S	4,7
T	7,6
U	1,8
V	1,0
W	2,0
X	0,3
Y	1,0
Z	0,0

Fonte: O autor, 2020.

Já neste segundo texto, das 2364 letras presentes, 112 são letras “S”. Percentualmente, em cada 100 letras, o “S” é encontrado 4,7 vezes (4,7 %).

Os valores presentes nas tabelas foram aproximados para uma casa decimal.

Observemos que as tabelas atentam à características linguísticas distintas que comprovam o fato de a análise levar em consideração a língua mãe utilizada no processo de encriptar o texto.

8 FUNÇÕES

A Matemática ao longo da história foi se modificando e se caracterizando em parte por meio de problemas oriundos do dia a dia, em um desenvolvimento contínuo e presente até os dias atuais.

Mas não somente os problemas cotidianos poderiam ser essa causa.

> Os problemas que motivaram os matemáticos podem ter sido de natureza cotidiana (contar, fazer contas); relativos à descrição dos fenômenos naturais (por que um corpo cai?); por que as estrelas se movem?); filosóficos (o que é conhecer? Como a matemática ajuda a alcançar o conhecimento verdadeiro?); ou, ainda, matemáticos (como legitimar certa técnica ou certos conceitos?). (ROQUE, 2012 - p. 30 e 31)

Várias motivações são, portanto, responsáveis por tal desenvolvimento.

Mas é fato que, dentre tantas motivações, a descrição de fenômenos naturais carrega em si o maior interesse em sistematizações e modelagens que envolvem o uso de ferramentas matemáticas. E o trato com funções se destaca neste quesito.

8.1 A DEFINIÇÃO DE FUNÇÃO

Uma função pode ser definida como uma relação direta entre elementos selecionados, que obedece a algumas regras.

De acordo com Lima (2019), podemos definir uma função por:

´Sejam dois conjuntos quaisquer A e B, subconjuntos de um conjunto universo dado.
Uma função $f: A \rightarrow B$ é tal que cada elemento $x \in A$ é associado a um único elemento $f(x) \in B$, chamado de valor que a função assume em x (ou no ponto x). Os conjuntos A e B são chamados, respectivamente, de **Domínio** e **Contradomínio da função**. Temos assim:

$$\text{Dom}\,(f) = \{x \in A / \exists y \in B \text{ e } y = f(x)\}.$$

O conjunto gerado pelas imagens em B de cada elemento do domínio, é denominado **Conjunto Imagem** da função, ou seja:

$$\text{Im}(f) = \{y \in B / \exists x \in A \text{ e } y = f(x)\}.$$

Em nível da Educação Básica, são estudadas algumas funções reais mais significativas, ou seja, aquelas em que A = B = IR, conjunto dos números reais, e que apresentam características e propriedades mais próximas da vivência em nível médio dos estudantes. Neste caso, a identificação da função considerada é abreviada a caracterização de sua imagem dada por y = f(x), tendo-se por implícito que Domínio e Contradomínio são ambos reais.

As funções reais consideradas são as funções constantes, afins, quadráticas, exponenciais, logarítmicas e trigonométricas, como nos exemplos a seguir:

- $f(x) = 3$
- $f(x) = 4x + 1$
- $f(x) = x^2 + 2x + 1$
- $f(x) = e^x$
- $f(x) = \log x \, (x > 0)$
- $f(x) = \text{sen}(x)$

Antes de relacionarmos funções e criptografia, será necessário ainda abordar algumas características especiais das funções.

8.2 CLASSIFICAÇÃO DAS FUNÇÕES QUANTO AO CONJUNTO IMAGEM

Existem funções que apresentam características especiais quanto ao seu conjunto imagem. São elas as funções injetoras (ou injetivas), sobrejetoras (ou sobrejetivas) e bijetoras (ou bijetivas).

Definição: Seja $f: A \to B$ função.

f é **injetiva** se, e só se, $(\forall x_1 \in A)\ (\forall x_2 \in A)\ (x_1 \neq x_2 \to f(x_1) \neq f(x_2)$

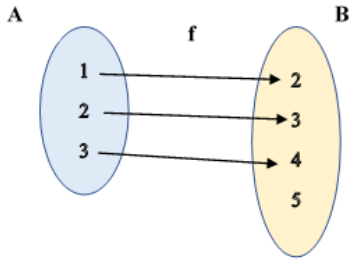
Ou seja, elementos diferentes do domínio possuem imagens diferentes no contradomínio.

Em geral se utiliza a contrapositiva da condicional de definição para verificar a injetividade de uma função:

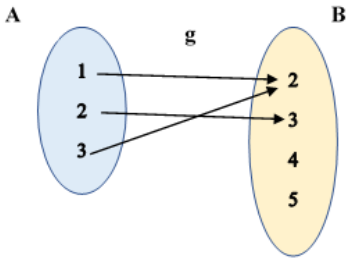
f é **injetiva** se, e só se, $(\forall x_1 \in A)\ (\forall x_2 \in A)\ (f(x_1) = f(x_2) \to x_1 = x_2)$

Utilizando um diagrama sagital, o conceito de injetividade fica mais claro.

Por exemplo, no diagrama sagital a seguir, a função f é injetiva já que as imagens de elementos diferentes também são diferentes.



Já no próximo exemplo, a função g não é injetiva já que $1 \neq 3$ porém $g(1) = g(3) = 2$.

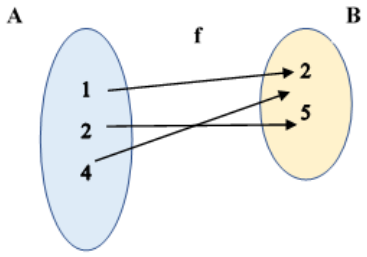


Definição: Seja $f: A \rightarrow B$ função.

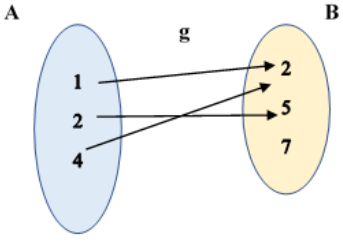
$$f \text{ é } \textbf{sobrejetiva} \text{ se, e só se, } (\forall y \in B)\ (\exists\, x \in A)\ (y = f(x))$$

Ou seja, todo o elemento do Contradomínio é imagem de algum elemento do Domínio. Neste caso: $B = \text{Im}\,(f)$.

Por exemplo, no diagrama a seguir a função f é sobrejetiva pois 2 = f(1) = f(4) e 5 = f(2). Ou seja, $B = \text{Im}\,(f) = \{2,5\}$.



Já neste próximo exemplo, a função g não é sobrejetiva pois não existe x em A tal que 7 = f(x). Assim, $B = \{2,5,7\} \neq \text{Im}\,(f) = \{2,5\}$.



Definição: Seja $f: A \to B$ função. f é **bijetiva** quando é injetiva e sobrejetiva.

8.3 FUNÇÃO COMPOSTA

Definição: Considere A, B e C subconjuntos de IR e as funções $f: A \longrightarrow B$ e $g: B \longrightarrow C$.

Chama-se **função composta** de g e f à função $gof: A \longrightarrow C$ dada por (gof)(x) = g(f(x)).

Por exemplo, considere as funções reais dadas por $f(x) = x^2$ e $g(x) = 2x + 1$.

- $(g \circ f)(x) = g\big(f(x)\big) = g(x^2) = 2(x^2) + 1 = 2x^2 + 1$
- $(f \circ g)(x) = f(g(x) = f(2x + 1) = (2x + 1)^2 = 4x^2 + 4x + 1$
- $(f \circ f)(x) = f\big(f(x)\big) = f(x^2) = (x^2)^2 = x^4$

8.4 FUNÇÃO IDENTIDADE

Definição: Seja A subconjunto de IR. A função $f: A \longrightarrow A$ dada por f(x) = x é denominada função identidade em A, denotada por I_A.

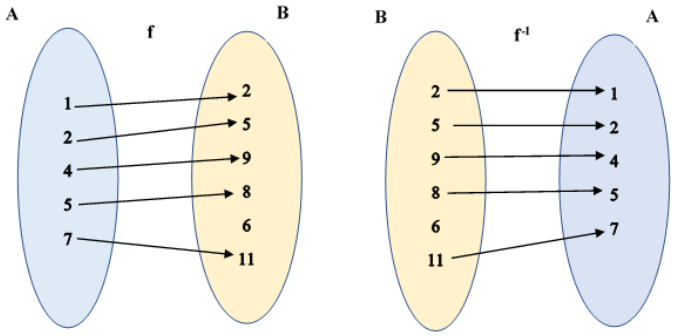
8.5 FUNÇÃO INVERSA

Definição: Considere A e B subconjuntos de IR. A função $f: A \longrightarrow B$ é dita **inversível** quando existe a função $g: B \longrightarrow A$ tal que $gof = I_A$ e $fog = I_B$. Neste caso, g e f são inversas, ou seja, g é a função inversa de f, $g = f^{-1}$ e, equivalentemente, f é a função inversa de g, $f = g^{-1}$.

A seguir, três exemplos serão dados a fim de concluirmos uma condição necessária e suficiente para existência da função inversa.

Figura 27 - Exemplo de relações I

D(f) = A e Im(f) = {2,5,9,8,4,11} ≠ B

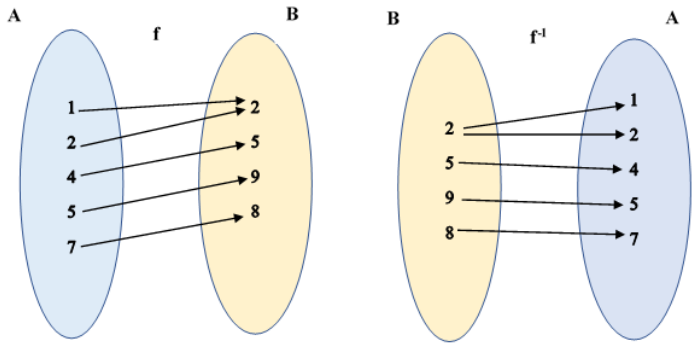


Fonte: O autor, 2020.

Nesse primeiro exemplo, vale notar que a relação mostrada (f^{-1}) não é uma função, visto que o elemento 6 não possui imagem. Observe que f é injetiva.

Figura 28 - Exemplo de relações II

D(f) = A e Im(f) = {2,5,9,8} = B

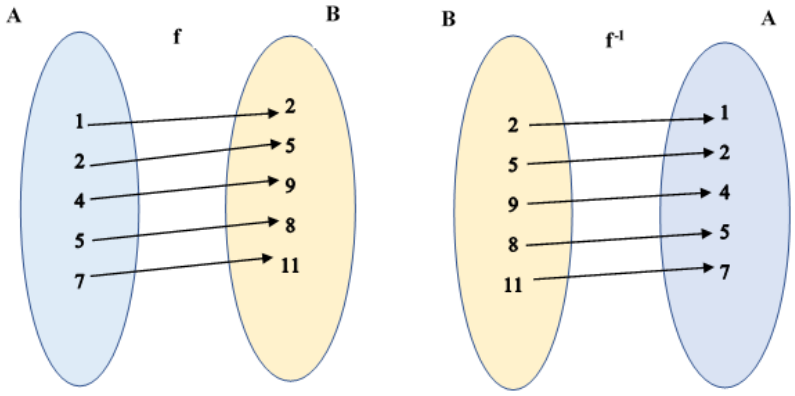


Fonte: O autor, 2020.

No segundo exemplo, a relação apresentada (f^{-1}) também não é uma função pelo fato de um mesmo elemento (2) possuir duas imagens distintas. Note que f é sobrejetiva.

Figura 29 - Exemplo de relações III

D(f) = A e Im(f) = B



Fonte: O autor, 2020.

Percebe-se nesse terceiro exemplo que f^{-1} é função, f o $f^{-1} = I_B$ e f^{-1} o f= I_A e f é bijetiva.

Ou seja, a inversibilidade está intimamente relacionada com a bijetividade.

Podemos assim enunciar o seguinte teorema:

Teorema: Seja $f: A \to B$ função.

f admite inversa f^{-1} se, e somente se, f é bijetiva.

Demonstração

(⇒) Se f admite a inversa $f^{-1}: B \to A$ então f é bijetiva.

- Sejam $x_1, x_2 \in A$ tais que suponha $f(x_1) = f(x_2)$. Como f^{-1} é função, temos:
  $f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \to (f^{-1} \text{ o } f)(x_1) = (f^{-1} \text{ o } f)(x_2) \to I_A(x_1) = I_A(x_2) \to x_1 = x_2$.
  → f é injetiva. (I)
- Seja $y \in B$. Como f^{-1} é função, existe $x \in A$, tal que $f^{-1}(y) = x$.
  Como f é função temos: $f(f^{-1}(y)) = f(x)) \to (f \text{ o } f^{-1})(y) = f(x) \to I_B(y) = f(x) \to y = f(x)$
  → f é sobrejetiva. (II)

Por (I) e (II), f é bijetiva. ■

($\Leftarrow$) Se f é bijetiva, então f admite inversa $f^{-1}: B \to A$.

- Seja $y \in B$. Como f é função bijetiva, existe um único $x \in A$ tal que $f(x) = y$, ou seja, existe um único $x \in A$ tal que $x = f^{-1}(y)$, o que nos garante que f^{-1} é função. ■

Esta demonstração de existência da função inversa para uma função bijetiva nos permite estabelecer a seguinte regra prática para a obtenção da expressão algébrica de f^{-1} , conhecida a expressão algébrica de f dada por $y = f(x)$.

1º) Na expressão algébrica de f, dada por $y = f(x)$ isolamos a variável x, obtendo assim o valor de x em função de y.

2º) Escrevemos $y = f^{-1}(x)$ e assim determinamos a imagem inversa de x.

De forma corriqueira, há o método alternativo que consiste na inversão das variáveis da função. Embora seja prático aos alunos, apresenta algumas inconsistências em sua execução. Portanto, aconselhamos ao professor o uso do método prático citado inicialmente.

Logo a seguir, no próximo subitem, exemplificaremos este procedimento.

8.6 CRIPTOGRAFIA E FUNÇÃO AFIM

Para cifrar uma mensagem por qualquer método, do mais antigo ao mais atual, é preciso garantir que quem receba a mensagem possa decodificá-la, sem ambiguidades ou falta de informações. Assim, deve-se garantir o processo de codificação satisfaça às seguintes condições:

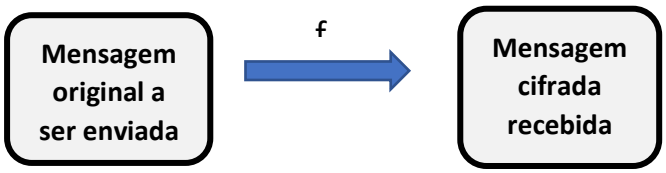
I) Mensagens distintas não podem ser codificadas e transformadas numa mesma mensagem cifrada.

II) Uma mensagem não pode dar origem a duas mensagens codificadas distintas.

III) Toda mensagem deve admitir uma codificação, ou seja, deve ser possível codificar qualquer mensagem, considerando universo de codificação.

As condições II e III nos permitem caracterizar o processo de codificação como uma função.

Figura 30 – Codificação de uma mensagem



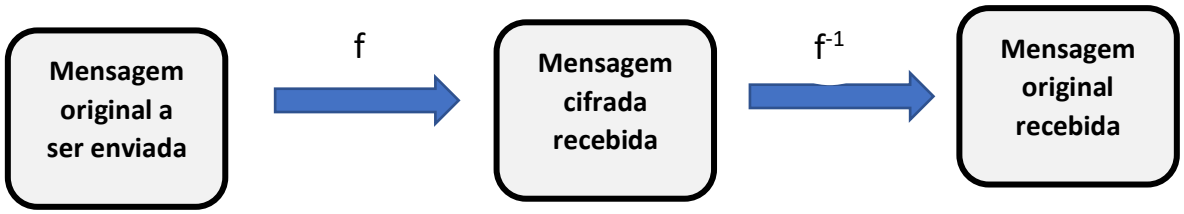
Fonte: O autor, 2020.

A condição I nos apresenta o princípio básico da Criptografia e caracteriza a função considerada como injetiva.

Assim, o processo de codificação nos remete, inicialmente, a encontrar uma função cifradora f injetiva entre o conjunto de mensagens escritas em determinado "alfabeto" (letras, números, símbolos e outros) e um outro conjunto de mensagens cifradas.

Para garantir a reversibilidade do processo fazendo com que as mensagens originais possam ser conhecidas, será necessário que a função cifradora f seja inversível. Ou seja, f também deve ser sobrejetiva e por definição, bijetiva.

Figura 31 – Transmissão de uma mensagem



Fonte: O autor, 2020.

O grande desafio neste procedimento é ocultar de modo eficiente os mecanismos para a inversão de f.

No presente trabalho, destinado a apresentação de atividades elaboradas para aplicação em turmas da EJA - Fundamental, nos deteremos apenas no uso da função afim como função cifradora, tendo em vista esta função ser sempre bijetiva sobre sua imagem.

Definição: Uma função f: IR → IR chama-se **função afim**[31] quando existem constantes a, b ∈ IR , tais que f(x) = ax + b, para qualquer x ∈ A.

- f(x) = 3x + 4, onde a = 3 e b = 4.
- f(x) = -2x + 1, onde a = -2 e b = 4

As funções afins possuem várias aplicações e relações com elementos do cotidiano. Também são chamadas de **funções polinomiais de grau 1.**

São casos particulares das funções afins as funções lineares, dadas por f(x) = ax e as funções constantes dadas por f(x) = b.

A função identidade, mencionada anteriormente, f(x) = x, é um caso particular da função afim, a função linear para a=1.

Teorema

Toda função afim, em que a ≠ 0, admite inversa.

Demonstração

Considere a função afim f: IR ⟶ IR , dada por f(x) = ax +b, a,b ∈ IR , a ≠ 0. Prove-se que f é bijetiva.

- Sejam x_1 e x_2 ∈ A, tais que $f(x_1) = f(x_2)$. Tem-se: $ax_1 + b = ax_2 + b \Rightarrow ax_1 = ax_2$ $\overset{a\neq 0}{\Longrightarrow} x_1 = x_2$. Logo, f é injetiva. ■ (I)
- Seja y ∈ B e considere x = $\frac{y-b}{a}$ → f(x) =a $\frac{y-b}{a}$ + b = y – b + b = y

  Logo f é sobrejetiva. (II)

  De (I) e (II), concluímos que f é bijetiva. ■

  Aqui, por exemplo, pode-se observar as relações da função e da inversa.

[31] CARVALHO, 1997, p.87

Quadro 9 - Aplicação de f e de f^{-1}

A= {1.2.3} e B = {2,4,6}

$\mathbf{f: A \to B}$	$\mathbf{f^{-1}: B \to A}$
$f(1) = 2$	$f^{-1}(2) = 1$
$f(2) = 4$	$f^{-1}(4) = 2$
$f(3) = 6$	$f^{-1}(6) = 3$

Fonte: O autor, 2020.

A sobrejetividade da função afim já nos indica como determinar sua inversa:

$$y = f(x) = ax + b \rightarrow f^{-1}(y) = x = \frac{y-b}{a}$$

Assim, as imagens da função inversa são dadas por $f^{-1}(y) = \frac{y-b}{a}$

E**xemplo**

Considere a seguinte a mensagem a ser transmitida:

USE MÁSCARA

Devemos inicialmente associar cada letra do alfabeto a um número pré-determinado. Por exemplo:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
12	13	14	15	16	17	18	19	20	21	22	23	24
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
25	26	27	28	29	30	31	32	33	34	35	36	37

A seguir vamos utilizar a função cifradora dada por f(x) = 2x + 3 para codificar cada letra de nossa mensagem:

Quadro 10 - Cifragem de "Use Máscara"

Letras da mensagem	Código Numérico	Cifragem f(x) = 2x + 3	Letras cifradas
U	32	f (32) = 2. 32 + 3 = 64 + 3 = 67	67
S	30	f (30) = 2. 30 + 3 = 60 + 3 = 63	63
E	16	f (16) = 2. 16 + 3 = 32 + 3 = 35	35
M	24	f (24) = 2. 24 + 3 = 48 + 3 = 51	51
A	12	f (12) = 2. 12 + 3 = 24 + 3 = 27	27
S	30	f (30) = 63	63
C	14	f (14) = 2. 14 + 3 = 28 + 3 = 31	31
A	12	f (12) = 27	27
R	29	f (29) = 2. 29 + 3 = 58 + 3 = 61	61
A	12	f (12) = 27	27

Fonte: O autor, 2020.

A mensagem cifrada a ser enviada será: 67 63 35 51 27 63 31 27 61 27.

Observe que o envio será feito com espaços entre os números, indicando blocos de 2 letras. Para o envio sem tais espaços, será preciso indicar ao receptor que deverá subdividi-la em blocos de 2 letras para evitar ambiguidades:

$$6763355127633127612 7 \rightarrow 67 / 63 / 35 / 51 / 27 / 63 / 31 / 27 / 61 / 27$$

O processo de decodificação se dá de forma inversa:

$$y = f(x) = 2x + 3 \Rightarrow x = \frac{y-3}{2} \Rightarrow f^{-1}(x) = \frac{x-3}{2}$$

9 METODOLOGIA

O método de pesquisa adotado teve por base a revisão narrativa[32] da bibliografia correlata ao tema com consulta de livros, artigos científicos, dissertações e outros documentos disponibilizados na rede mundial de computadores.

A partir da avaliação do material adquirido foi permitido um entendimento maior do tema estudado e se solidificou a ideia de construção de material passível de aplicação em turmas da EJA.

O projeto de pesquisa inicial previa a aplicação do material desenvolvido em turmas em que o pesquisador exerce a docência. A reformulação foi necessária por conta do impedimento de aulas presenciais durante a pandemia relativa ao Novo Coronavírus (COVID – 19).

Em cada atividade sugerida são indicados os objetivos gerais e específicos, público-alvo e estratégias para aplicação da atividade. As estratégias citadas são apenas um norteador ao professor, cabendo ao mesmo segui-las ou adaptá-las a sua realidade.

Todo o processo de estudo e pesquisa, além da compilação e confecção das atividades, foi realizado no período de junho de 2019 a agosto de 2020.

O conjunto de tarefas e a pesquisa em si, resultam em um produto para uso de professores de tal segmento.

[32] Na **revisão narrativa** tem-se por base apenas alguns trabalhos ou fontes sobre o assunto que é considerado mais importante. Tem o objetivo de trazer uma revisão atualizada do conhecimento estudado, visto que é adequada para a fundamentação teórica de trabalhos acadêmicos.
Disponível em: <https://guiadamonografia.com.br/tipos-de-revisao-de-literatura/>. Acessado em 04/03/2020.

10 PROPOSTA DE ATIVIDADES

Apresentamos aqui a proposta de um conjunto de atividades com enfoque no Ensino de Jovens e Adultos – EJA – Fundamental, utilizando uma linguagem clara e objetiva.

Em alguns casos, fazemos também alusão a elementos do contexto histórico da criptografia e outros que o estudante já “ouviu falar” em situações do seu dia a dia, ou até mesmo podem fazer parte do seu cotidiano. Tal fato não invalida ou inviabiliza sua utilização no segundo segmento do Ensino Fundamental.

De modo geral, as aulas no EJA são projetadas sobre temas específicos e elaboradas pelo docente responsável, sempre buscando relacionar a temas transversais que proporcionam a integração com diversas áreas de conhecimento. Fez-se, portanto, necessária uma busca intensa por ideias que motivassem o projeto em si para a obtenção das relações citadas.

Ao longo do período de pesquisa, houve certa dificuldade ao tentar adaptar os conteúdos e atividades à realidade dos alunos do EJA. Em geral, as publicações ora eram carregadas de rigor matemático ora eram aplicáveis a outras realidades e segmentos de ensino. Em sua grande maioria, as publicações pesquisadas eram voltadas a aplicações ao ensino médio, conforme trabalho de Azevedo (2014), fugindo assim ao espectro de pesquisa do presente projeto. Foi, portanto, necessário fazer adaptações e criação de atividades adequadas ao público-alvo.

A sequência didática a ser seguida deverá ser determinada pelo professor de acordo com as especificidades de sua atuação e do grupo em que atua.

Antes de iniciar a aplicação das atividades, sugerimos que, em aula imediatamente anterior, seja aplicado um questionário introdutório ao tema, de acordo com o ciclo de aprendizagem do EJA - Fundamental, Bloco I ou Bloco II. Poderia inclusive ser indicado como uma tarefa de casa a trazer na aula seguinte. Desta forma, o planejamento poderia ser adaptado e as intervenções docentes mais condizentes com o nível de conhecimento dos alunos sobre o tema. Em tais questionários destaca-se o caráter introdutório dos temas em si, não havendo a necessidade de conhecimentos técnicos prévios por parte dos alunos.

10.1 QUESTIONÁRIOS

BLOCO I

1. Você sabe o que é um código?
2. Se a resposta à questão anterior for SIM, explique o que você acha que é e dê um exemplo.
3. Você sabe o significado do verbo “CRIPTOGRAFAR”?
4. O que diz o dicionário?
5. Já ouviu ou viu em algum texto a palavra “CRIPTOGRAFIA”?
6. Qual o seu significado?
7. A Criptografia faz parte de nosso dia a dia. Você tem conhecimento ou sabe de algum aparelho onde ela é utilizada?
8. Você já ouviu falar sobre sistema de numeração?
9. Você já ouviu falar sobre numeração binária ou código binário? Onde?
10. Se a resposta à questão anterior for sim, sabe de algum aparelho onde esse código é utilizado?

BLOCO II

1. Você sabe o que é um código?
2. Se a resposta à questão anterior for SIM, explique o que você acha que é e dê um exemplo.
3. Você sabe o significado do verbo “CRIPTOGRAFAR”?
4. O que diz o dicionário?
5. Já ouviu ou viu em algum texto a palavra “CRIPTOGRAFIA”?
6. Qual o seu significado?
7. A Criptografia faz parte de nosso dia a dia. Você tem conhecimento ou sabe de algum aparelho onde ela é utilizada?
8. Você sabe o que é uma função? Pode dar algum exemplo?
9. Você sabe o que é a função inversa?
10. Já ouviu falar da condição para que uma função tenha inversa? Qual seria?

10.2 ATIVIDADES PROPOSTAS

Foram elaboradas quinze atividades que podem ser aplicadas tanto no Bloco I como no Bloco II da EJA - Fundamental. São apresentadas com seus objetivos gerais e específicos, público-alvo, referências e sugestões de leitura. Vale, ainda, ressaltar que as sugestões propostas foram pensadas em um ambiente de ensino que leva em consideração a estrutura de organização espacial, física e pedagógica de uma escola da Prefeitura Municipal do Rio de Janeiro.

As resoluções das atividades propostas, produto final deste trabalho, encontram-se no Apêndice.

ATIVIDADE 1 – CÓDIGO MORSE[33]

O código Morse e sua codificação do alfabeto.

Objetivo Geral: Trabalhar a criptografia contida no código Morse.

Objetivo específico: Explorar as necessidades de linguagens e códigos variados em vista dos momentos históricos;

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II.

Em 1835, o inventor estadunidense Samuel Finley Breese Morse (1791 – 1872) desenvolveu um código constituído por um sistema binário (através de ponto e traços), que permitia a transmissão de mensagens por meio de sons curtos e longos com o uso de um telégrafo. Tal invenção, permitia cifrar um alfabeto inteiro, além da transmissão de mensagens criptografadas.

A seguir, um quadro com os símbolos, números e letras correspondentes:

A	**.-**	**M**	**--**	**Y**	**-.--**	**6**	**-....**
B	**-...**	**N**	**-.**	**Z**	**--..**	**7**	**--...**
C	**-.-.**	**O**	**---**	**Ä**	**.-.-**	**8**	**---..**
D	**-..**	**P**	**.--.**	**Ö**	**---.**	**9**	**----.**
E	**.**	**Q**	**--.-**	**Ü**	**..--**	**.**	**.-.-.-**
F	**..-.**	**R**	**.-.**	**Ch**	**----**	**,**	**--..--**
G	**--.**	**S**	**...**	**0**	**-----**	**?**	**..--..**
H	**....**	**T**	**-**	**1**	**.----**	**!**	**..--.**
I	**..**	**U**	**..-**	**2**	**..---**	**:**	**---...**
J	**.---**	**V**	**...-**	**3**	**...--**	**“**	**.-..-.**
K	**-.-**	**W**	**.--**	**4**	**....-**	**‘**	**.----.**
L	**.-..**	**X**	**-..-**	**5**	**.....**	**=**	**-...-**

[33]Adaptada de (BEZERRA, MALAGUTTI, RODRIGUES, 2010, p. 54).

Telégrafo[34]

Além do quadro, há ainda o tempo de envio de uma mensagem com o código Morse. A seguir, são relacionados os tempos de cada símbolo:

Caracteres	Tempo
Ponto	1 unidade de tempo
Traço	3 unidades de tempo
Intervalo entre letras	3 unidades de tempo
Intervalo entre palavras	7 unidades de tempo

Como exemplo, veja como ficaria o tempo de envio da mensagem SOS:

S intervalo O intervalo S

... intervalo --- intervalo ...

3 + 3 + 9 + 3 + 3 = 21 unidades de tempo

Portanto, levaria 21 unidades de tempo para que a mensagem fosse enviada (**...---...**).

1) Durante a Segunda Grande Guerra, um porta-aviões norte – americano prevendo um ataque iminente, encaminhou um pedido de socorro por meio da mensagem **MAYDAY** (do francês “Venez m’aider – que significa “venha me ajudar”). Determine o tempo de envio dessa palavra utilizando o código Morse.

2) O código Morse foi usado como padrão internacional para comunicações marítimas até 1999. Quando a Marinha francesa cessou de usar o código Morse em 1997, a mensagem final transmitida foi[35]:

[34] Disponível em: https://conhecimentocientifico.r7.com/telegrafo/. Acesso em 20/10/20

[35] Disponível em: <https://propagacaoaberta.com.br/codigo-morse-tambem-conhecido-como-telegrafia-e-cw/>. Adaptado. Acesso em 20/10/2020

-.-. .... .- -- .- -. -.. --- / - --- -.. --- ... .-.-.- / . ... - . / / --- / -. --- ... ... --- / .- .. - .. -- --- / --. .-. .. - --- / .- -. - . ... / -.. --- / -. --- ... ... --- / ... .. .-.. -. -.-. .. --- / . - . .-. -. --- .-.-.-

Neste exercício, as barras foram utilizadas para representar o espaço entre as palavras. Qual foi a mensagem final transmitida (em português)?

Referências e Sugestões de leitura

- Educa+Brasil: https://www.educamaisbrasil.com.br/enem/lingua-portuguesa/codigo-morse
- Life4sec: https://life4sec.com.br/entry/118-c%C3%B3digo-morse/
- Wikipédia: https://pt.wikipedia.org/wiki/C%C3%B3digo_Morse
- O Guia dos Curiosos: https://www.guiadoscuriosos.com.br/curiosidades/variedades/deu-a-louca-no-mundo/invencoes/o-que-e-mais-rapido-celular-ou-telegrafo/
- https://www.invertexto.com/codigo-morse

ATIVIDADE 2 – CÓDIGO BRAILLE

O código Braille e sua relação com cifras e códigos relacionados ao alfabeto, além de sua importância para as pessoas com deficiência visual.

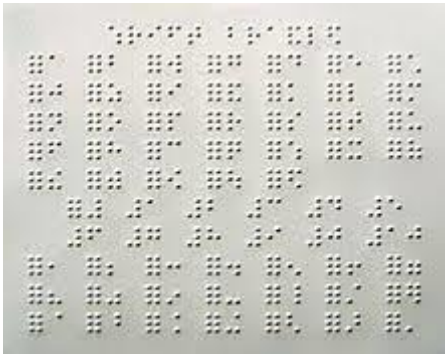
Objetivo Geral: Trabalhar a criptografia contida no código Braille.

Objetivos específicos: Explorar as relações entre a linguagem usual e a não usual, utilizando os símbolos envolvidos; reforçar a importância da linguagem e dos códigos às pessoas que dela necessitam.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II.

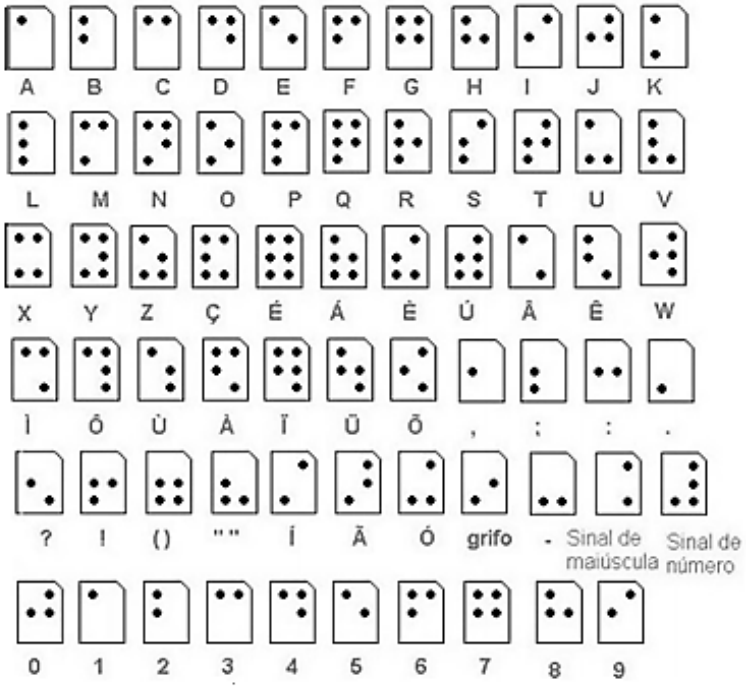
O código Braille é um sistema de escrita e leitura tátil para as pessoas cegas ou com baixa visão, inventado pelo francês Louis Braille, que ficou cego aos três anos de idade.

O sistema consta do arranjo de seis pontos em relevo, dispostos na vertical em duas colunas de três pontos cada, no que se convencionou chamar de "cela braille", semelhante a uma peça de dominó. A diferente disposição desses seis pontos permite a formação de 63 combinações ou símbolos para escrever textos em geral, anotações científicas, partituras musicais, além de escrita estenográfica.



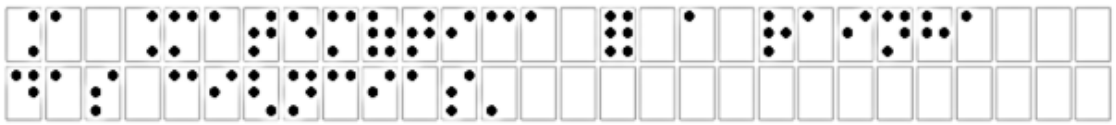
Texto em Braille

A seguir, o quadro de relação entre os símbolos no código Braille.



Fonte: Sistema para Impressão de Textos em Braille. Disponível em:<https://pesquisa.setrem.com.br/970/revista-setrem>. Acesso em: 25 set. 2020.

1) Utilizando o quadro anterior, você conseguiria decifrar a mensagem abaixo?



2) O Brasil conhece o sistema desde 1854, data da inauguração do Imperial Instituto dos Meninos Cegos no Rio de Janeiro. Fundado por D. Pedro II, o Instituto já tinha como missão a educação e profissionalização de pessoas com deficiência visual.[36]

Como seria escrito em Braille o nome atual de tal Instituto?

INSTITUTO BENJAMIN CONSTANT

[36] Disponível em: http://www.escoladailha.com.br/portal/quem-inventou-o-braile/. Acesso em 20/10/2020

Referências e Sugestões de leitura

- INSTITUTO BENJAMIN CONSTANT
  http://www.ibc.gov.br/index.php?option=com_content&view=article&id=675:o-sistema-braille&catid=121&Itemid=373
- Wikipédia
  https://pt.wikipedia.org/wiki/Braille
- Nova Escola
  https://novaescola.org.br
- Tradutor para Braille on line
  https://www.atractor.pt/mat/matbr/matbraille.html
- Braille Fácil 4.0
  http://intervox.nce.ufrj.br/brfacil/

ATIVIDADE 3 – CPF[37]

Segurança e controle no número que representa o Cadastro de Pessoas Físicas.

Objetivo Geral: Trabalhar codificação e segurança utilizando o C.P.F.

Objetivos específicos: Explorar os cálculos identificando a segurança e o método envolvidos; abordar e reforçar o tema segurança utilizando a criptografia.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II.

O **Cadastro de Pessoas Físicas** (**CPF)** é o registro mantido pela Receita Federal do Brasil no qual podem se inscrever, uma única vez, quaisquer pessoas naturais, independentemente de idade ou nacionalidade, inclusive falecidas. Cada inscrito é unicamente identificado por um *número de inscrição* no CPF composto por 11 algarismos. Esse número jamais muda senão por decisão judicial ou administrativa.

$$A_1\, A_2\, A_3\, A_4\, A_5\, A_6\, A_7\, A_8\, R - D_{V1}\, D_{V2}$$

Os oito primeiros algarismos formam o número básico de inscrição da pessoa física. O nono algarismo (indicado pela letra R) se refere à região fiscal de registro da inscrição. O dígito D_{V1} (dígito verificador 1) é o número formado utilizando um cálculo (será explicado e exemplificado abaixo) com os nove algarismos anteriores a ele. De forma similar, é calculado o D_{V2} (dígito verificador 2).

Como é feito o cálculo de D_{V1}? E de D_{V2}?

Vejamos um exemplo para esclarecer.

Deseja-se calcular os dígitos verificadores para o seguinte C.P.F.: 123. 456.789 - D_{V1} D_{V2}

Cálculo de D_{V1}

[37]Idem, p. 8.

Cada um dos nove algarismos anteriores a D_{V1}, a partir da esquerda, é multiplicado por 10, 9, 8, 7, 6, 5, 4, 3 e 2, e os produtos resultantes são somados. A soma resultante é dividida por 11.

1.10 + 2.9 + 3.8 + 4.7 + 5.6 + 6.5 + 7.4 + 8.3 + 9.2 = 210

Dividindo 210 por 11, obtém-se 1 como resto.

O primeiro dígito verificador D_{V1} será a diferença entre 11 e o resto da divisão efetuada. Caso essa diferença seja maior ou igual a 10, considera-se $D_{V1} = 0$.

Ou seja, $D_{V1} = 11 – 1 = 10 \rightarrow$ Toma-se $D_{V1} = 0$.

A seguir, o valor de D_{V1} é colocado em sua posição para o início do cálculo de D_{V2}.

C.P.F.: 123. 456.789 – 0 D_{V2}

Cálculo de D_{V2}

Cada um dos dez algarismos anteriores a D_{V2}, a partir da esquerda, é multiplicado por 11, 10, 9, 8, 7, 6, 5, 4, 3 e 2, e os produtos resultantes são somados. O valor de D_{V2} é então obtido de maneira análoga ao feito para D_{V1}.

1.11 + 2.10 + 3.9 + 4.8 + 5.7 + 6.6 + 7.5 + 8.4 + 9.3 + 0.2 = 255

Dividindo 255 por 11, obtém-se 2 como resto.

Então, $D_{V1} = 11 – 2 = 9$.

Dessa forma, o C.P.F. considerado será: 123.456.789 – 09.

1) Calcule os dígitos verificadores para o C.P.F.: 106. 723. 645 - D_{V1} D_{V2}

2) A regra de formação/codificação do C.P.F. nos permite identificar sua validade ou não. Assim, verifique se o código numérico 132.442.337 – 45 representa ou não um C.P.F. válido.

Referências e Sugestões de leitura

- Receita Federal
  https://receita.economia.gov.br/acesso-rapido/direitos-e-deveres/educacao-fiscal/publicacoes/folhetos/cpf.pdf/view
- Gerador de C.P.F.
  https://www.geradorcpf.com/algoritmo_do_cpf.htm.
- C.P.F. Válido
  https://cpfvalido.com.br/como-o-numero-do-cpf-e-formado/.

ATIVIDADE 4 – CIFRA MAÇÔNICA

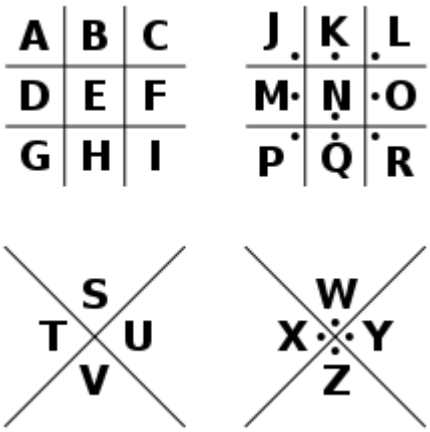
Codificação do alfabeto por métodos alternativos.

Objetivo Geral: Trabalhar criptografia utilizando a Cifra Maçônica, em frases simples.

Objetivos específicos: Explorar a cifra e seus poucos símbolos; Possibilidade de associação e apropriação da linguagem à símbolos matemáticos.

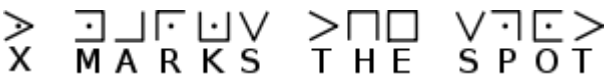
Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental II (6º ou 7º anos)

A Cifra Maçônica (em inglês "Pigpen Cipher" – "chiqueiro" em tradução literal – ou "Freemason's Cipher"), é uma cifra de substituição que possui quatro disposições para identificar suas letras: duas matrizes 3x3 (uma delas com pontos associados a cada espaço) que lembram o "jogo da velha" e, duas "cruzes" em formato de "X" (uma delas com pontos associados a seus espaços). A seguir, a figura representa esse padrão de cifra.



Assim, cada letra é representada pelas arestas em sua volta, indicando a sua posição dentro da matriz 3x3 ou na cruz. Por exemplo, a letra A é representada pelo símbolo  e a letra X pelo símbolo  .

Um exemplo bastante comum encontrado em muitos textos e páginas da internet é:

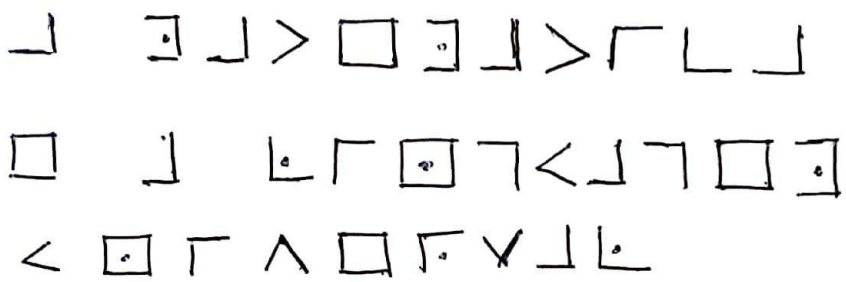


A frase acima “X marks the spot”, traduzida quer dizer “X indica o local”.

1) Utilizando a Cifra Maçônica, cifre a seguinte frase:

OS NÚMEROS GOVERNAM O MUNDO

2) Agora, com domínio básico sobre a cifra, decodifique a escrita abaixo:



Referências e Sugestões de leitura

- Wikipédia
  https://pt.wikipedia.org/wiki/Cifra_ma%C3%A7%C3%B3nica
- PlanetCalc
  https://pt.planetcalc.com/7842/
- AnchisesLandia – Brazilian Security Blogger
  https://anchisesbr.blogspot.com/2017/07/seguranca-cifra-maconica.html.
- Aldeia numa Boa
  www.numaboa.com.br

ATIVIDADE 5 – CIFRA DE VIGENÈRE

Apresentação da Cifra de Vigenère, utilizada por meio do quadrado de Vigenère, e tem como referência a Cifra de César.

Objetivo Geral: Trabalhar criptografia utilizando a Cifra Vigenère, associando-a à Cifra de César.

Objetivos específicos: Explorar a cifra e suas potencialidades; Possibilidade de introdução básica ao conceito de linhas e colunas em uma matriz.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental II (6º ou 7º anos)

A **Cifra de César** é uma técnica de criptografia bastante simples e provavelmente a mais conhecida de todas. Trata-se de um tipo de **cifra de substituição**, na qual cada letra de uma mensagem a ser criptografada é substituída por outra letra, presente no alfabeto, porém deslocada um certo número de posições.

Por exemplo, se usarmos uma troca de nove posições à esquerda, cada letra é substituída pela letra que está nove posições adiante no alfabeto, e nesse caso a letra A seria substituída pela letra J, B por K, C por L, e assim sucessivamente. A mensagem cifrada não terá espaços entre as letras ou palavras.

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

A cifra de César recebe esse nome pois, segundo o escritor Suetônio, foi utilizada por Júlio César para se comunicar com seus generais, protegendo mensagens militares.

Essa cifra é uma cifra de substituição monoalfabética, o que significa que cada letra do texto plano é substituída por uma outra letra do alfabeto no texto criptografado (cifrado), de forma constante (sempre as mesmas letras são utilizadas).

Utilizando o alfabeto cifrado acima:

1) Codifique a mensagem: **LAVE SEMPRE SUAS MÃOS.**

2) Decodifique a cifra: **BNVYANDBNVJBLJAJJXBJRAMNLJBJ**

Utilizando o conhecimento que acabamos de adquirir acerca da Cifra de César, podemos ir um pouco mais além com a Cifra de Vigenère.

A Cifra de Vigenère é uma cifra polialfabética, que utiliza a mesma ideia da Cifra de César, porém utilizando várias listas do alfabeto, reorganizadas em posições diferentes do alfabeto original. A seguir, encontra-se o quadrado de Vigenère que contém as listas de alfabetos que servirão de norteadores e base para o nosso estudo sobre essa cifra.

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

Como exemplo, se quisermos cifrar a mensagem **ESTUDE MATEMÁTICA** iremos, inicialmente, juntar as letras para eliminar os espaços e não haver distorções e, posteriormente, utilizar uma palavra-chave, por exemplo, **SOMA**.

O processo, então, é bem simples. Basta alinharmos a frase citada à palavra-chave, conforme visto abaixo:

E	S	T	U	D	E	M	A	T	E	M	A	T	I	C	A
S	**O**	**M**	**A**	**S**	**O**	**M**	**A**	**S**	**O**	**M**	**A**	**S**	**O**	**M**	**A**

Utilizando o quadrado de Vigenère, ciframos, por exemplo, a letra E, por meio da letra presente na casa onde a linha de E (no alfabeto vertical) e a coluna de S (no alfabeto horizontal) "se encontram". Nesse caso, a letra W.

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

Utilizando seguidamente esse processo, teremos a codificação:

$$\text{ESTUDEMATEMATICA} \underset{SOMA}{\Longleftrightarrow} \text{WGFUVSYALSYALWOA}$$

(palavra-chave)

O processo para inverter a cifra é completamente análogo, bastando tratar a palavra original como a cifrada com a utilização da palavra-chave.

Tendo por base o texto e suas impressões sobre a cifra:

3) Codifique a palavra **PROPORCIONALIDADE**, utilizando a palavra-chave **RAZÃO** (para codificar utilize RAZAO).

4) Decodificar a palavra **UFREEBYRGGM**, utilizando a palavra-chave **FRAÇÃO** (para decodificar utilize FRACAO).

Referências e Sugestões de leitura

- Khan Academy
  https://pt.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher
- Guru da Ciência
  https://www.youtube.com/watch?v=Iw-CO4MjDkE
- Aldeia numa Boa
  www. numaboa.com.br
- Clube dos Geeks
  http://clubedosgeeks.com.br/sem-categoria/cifra-de-cesar-criptografia-monoalfabetica
- M3 – IME - Unicamp
  file:///C:/Users/User/Downloads/ogolpe-guia.pdf
- Wikipédia
  https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re
- Fábrica de Noobs
  https://www.youtube.com/watch?v=Tc--MPir6rI

ATIVIDADE 6 – CIFRA ADFGVX

A Cifra ADFGVX e sua codificação em três etapas.

Objetivo Geral: Trabalhar a criptografia utilizando a Cifra ADFGVX.

Objetivos específicos: Explorar a cifra e suas potencialidades; Possibilidade de introdução básica ao conceito de linhas e colunas em uma matriz.

Público-alvo: Alunos da EJA – Bloco I ou II e do Ensino Fundamental II (6º ou 7º anos)

A cifra ADFGVX (ou "super cifra") é um método de criptografia desenvolvido em 1918 pelo exército alemão no final da Primeira Guerra Mundial. As letras A – D – F – G – V – X foram escolhidas por serem muito distintas em código Morse evitando assim erros de transcrição nas comunicações via telégrafo.

É construída em uma grade de 6x6, sendo cada espaço preenchido de forma aleatória pelas 26 letras do alfabeto e os 10 dígitos possíveis (0 a 9). A linha e a coluna de orientação (em negrito abaixo) são identificadas por uma das letras componentes do nome da cifra em questão (ADFGVX). A seguir, um exemplo como possibilidade:

	A	**D**	**F**	**G**	**V**	**X**
A	9	E	5	2	A	F
D	D	O	W	Y	G	V
F	P	4	Q	B	U	X
G	T	3	K	0	C	J
V	H	S	1	Z	7	N
X	M	8	I	6	L	R

O **segundo passo** é identificar cada letra da mensagem que se deseja transmitir em sua posição na grade e substituí-la pelas letras correspondentes na sua linha e coluna de orientação. Por exemplo, 6 será substituído por XG e assim por diante. Tomemos um exemplo para ilustrar.

Mensagem ➔ AULA ÀS 8H

Texto original ➔ A U L A A S 8 H

Texto cifrado ➔ AV FV XV AV AV VD XD VA

O **terceiro passo** é, de posse de uma palavra-chave (utilizaremos **NOTA**), organizar esse texto cifrado por linhas. Resta a seguir, organizamos as letras da palavra-chave em ordem alfabética.

N	**O**	**T**	**A**		**A**	**N**	**O**	**T**
A	V	F	V		V	A	V	F
X	V	A	V		V	X	V	A
A	V	V	D		D	A	V	V
X	D	V	A		A	X	D	V

O texto cifrado é obtido por colunas:

VV DA AX AX VV VD FA VV

O processo para a reversão, é exatamente a tomada de passos de forma invertida, de posse da palavra-chave é claro.

Cifre a palavra **QUADRADO** utilizando a palavra-chave **RETA** e a grade apresentada.

Referências e Sugestões de leitura

- Wikipédia
  https://pt.wikipedia.org/wiki/Cifra_ADFGVX
- Youtube
  https://www.youtube.com/watch?v=KgbeYJXVbh8
  https://www.youtube.com/watch?v=WqMk_2EQ93M

ATIVIDADE 7 – BASE BINÁRIA - QUADRADINHO POR QUADRADINHO[38]

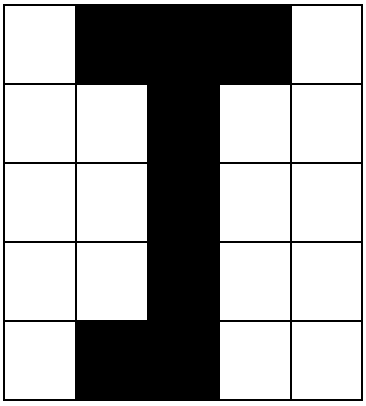
Introdução e exploração dos conceitos iniciais de base binária por meio de figuras em malhas quadriculadas 5 x 5.

Objetivo Geral: Explorar o conceito de numeração binária em situações lúdicas.

Objetivos específicos: Explorar o conceito de numeração binária em malha quadriculada 5 x 5; determinar a relação entre a numeração binária e a figura formada.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental II (6º ou 7º anos)

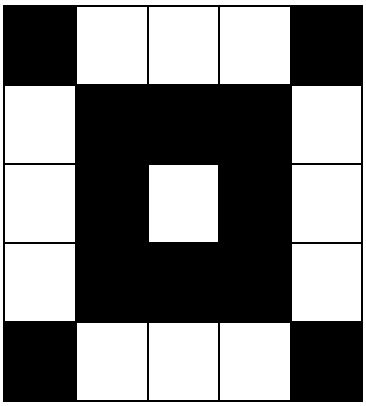
Observe a seguinte malha quadriculada 5 x 5 e a disposição de preenchimento de suas linhas.



Vamos representar cada linha da grade por um número, dessa forma: em cada linha, os quadrados pintados são representados por 1 e os não pintados por 0. Dessa maneira as linhas são representadas pela seguinte sequência: 01110, 00100, 00100, 00100 e 01100. Note que, em cada linha, os quadrados pintados são representados por **1**. Já os quadrados não pintados são representados por **0**. O desenho acima representa a letra **J** (jota).

[38]Adaptada de (ALMEIDA, 2013, p.47)

1) Qual a sequência de 0’s e 1’ que representa as linhas da malha a seguir?



2) Qual a malha quadriculada 5 x 5 é representada pela seguinte sequência:
11111, 10000, 11111, 10000, 10000?

3) A seguir, você terá a oportunidade de criar seu próprio desenho, de forma livre, e representá-lo na forma binária respeitando sempre a ordem estipulada no exemplo anterior. Baseando-se no exemplo anterior, faça um desenho na malha abaixo e o represente na forma binária, considerando os quadrados pintados ou não em sua figura.

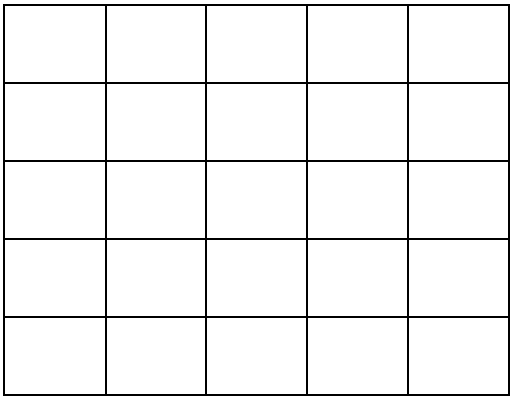
1ª linha: _____

2ª linha: _____

3ª linha: _____

4ª linha: _____

5ª linha: _____



ATIVIDADE 8 – BASE BINÁRIA - ACENDE / APAGA[39]

Experimento com lâmpadas onde o fato de estarem acesas ou não determina a representação binária.

Objetivo Geral: Explorar o conceito de numeração binária em situações lúdicas.

Objetivo específico: Utilizar o experimento das lâmpadas acesas / apagadas para aumentar a compreensão sobre numeração binária.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental II (6º ou 7º ano)

Observações sobre a aplicação da atividade

Nesta atividade é proposto o experimento com lâmpadas onde o fato de estarem acesas ou não determina a representação binária 0 ou 1. Caso a lâmpada esteja apagada, representa-se por 0, caso contrário, por 1. Baseado nessa representação, são apresentados desenhos em branco, em um primeiro momento, onde os alunos pintam as lâmpadas de acordo com a numeração binária pré-determinada, enquanto em um momento posterior, é proposto o contrário, com os desenhos prontos e cabendo aos alunos a obtenção dos números binários. Havendo a possibilidade, a construção do dispositivo pode tornar mais palpável a representação binária e seus resultados. A experimentação física do dispositivo, pode render uma compreensão ampla dos conceitos citados e trabalhados. Mas não é um pré-requisito

O dispositivo representado a seguir funciona da seguinte forma:

- A sequência das lâmpadas é da direita para a esquerda
- Acionar uma lâmpada é equivalente a acendê-la, se estiver apagada, ou apagá-la, caso esteja acesa.
- Quando uma lâmpada se apaga, a lâmpada imediatamente à sua esquerda se aciona.
- Apenas a primeira lâmpada é acionada manualmente.

[39]Idem, p.50.

Experimento com lâmpadas[40]

Conhecido o funcionamento do dispositivo, vamos atribuir valores para o estado de cada lâmpada: uma lâmpada acesa equivale ao número um e uma lâmpada apagada equivale ao número zero.

Iniciando o processo com todas as lâmpadas apagadas, acionamos a primeira lâmpada. Temos o primeiro número do sistema binário de numeração. O segundo acionamento nos mostra o segundo número do sistema binário, o terceiro acionamento nos mostra o terceiro número e assim sucessivamente.

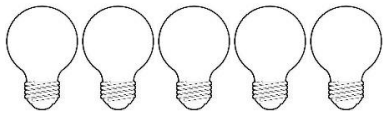
Veja o esquema de um possível estado do dispositivo:

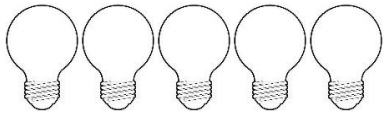
Início	0	0	0	0
1º acionamento	0	0	0	1
2º acionamento	0	0	1	0
3º acionamento	0	0	1	1
4º acionamento	0	1	0	0
5º acionamento	0	1	0	1
6º acionamento	0	1	1	0

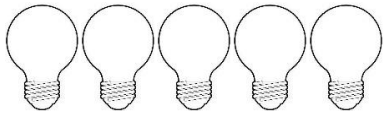
[40]ALMEIDA (2013, p. 38)

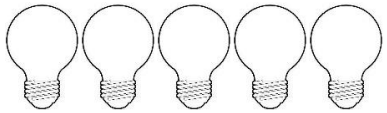
Temos: lâmpada acesa (1) e lâmpada apagada (0). No primeiro acionamento, acendemos a primeira lâmpada; ao apagá-la no segundo acionamento, a segunda lâmpada foi acionada. No terceiro acionamento, acendemos a primeira lâmpada, e assim por diante.

1) De posse do exemplo anterior, indique o estado de cada lâmpada (acesa ou apagada) de acordo com o número binário indicado.

a)  ➔ **00001**

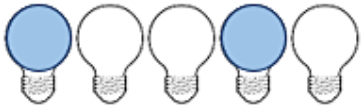
b)  ➔ **00100**

c)  ➔ **01010**

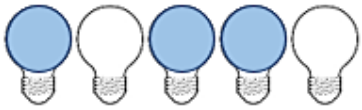
d)  ➔ **10101**

2) Da mesma forma, agora escreva o número binário correspondente ao estado em que se encontra o dispositivo.

a)  ➔ _____

b)  ➔ _____

c)  ➔ _____

d)  ➔ _____

ATIVIDADE 9 – BASE BINÁRIA - CUSTO DAS LÂMPADAS

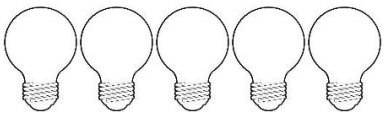
Relação entre base binária e base decimal por meio do custo de lâmpadas acesas no experimento Acende/Apaga.

Objetivo Geral: Explorar o conceito de numeração binária em um exemplo específico.

Objetivos específicos: Utilizar o sistema monetário para auxiliar a compreensão sobre numeração binária; conseguir escrever números na base 10 em base binário e vice-versa.

Público-alvo: Alunos do EJA – Fundamental – Bloco I e do Ensino Fundamental II.

Vamos considerar a disposição das lâmpadas na atividade anterior:



Considere que a instalação foi feita de modo errado, aumentando o custo de cada lâmpada ligada.

Para efeito de fixação, numeremos da seguinte maneira: a primeira lâmpada da direita corresponde ao valor de R$1,00 de custo de energia (por hora) quando ligada.

Cada lâmpada seguinte (sempre da direita para a esquerda), em termos de custo, equivale ao dobro da anterior quando ligada. Assim, temos a seguinte configuração, com todas as lâmpadas acesas:

 1	 1	 1	 1	 1	Lâmpada
16 reais	8 reais	4 reais	2 reais	1 real	Custo

O custo total, nesse caso, seria de 16 + 8 + 4 + 2 + 1 = 31 reais representado pelo número binário 11111.

Como poderíamos representar em binário um custo de 18 reais?

Observe que a soma dos custos de cada lâmpada deverá nos dar como resultado 18 reais.

 1	 0	 0	 1	 0	Lâmpada
16 reais	Sem custo	Sem custo	2 reais	Sem custo	Custo

Temos então: 10010

O número 3 que pode ser representado por **00011** (custo de 2 + 1 = 3 reais)

1) Escreva como número binário os custos a seguir (em reais):

26 ➔

20 ➔

19 ➔

18 ➔

13 ➔

11 ➔

9 ➔

7 ➔

2) Utilizando o raciocínio luz acesa (1) ou luz apagada (0), escreva os custos associados aos binários a segur:

10010 ➔

00100 ➔

10000 ➔

10101 ➔

ATIVIDADE 10 – DA BASE 10 PARA A BASE 2

Escrever em base binária, um outro representado na base decimal.

Objetivo Geral: Explorar o conceito de numeração binária.

Objetivo específico: Efetuar a transformação de um número da base decimal para a base binária e vice versa.

Público-alvo: Alunos do EJA – Fundamental – Bloco I e do Ensino Fundamental II.

Observações sobre a aplicação da atividade

O professor inicia a atividade retomando a conversa sobre a atividade anterior e mostrando as relações numéricas apresentadas a seguir. Cabe ressaltar a relação direta com as atividades mencionadas

O sistema de base 2 é um sistema posicional similar ao nosso sistema de base 10. Nele, são destacadas as potências de 2 em sequência.

Para efeito de comparação, expressemos o valor nas duas bases:

- Na base 10 ➔ $18 = 10 + 8 = 1.10^1 + 8.10^0$. Ou seja, representamos: $18 = [18]_{10}$.

Base 10	Potências de base 10		Base 10
	$10^1 = 10$	$10^0 = 1$	
18	1	8	18

- Na base 2 ➔ $18 = 16 + 2 = 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 0.2^0$. Ou seja, representamos: $18 = [10010]_2$.

Base 10	Potências de base 2					Base 2
	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
18	1	0	0	1	0	10010

Note que nos dois sistemas, a representação é dada pelos valores que acompanham as potências. Se fosse outra base, a representação seria diferente, levando em conta a base e a posição das potências.

Com o auxílio do quadro de potências de 2, represente na base 2 os seguintes números da base 10:

a) 26

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
26								

b) 30

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
30								

c) 56

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
56								

d) 47

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
47								

e) 72

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
72								

ATIVIDADE 11 – CODIFICAÇÃO COM A BASE BINÁRIA

Uso da base binária para codificar o alfabeto.

Objetivo Geral: Explorar o conceito de numeração binária em um exemplo específico.

Objetivos específicos: Utilizar o alfabeto para aumentar a compreensão sobre numeração binária; conseguir escrever ou determinar uma frase com o código binário e/ou vice-versa.

Público-alvo: Alunos do EJA – Fundamental - Bloco I e do Ensino Fundamental II.

Observações sobre a aplicação da atividade

O professor inicia a atividade retomando a conversa sobre a atividade anterior e mostrando as relações numéricas apresentadas a seguir. Após, apresenta uma das possíveis representações do alfabeto na numeração binária. Cabe ressaltar a relação direta com as atividades mencionadas anteriormente

Matheus e Ana Luisa são dois amigos que adoram brincar e aprontar desde pequenos.

Os dois criaram um código para se comunicarem sem que os adultos percebessem e soubessem do que se tratava.

Muito estudiosos, basearam sua linguagem em um código de base 2 (código binário) que continha o alfabeto (em sequência padrão e com as letras numeradas de 1 a 26) como vemos a seguir:

Letra (posição na base10)	Formato binário (base2)
A (1)	00001
B (2)	00010
C (3)	00011
D (4)	00100
E (5)	00101
F (6)	00110
G (7)	00111
H (8)	01000
I (9)	01001
J (10)	01010
K (11)	01011
L (12)	01100
M (13)	01101
N (14)	01110
O (15)	01111
P (16)	10000
Q (17)	10001
R (18)	10010
S (19)	10011
T (20)	10100
U (21)	10101
V (22)	10110
W (23)	10111
X (24)	11000
Y (25)	11001
Z (26)	11010

Ao se comunicarem, tinham em mente que deveriam evitar frases muito longas, então era sempre um “como você está”, “estou bem”, “o que jantou?”, e outras mais.

Ambos usavam hífen para separar as letras, além de barra (/) para separar as palavras. Também usavam os sinais usuais como exclamação, interrogação e ponto final.

Certo dia, Matheus recebeu uma mensagem codificada e ficou bem preocupado. Logo, tratou de responder com outra mensagem. Em seguida, Ana Luisa enviou mais uma mensagem, o que fez Matheus ficar bem triste.

A seguir, as mensagens enviadas:

- Ana Luisa: **00101-10011-10100-01111-10101** / **01101-10101-01001-10100-01111** / **10100-10010-01001-10011-10100-00101**.

- Matheus: **01111** / **10001-10101-00101** / **01000-01111-10101-10110-00101**.

- Ana Luisa: **01001-10010-00101-01101-01111-10011** / **01110-01111-10011** / **01101-10101-00100-00001-10010**.

1) De acordo com a tabela de codificação utilizada por eles, qual foi o diálogo estabelecido entre Matheus e Ana Luisa?

2) Com o teor do diálogo conhecido, decodifique a resposta enviada por Matheus, representada a seguir:

01110-00001-01111 / **01001-01101-10000-01111-10010-10100-00001** / **00001** / **00100-01001-10011-10100-00001-01110-00011-01001-00001**.

10011-00101-10001-00101-01101-01111-10011 / **10011-00101-01101-10000-10010-00101** / **00001-01101-01001-00111-01111-10011**.

ATIVIDADE 12 – CIFRA DE CÉSAR - O CELULAR PERDIDO

Utilização da Cifra de César e a representação de um número no sistema binário para codificar.

Objetivo Geral: Explorar o uso da Cifra de César e a representação de um número no sistema binário.

Objetivos Específicos: Codificar uma mensagem com a Cifra de César; transformar um número do sistema decimal em outro do sistema binário.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental II

Observações sobre a aplicação da atividade

Neste caso temos duas possibilidades de estratégia inicial:

Caso a turma em questão já possua conhecimento prévio de Criptografia e/ou já tenha acontecido a aplicação das atividades específicas de 1 a 6, bastará que o professor faça uma breve revisão do que foi visto, antes de iniciar. Se não for o caso, recomendamos que aplique primeiro algumas atividades dentre as de 1 a 6 para que o aluno se familiarize com o tema.

Esta atividade é realizada com os estudantes se reunidos em duplas para trocar mensagens, montar funções e desafiar seus colegas a decodificá-las, utilizando a tabela-base

Ao acordar bem cedo pela manhã, Juliana não imaginava o que aquela segunda-feira de julho reservaria para sua vida. Por volta das 6h, começou a “rodar” com seu Voyage prestando serviço a uma empresa de translado por aplicativo. Ela era nova nessa modalidade e por isso precisava se destacar com rapidez.

Às 9h, sinalizou positivo para uma “corrida” que a levaria da Glória ao Galeão em uma viagem que jamais esqueceria. Logo, avistou o passageiro Rafael, que faria a corrida até o aeroporto. Em um trajeto que durou cerca de 1 hora (o trânsito estava lento nesse dia), ambos conversavam animadamente sobre política e temas da atualidade. A viagem foi realizada sem complicações. O problema surgiu depois.

Ao retornar, Juliana notou um brilho diferente vindo do banco de trás. Era o celular de Rafael. Com um agravante: ele havia acabado de comprar. Ela deduziu isso pela caixa que estava ao lado do aparelho com todos os manuais e acessórios presentes. Percebendo o que havia acontecido, Juliana parou em um posto pelo caminho e começou a mexer no aparelho para buscar alguma informação que pudesse fazê-la identificar algum número que lhe permitisse contatar Rafael ou algum parente próximo. Ela descobriu que não seria uma tarefa fácil, pois o Rafael havia conseguido colocar uma senha para o acesso. Para dificultar, era uma senha que utilizava criptografia moderna que libera o acesso em duas etapas e em cada uma delas, havia uma senha com 6 dígitos. Daí, Juliana pensou: "como farei para descobrir esses códigos"?

Como uma resposta a seus pensamentos, o smartphone piscou e mostrou que havia uma dica para cada uma das duas senhas: Nome – cifra de César – 2 casas a frente; Idade – binário. Assim, Juliana percebeu que as informações citadas, deveriam ser relacionadas ao nome Rafael e a idade dele. Por sorte, Rafael havia comentado que tinha 35 anos.

Assim, Juliana se deparou com três situações: resolver o primeiro problema utilizando a primeira dica; resolver o segundo problema com a segunda dica; e com a permissão do acesso ao smartphone, conseguir contato com alguma pessoa próxima a Rafael. Vamos ajudá-la?

Primeira dica: Nome – cifra de César – 2 casas

1) Complete a tabela a seguir com o alfabeto cifrado correspondente.

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**

2) Qual a cifragem do nome RAFAEL?

Segunda dica: Idade – binário

3) Escreva a idade de Rafael, 35 anos, no sistema binário.

4) Qual é o código final que desbloqueia o celular do Rafael?

ATIVIDADE 13 – FUNÇÕES - O NÚMERO DA CASA DE MARIANA

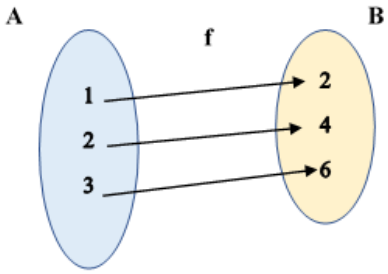
A expressão algébrica da função inversa de uma função afim.

Objetivo Geral: Determinar a função inversa de uma função bijetora dada.

Objetivo específico: Determinar a expressão algébrica da função inversa de uma função afim.

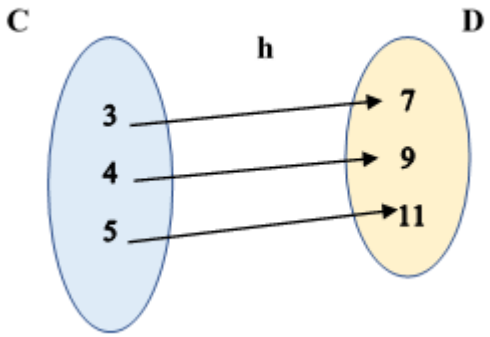
Público-alvo: Alunos da EJA – Fundamental – Bloco II e do Ensino Fundamental II (9º ano).

1) Considere o diagrama a seguir relativo à função f: A → B:



a) Qual o Domínio de f?
b) Qual o Contradomínio de f?
c) Qual o Conjunto Imagem de f?
d) Observando a forma como as imagens foram determinadas, qual seria a expressão algébrica de f dada por $y = f(x)$?
e) Esta função tem inversa? Por quê?
f) Qual seria a expressão algébrica da inversa f^{-1}?

2) Considere o diagrama a seguir relativo à função h: C → D:



a) Qual o Domínio de h?
b) Qual o Contradomínio de h?
c) Qual o Conjunto Imagem de h?
d) Observando a forma como as imagens foram determinadas, qual seria a expressão algébrica de h dada por y = h(x)?
e) Esta função tem inversa? Por quê?
f) Qual seria a expressão algébrica da inversa h^{-1}?

3) Mariana deseja enviar o seu endereço por mensagem para seu amigo Pedro. Ele está curioso pois sabe em que rua ela mora, mas não o número de sua residência. E assim, ela resolveu fazer uma brincadeira com ele: codificou e lhe enviou o número de sua casa, cifrando cada algarismo por meio da função real dada por $f(x) = x - 2$.

Mas Mariana não sabia que Pedro entendia bem de Criptografia. Qual não foi a sua surpresa ao vê-lo chegar para o lanche da tarde!

a) O número da casa de Mariana é 784. Qual foi o número enviado para Pedro?

b) Como Pedro fez para descobrir o número da casa de Mariana? Represente esta situação em um diagrama.

ATIVIDADE 14 – FUNÇÕES E CRIPTOGRAFIA - MENSAGEM SECRETA[41]

Relacionando temas como função afim, função inversa e criptografia por meio do alfabeto e codificação de mensagens.

Objetivo Geral: Explorar o conceito de função afim na Criptografia, visando contextualizar a aprendizagem.

Objetivos Específicos: Efetuar a leitura de uma tabela dada para decifrar algumas frases específicas; calcular imagens de elementos do domínio de uma função afim.

Público-alvo: Alunos da EJA – Fundamental – Bloco II e do Ensino Fundamental II (9º ano).

Observações sobre a aplicação da atividade

Neste caso temos duas possibilidades de estratégia inicial: caso a turma em questão já tenha tido conhecimento prévio de Criptografia com a aplicação das atividades específicas de 1 a 6, bastará que o professor faça uma breve revisão do que foi visto, antes de iniciar. Senão for o caso, recomendamos que aplique primeiro uma ou duas atividades dentre as de 1 a 6 para que o aluno se familiarize com o tema.

Esta atividade é realizada com os estudantes se reunidos em duplas para trocar mensagens, montar funções e desafiar seus colegas a decodificá-las, utilizando a tabela-base apresentada.

Juliana deseja enviar uma mensagem secreta a Rafael. Para isso, segue a orientação descrita nas etapas a seguir:

Etapa 1

Juliana começa por estabelecer uma correspondência entre os números de 1 a 26 e as letras do alfabeto:

[41] Adaptada de SINGH (2003, p.68)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	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

Etapa 2

Juliana escolhe um texto para ser codificado e obtém a sequência numérica correspondente ao texto de acordo com a tabela.

MATEMÁTICA RECREATIVA

Ajude Juliana a encontrar a sequência numérica correspondente a este texto:

M	A	T	E	M	A	T	I	C	A	R	E	C	R	E	A	T	I	V	A
13	1																		

Etapa 3

Para obter a mensagem cifrada, Juliana escolhe a função afim cifradora dada por $y = f(x) = 2x + 1$ e transmite a Rafael a sequência numérica obtida por meio das imagens de obtidas.

Complete os cálculos que faltam para cifrar a mensagem. Observe os exemplos das letras M e A.

Letra	**Sequência Original**	**Imagem da Função $y = f(x) = 2x + 1$**	**Sequência Cifrada**
M	13	$f(x) = 2x + 1 = 2.13 + 1 = 26 + 1 = 27$	27
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 5$	5
T			
E			
M			27
A			5
T			
I			
C			
A			5
R			5
E			
C			
R			
E			
A			
T			
I			
V			5
A			

A sequência numérica transmitida por Juliana foi:

_____

E então, como Rafael irá decodificar a mensagem?

Será preciso conhecer a função cifradora f para realizar o processo inverso por meio de sua função inversa decifradora f^{-1}.

Depois de algumas tentativas sem sucesso, Rafael pede a Juliana que lhe diga qual é a função cifradora que nós já conhecemos:

$f(x) = 2x + 1$.

Para encontrar a função inversa f^{-1}, Rafael lança mão da seguinte regra prática:

1º) Na expressão algébrica de f, dada por $f(x) = 2x + 1$, "isolamos" o x utilizando os artifícios algébricos necessários.

_____

2º) Transformamos algebricamente a expressão utilizando o operador f^{-1}, em função de x para obtermos f^{-1}.

_____

Utilizando f^{-1} preencha a tabela a seguir e veja como Rafael decifrou a mensagem recebida.

Sequência Cifrada	**Imagem da Função Inversa** $\mathbf{y = f^{-1}(x) =}$ _____	**Sequência Original**	**Letra**

Antes de terminarmos, uma questão a mais:

E se Juliana não tivesse dito a Rafael que a função cifradora era $y = f(x) = 2x + 1$?

Você tem alguma sugestão de como ele poderia descobrir f ?

ATIVIDADE 15 – ANÁLISE DE FREQUÊNCIAS - CONSOANTES E VOGAIS

O conceito de Criptografia por meio da análise da frequência das letras presentes em textos do nosso alfabeto.

Objetivos Geral: Explorar o conceito de Criptografia, analisando a frequência das letras presentes em textos do nosso alfabeto.

Objetivos específicos: Rever o cálculo de porcentagens; analisar a frequência das letras de uma frase ou texto proposto; por comparação de frequências, decifrar uma frase criptografada.

Público-alvo: Alunos da EJA – Fundamental – Bloco I ou II e do Ensino Fundamental.

O professor de Matemática escreveu uma frase no quadro e pediu que seus alunos tentassem descobrir o significado. A frase era:

B NBUFNBUJDB F DPOIFDJEB DPNP B SBJOIB EBT DJFODJBT.

Antes de analisar a frase, deve-se observar a frequência com que as letras aparecem na língua portuguesa. A seguir, um texto que servirá de auxílio para a análise da frequência dessas letras. (texto com 650 letras)

“Entre os hábitos com mais força na rotina dentro da pandemia estão o consumo de conteúdo em vídeo, cozinhar e cuidar mais da casa. Mudanças em como as pessoas enxergam os lares devem ter impactos até na arquitetura, de acordo com a pesquisa. O escritório deve começar a fazer parte da maioria das plantas e produtos como velas aromáticas e destinados a deixar a casa mais confortável vão ganhar força. A pandemia também deve começar a gerar mudanças no urbanismo. Com as cidades grandes liderando os casos de infecções pelo coronavírus, um sentimento de valorizar uma vida calma também parece emergir. Na pandemia, as cidades médias têm ganhado apelo”.[42]

[42] Disponível em: <https://exame.com/especiais/mais-conectado-economico-e-caseiro-como-o-coronavirus-mudou-o-brasileiro/> Acesso em 29/08/2020

1) Complete a tabela a seguir, com a frequência de cada uma das letras que aparece no texto acima. Como exemplo, é exibida a frequência da letra A.

Letras	**Cálculo da Porcentagem**	**Frequência (%)**
A	$\frac{88}{650} = 0{,}135$	13,5
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		

2) Calcule e faça uma tabela com a frequência das letras que aparecem na mensagem a ser decifrada:

B NBUFNBUJDB F DPOIFDJEB DPNP B SBJOIB EBT DJFODJBT.

Letras	Cálculo da Porcentagem	Frequência (%)
A		
B		
D		
E		
F		
I		
J		
N		
O		
P		
S		
T		
U		

3) Comparando as frequências observadas, descubra o conteúdo cifrado.

11 CONSIDERAÇÕES FINAIS

A Criptografia, por ser um tema de por vezes complexo, foi trabalhada nessa pesquisa, de forma a adaptar conteúdos importantes e de fácil compreensão para o público –alvo da educação de Jovens e Adultos. A riqueza desse tema também nos permitiu relacionar conteúdos matemáticos às situações do mundo real, o que se torna de grande ajuda para desenvolver habilidades e competências na resolução de problemas.

Nossa motivação veio da carência, no ensino público, de propostas de ações voltadas para esta modalidade de ensino, cujo processo de ensino-aprendizagem sofre grandes reveses, pelos mais diversos motivos.

Assim, ao longo desse trabalho tivemos como objetivo a elaboração de atividades adequadas que pudessem enriquecer a prática docente em sala de aula, lhe dando um embasamento teórico e prático sobre Criptografia e suas técnicas, de forma que possam ser utilizadas para contextualizar conteúdos do currículo básico escolar, principalmente os destacados no trabalho como Funções e Sistemas de Numeração.

Também buscamos transitar entre os entes acadêmico-teórico e prático, fazendo sempre referência à Educação de Jovens e Adultos, independentemente das limitações geradas pela pandemia mundial do COVID-19.

No sentido de tentar reduzir desigualdades, o projeto em si contempla o princípio de equidade à luz do BNCC que preza reconhecer as diferenças existentes entre os estudantes nos vieses social e cultural, bem como as diferentes necessidades de cada aluno.

Esperamos desta forma, ter contribuído para auxiliar ao professor na obtenção de ferramentas e artifícios no processo ensino-aprendizagem adequados aos estudantes da Educação de Jovens e Adultos.

REFERÊNCIAS

ALMEIDA, M.A. **Codificando o alfabeto por meio do sistema de numeração binário**. 2013. 60 f. Dissertação (Programa de Mestrado Profissional em Matemática) – Universidade Federal de São Carlos, São Carlos – SP, 2013.

AMARO, E. COVID 19: Uma reflexão sobre o momento que vivemos. **Portal Hospitais Brasil**, São Paulo, 2020. Disponível em: https://portalhospitaisbrasil.com.br/artigo-covid-19-uma-reflexao-sobre-o-momento-que-vivemos/. Acesso em: 18 set. 2020.

ATRACTOR. **Tradutor para Braille**. Disponível em: https://www.atractor.pt/mat/matbr/matbraille.html. Acesso em: 22 set. 2020.

AZEVEDO, R. S. **Resolução de problemas no ensino de função afim**. 2014. 34 f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional) – IMPA, Rio de Janeiro – RJ, 2014.

BEZERRA, D. J.; MALAGUTTI, P. L.; RODRIGUES, V. C. S. Aprendendo Criptologia de Forma Divertida. *In*: BIENAL DA SBM, 5., 2010, Paraíba. **Anais** [...]. Paraíba: Universidade Federal da Paraíba, 2010. p. 1 – p. 139.

BOYER, C. B. **História da matemática**. Revista por Uta C. Merzbach; tradução Elza F. Gomide. 2ª ed. São Paulo: Edgard Blucher, 1996.

BRASIL. COMISSÃO NACIONAL DE AVALIAÇÃO DA EDUCAÇÃO. **História**. Brasília, DF: MEC, © 2018. Disponível em: http://portal.mec.gov.br/conaes-comissao-nacional-de-avaliacao-da-educacao-superior/97-conhecaomec-1447013193/omec-1749236901/2-historia. Acesso em: 29 ago. 2020.

_____ [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988.

_____ **Lei Nº 13.005**, de 25 de junho de 2014. Aprova o Plano Nacional de Educação - PNE e dá outras providências. Brasília, DF: Planalto, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13005.htm#:~:text=Aprova%20o%20Plano%20Nacional%20de,Art. Acesso em: 08 set. 2020.

_____ **Lei nº 9.394**, de 20 de dezembro de 1996. Lei de Diretrizes e Bases da Educação Nacional. Brasília, DF: Planalto, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 29 ago. 2020.

_____ Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, DF: MEC, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 03 set. 2020.

_____ Ministério da Educação. **FUNDEB**. Brasília, DF: MEC, 2007.

_____ Ministério da Educação. **Plano Nacional da Educação**. Brasília, DF: MEC, 2017. Disponível em: http://portal.mec.gov.br/arquivos/pdf/L10172.pdf. Acesso em 08 jul. 2020.

_____ Ministério da Educação. **Plano Nacional de Alfabetização**. Brasília, DF: MEC, 2019. Disponível em: http://portal.mec.gov.br/images/banners/caderno_pna_final.pdf. Acesso em: 03 set. 2020.

CARVALHO, P, C, P.; LIMA, E. L.; MORGADO, A.C WAGNER, E. **A Matemática do Ensino Médio**. Vol. 1. Rio de Janeiro: IMPA, 1997.

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

COVID: UK at 'critical point' in pandemic, top scientists to warn. **BBC NEWS**. Reino Unido, 21 de set. de 2020. Disponível em: https://www.bbc.com/news/uk-54229845. Acesso em: 21 set. 2020.

DI PIERRO, M. C. A educação de jovens e adultos no Plano Nacional de Educação: avaliação, desafios e perspectivas. **Educação & Sociedade**, Campinas, v. 31, n. 112, p. 939-959, jul.-set. 2010. Disponível em: https://www.scielo.br/pdf/es/v31n112/15.pdf. Acesso em: 03 set. 2020.

EVES, H. **Introdução à história da matemática**. Tradução: Hygino H. Domingues. Campinas, SP: Editora da Unicamp, 2004.

FAUSTO, B. **História do Brasil**. 12ª ed. 1ª reimpressão. São Paulo: Edusp, 2006. Disponível em: https://mizanzuk.files.wordpress.com/2018/02/boris-fausto-historia-do-brasil.pdf. Acesso em 29 ago. 2020.

FEITOSA, S. C. S.; GADOTTI, Moacir. **Método Paulo Freire**: princípios e práticas de uma concepção popular de educação. São Paulo: Universidade de São Paulo, 1999.

FERRARI, M. Paulo Freire, o mentor da Educação para a consciência. **Nova Escola**, 2008. Disponível em: https://novaescola.org.br/conteudo/460/mentor-educacao-consciencia. Acesso em: 03 set. 2020.

FERREIRA, L. C. A educação de jovens e adultos em (im)prováveis e de (in)certezas: a BNCC em discussão. **Revista Augustus**, Rio de Janeiro, v. 24, n. 47, p. 9-27, 2019. Disponível em: https://revistas.unisuam.edu.br/index.php/revistaaugustus/article/view/334/150.Acesso em :08 set. 2020.

FREIRE, P. **Pedagogia do Oprimido**. Rio de Janeiro: Paz e Terra, 2020.

FREIRE, Q. G. **Pesquisa mostra Paes liderando e Benedita e Crivella empatados**. diáriodoRio.com, 15 de set. de 2020. Disponível em: https://diariodorio.com/pesquisa-mostra-paes-liderando-e-benedita-e-crivella-empatados/. Acesso em: 21 set. 2020.

HADDAD, S.; DI PIERRO, M. C. Escolarização de jovens e adultos. **Revista Brasileira de Educação**, nº 14, p. 108-194, 2000. Disponível em: https://www.scielo.br/pdf/rbedu/n14/n14a07.pdf. Acesso em: 08 set. 2020.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. **Mapa do analfabetismo no Brasil**. Brasília, DF, 2003.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Censo Demográfico 2000/2010**. Brasília, DF, 2010. Disponível em: http://www.educacao.df.gov.br/wp-conteudo/uploads/2019/03/i_c_taxa_analfabetismo_totaldf_ibge_censo_2010.pdf. Acesso em: 29 ago. 2020.

INTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Censo Demográfico 2000**: sinopse preliminar. Rio de Janeiro, v.7, p. 10-415, 2000. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/periodicos/308/cd_2000_v7.pdf. Acesso em 29 ago. 2020.

LIMA, E. L. **Curso de Análise**. 15ª ed. Rio de Janeiro: IMPA, 2019.

MEDEIROS, V. Z.; CALDEIRA, A. M.; OLIVEIRA, L. M.; MACHADO, M. A. S. **Pré-Cálculo**. São Paulo: Pioneira Thomson Learnig, 2006.

ROQUE, T. **História da Matemática**: Uma visão crítica, desfazendo mitos e lendas. 1ª ed. [S. L.]: Zahar, 2012.

SINGH, S. **O Livro dos Códigos**. Tradução de Jorge Kalife. 3ª ed. Rio de Janeiro: Record, 2003.

SOUSA, D. P., PIRES, J. D. Criptoanálise como proposta didática para o ensino de estatística. **Revista de Ensino de Ciências e Matemática (REnCiMa)**, São Paulo, v.9, n.2, p. 1-11, 2018.

STRELHOW, T. B. Breve história sobre a educação de jovens e adultos no Brasil. **Revista HISTEDBR On-line**, Campinas, n. 38, p. 49-59, 2010. Disponível em: http://www.histedbr.fe.unicamp.br/revista/edicoes/38/art05_38.pdf. Acesso em: 03 set. 2020.

TKOTZ, V. **Análise de frequência on line**. Aldeia Numaboa. Copyright © 1998 – 2020. Disponível em: http://numaboa.com.br/criptografia/criptoanalise/309-Ferramenta-de-frequencia. Acesso em 21 set. 2020.

TKOTZ, V. **Criptografia** – Segredos Embalados para Viagem. São Paulo: Novatec, 2005.

VIEGAS, A. C. C.; MORAES, M. C. S. Um Convite ao Retorno: relevâncias no histórico da EJA no Brasil. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 12, n. 1, p. 456-478, 2017.

VIZOLLI, I.; CARVALHO, E. E. de S.; PEREIRA, O. R. CRIPTOGRAFIA: UMA POSSIBILIDADE PARA O ENSINO DE FUNÇÃO INVERSA. **REAMEC - Rede Amazônica de Educação em Ciências e Matemática**, Cuiabá, v. 7, n. 1, p. 196-212, 2019. Disponível em: https://periodicoscientificos.ufmt.br/ojs/index.php/reamec/article/view/8146. Acesso em: 21 set. 2020.

WALL, E. S. **Teoria dos números para professores do ensino fundamental**. Tradução: Roberto Cataldo Costa; revisão técnica Katia Stocco Smole. Porto Alegre: AMGH, 2014.

APÊNDICE A – RESOLUÇÃO DAS ATIVIDADES PROPOSTAS

ATIVIDADE 1 – CÓDIGO MORSE

Letras (ou espaço)	Codificação	Unidades de Tempo
M	- -	6
Espaço entre letras		3
A	. -	4
Espaço entre letras		3
Y	- . - -	10
Espaço entre letras		3
D	- . .	5
Espaço entre letras		3
A	. -	4
Espaço entre letras		3
Y	- . - -	10

Portanto: MAYDAY ➔ -- .- -.-- -.. .- -.-- ➔ 54 unidades de tempo

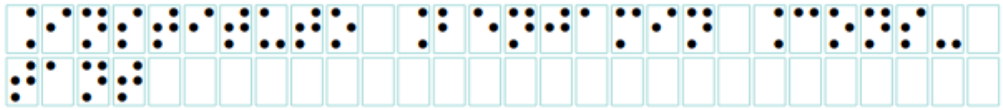
2) Comparando com a tabela de codificação, a mensagem em português foi:

Chamando todos. Este é o nosso último grito antes do nosso silêncio eterno.

ATIVIDADE 2 – CÓDIGO BRAILLE

1) A mensagem decifrada será: A Matemática é a rainha das ciências.

2)



ATIVIDADE 3 – CPF

1) Calculando os dígitos verificadores (D_{V1} e D_{V2}) de 106.723.645:

D_{V1}

1.10 + 0.9 + 6.8 + 7.7 + 2.6 + 3.5 + 6.4 + 4.3 + 5.2 = 180

Dividindo 180 por 11, temos resto 4. Daí, $D_{V1} = 11 – 4 = 7$

D_{V2}

1.11 + 0.10 + 6.9 + 7.8 + 2.7 + 3.6 + 6.5 + 4.4 + 5.3 + 7.2 = 228

Dividindo 228 por 11, temos resto 8. Daí, $D_{V2} = 11 – 8 = 3$

Portanto o C.P.F. será: 106.723.645 – 73.

2) Verificando D_{V1} e D_{V2}:

D_{V1}

1.10 + 3.9 + 2.8 + 4.7 + 4.6 + 2.5 + 3.4 + 3.3 + 7.2 = 150

Dividindo 10 por 11, temos resto 7. Daí, $D_{V1} = 11 – 7 = 4$, confere.

D_{V2}

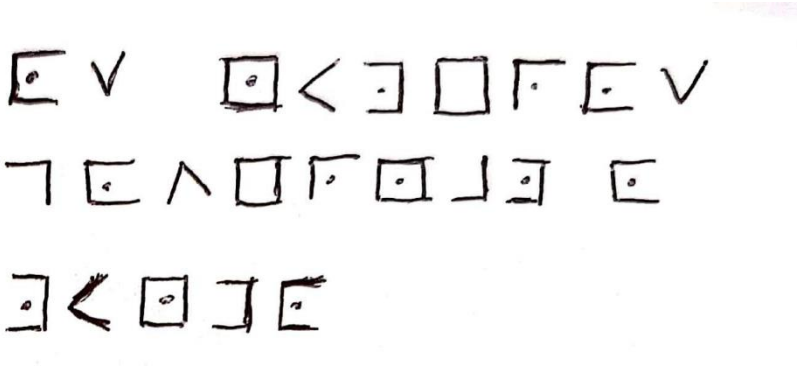
1.11 + 3.10 + 2.9 + 4.8 + 4.7 + 2.6 + 3.5 + 3.4 + 7.3 + 4.2 = 187

Dividindo 187 por 11, temos resto 0. Daí, $D_{V2} = 0$, não confere.

Portanto, 132.442.337 – 45 não é um C.P.F. válido.

ATIVIDADE 4 – CIFRA MAÇÔNICA

1)



2) Frase cifrada: A MATEMÁTICA É A LINGUAGEM UNIVERSAL.

ATIVIDADE 5 – CIFRA DE VIGENÈRE

1) Codificação: UJENBNVYANBDJBVJXB

2) DECODIFICAÇÃO: SEMPRE USEM MASCARA AO SAIR DE CASA

3) Codificação: GRNPCICHOBRLHDOUE.

4) Decodificação: PORCENTAGEM

ATIVIDADE 6 – CIFRA ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A	9	E	5	2	A	F
D	D	O	W	Y	G	V
F	P	4	Q	B	U	X
G	T	3	K	0	C	J
V	H	S	1	Z	7	N
X	M	8	I	6	L	R

QUADRADO → FF FV AV DA XX AV DA DD

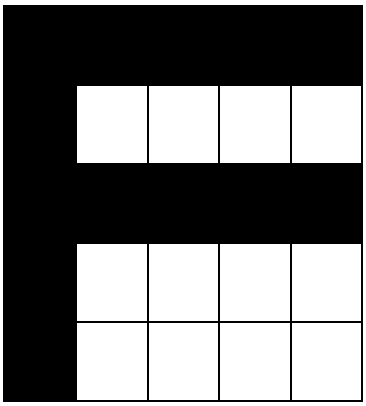
R	**E**	**T**	**A**		**A**	**E**	**R**	**T**
F	F	F	V		V	F	F	F
A	V	D	A		A	V	A	D
X	X	A	V		V	X	X	A
D	A	D	D		D	A	D	D

Palavra cifrada: VAVDFVXAFAXDFDAD

ATIVIDADE 7 – BASE BINÁRIA - QUADRADINHO POR QUADRADINHO

1) 10001 – 01110 – 01010 – 01110 - 10001

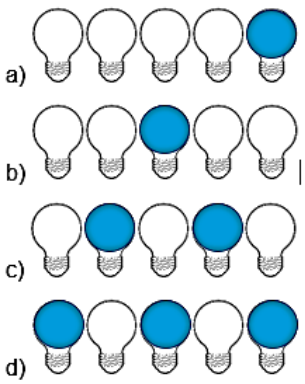
2)



3) A atividade não possui uma solução única definida, visto que fica a critério do leitor.

ATIVIDADE 8 – BASE BINÁRIA – ACENDE / APAGA

1)



2) a) 01010

b) 10010

c) 01011

d) 10110

ATIVIDADE 9 – BASE BINÁRIA – CUSTO DAS LÂMPADAS

1) 26 ➔ 11010

20 ➔ 10100

19 ➔ 10011

18 ➔ 10010

13 ➔ 01101

11 ➔ 01011

9 ➔ 01001

7 ➔ 00111

2) 10010 ➔ 18

00100 ➔ 4

10000 ➔ 16

10101 ➔ 21

ATIVIDADE 10 – DA BASE 10 PARA A BASE 2.

a) 26

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
26			1	1	0	1	0	11010

b) 30

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
30			1	1	1	1	0	11110

c) 56

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
56		1	1	1	0	0	0	111000

d) 47

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
47		1	0	1	1	1	1	101111

e) 72

Base 10	Potências de base 2							Base 2
	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	
72	1	0	0	1	0	0	0	1001000

ATIVIDADE 11 – CODIFICAÇÃO COM A BASE BINÁRIA

1) ANA LUISA: “ESTOU MUITO TRISTE”.

MATHEUS: “O QUE HOUVE”?

ANA LUISA: “IREMOS NOS MUDAR”.

2) MATHEUS: “NÃO IMPORTA A DISTÂNCIA. SEREMOS SEMPRE AMIGOS”!

ATIVIDADE 12 – CIFRA DE CÉSAR - O CELULAR PERDIDO

1)

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

2) RAFAEL ⇔ **TCHCGN**

3) 35 = **100011**

4) 1ª senha: **TCHCGN**

2ª senha: **100011**

ATIVIDADE 13 – FUNÇÕES - O NÚMERO DA CASA DE MARIANA

1) a) Domínio de $f = \{1, 2, 3\}$

b) Contradomínio de $f = \{2, 4, 6\}$

c) Imagem de $f = \{2, 4, 6\}$

d) $y = f(x) = 2x$

e) Sim. Toda função bijetiva admite inversa.

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

2) a) Domínio de $f = \{3, 4, 5\}$

b) Contradomínio de $f = \{7, 9, 11\}$

c) Imagem de $f = \{7, 9, 11\}$

d) $y = f(x) = 2x + 1$

e) Sim. Toda função bijetiva admite inversa.

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

3) a) *f(7) = 7 – 2 = 5*

f(8) = 8 – 2 = 6

f(4) = 4 – 2 = 2

Portanto, o número enviado para Pedro foi 562.

b) Pedro utilizou a inversa de f:

- $f^{-1}(x) = x + 2 \underset{x=5}{\Longrightarrow} 5 + 2 = 7$
- $f^{-1}(x) = x + 2 \underset{x=6}{\Longrightarrow} 6 + 2 = 8$
- $f^{-1}(x) = x + 2 \underset{x=2}{\Longrightarrow} 2 + 2 = 4$

ATIVIDADE 14 – FUNÇÕES E CRIPTOGRAFIA - MENSAGEM SECRETA

Etapa 2

M	A	T	E	M	A	T	I	C	A	R	E	C	R	E	A	T	I	V	A
13	1	20	5	13	1	20	9	3	1	18	5	3	18	5	1	20	9	22	1

Etapa 3

Letra	Sequência Original	Imagem da função $y = f(x) = 2x + 1$	Sequência Cifrada
M	13	$f(x) = 2x + 1 = 2.13 + 1 = 26 + 1 = 27$	27
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 3$	3
T	20	$f(x) = 2x + 1 = 2.20 + 1 = 41$	41
E	5	$f(x) = 2x + 1 = 2.5 + 1 = 11$	11
M	13	$f(x) = 2x + 1 = 2.13 + 1 = 26 + 1 = 27$	27
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 3$	3
T	20	$f(x) = 2x + 1 = 2.20 + 1 = 41$	41
I	9	$f(x) = 2x + 1 = 2.9 + 1 = 19$	19
C	3	$f(x) = 2x + 1 = 2.3 + 1 = 7$	7
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 3$	3
R	18	$f(x) = 2x + 1 = 2.18 + 1 = 37$	37
E	5	$f(x) = 2x + 1 = 2.5 + 1 = 11$	11
C	3	$f(x) = 2x + 1 = 2.3 + 1 = 7$	7
R	18	$f(x) = 2x + 1 = 2.18 + 1 = 37$	37
E	5	$f(x) = 2x + 1 = 2.5 + 1 = 11$	11
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 3$	3
T	20	$f(x) = 2x + 1 = 2.20 + 1 = 41$	41

I	9	$f(x) = 2x + 1 = 2.9 + 1 = 19$	19
V	22	$f(x) = 2x + 1 = 2.22 + 1 = 45$	45
A	1	$f(x) = 2x + 1 = 2.1 + 1 = 3$	3

A sequência numérica transmitida foi:

27-5-41-11-27-5-41-19-7-5-37-11-7-37-11-5-41-19-45-5

Encontrando a função inversa:

$$f(x) = 2x + 1 \xrightarrow[\text{isolando x}]{} x = \frac{f(x)-1}{2} \xrightarrow[\text{aplicando o operador } f^{-1}]{} f^{-1}(x) = \frac{x-1}{2}$$

Sequência Cifrada	**Imagem da Função Inversa** $\mathbf{y = f^{-1}(x) = \frac{x-1}{2}}$	**Sequência Original**	**Letra**
27	$f^{-1}(x) = \frac{x-1}{2} = \frac{27-1}{2} = 13$	13	M
3	$f^{-1}(x) = \frac{x-1}{2} = \frac{2}{2} = 1$	1	A
41	$f^{-1}(x) = \frac{x-1}{2} = \frac{40}{2} = 20$	20	T
11	$f^{-1}(x) = \frac{x-1}{2} = \frac{10}{2} = 5$	5	E
27	$f^{-1}(x) = \frac{x-1}{2} = \frac{26}{2} = 13$	13	M
3	$f^{-1}(x) = \frac{x-1}{2} = \frac{2}{2} = 1$	1	A
41	$f^{-1}(x) = \frac{x-1}{2} = \frac{40}{2} = 20$	20	T
19	$f^{-1}(x) = \frac{x-1}{2} = \frac{18}{2} = 9$	9	I
7	$f^{-1}(x) = \frac{x-1}{2} = \frac{6}{2} = 3$	3	C
3	$f^{-1}(x) = \frac{x-1}{2} = \frac{2}{2} = 1$	1	A

37	$f^{-1}(x) = \frac{x-1}{2} = \frac{36}{2} = 18$	18	R
11	$f^{-1}(x) = \frac{x-1}{2} = \frac{10}{2} = 5$	5	E
7	$f^{-1}(x) = \frac{x-1}{2} = \frac{6}{2} = 3$	3	C
37	$f^{-1}(x) = \frac{x-1}{2} = \frac{36}{2} = 18$	18	R
11	$f^{-1}(x) = \frac{x-1}{2} = \frac{10}{2} = 5$	5	E
3	$f^{-1}(x) = \frac{x-1}{2} = \frac{2}{2} = 1$	1	A
41	$f^{-1}(x) = \frac{x-1}{2} = \frac{40}{2} = 20$	20	T
19	$f^{-1}(x) = \frac{x-1}{2} = \frac{18}{2} = 9$	9	I
45	$f^{-1}(x) = \frac{x-1}{2} = \frac{44}{2} = 22$	22	V
5	$f^{-1}(x) = \frac{x-1}{2} = \frac{2}{2} = 1$	1	A

Em relação ao questionamento lançado, espera-se que o aluno observe e relacione minimamente, o fato de todos os valores resultantes na sequência cifrada serem ímpares. A partir de tal fato, a correlação com a caracterização 2k + 1, referente aos números ímpares (paridade).

ATIVIDADE 15 – ANÁLISE DE FREQUÊNCIAS - CONSOANTES E VOGAIS

Letras	Cálculo da Porcentagem	Frequência (%)
A	$\frac{88}{650} = 0{,}135$	13,5
B	$\frac{4}{650} = 0{,}006$	0,6
C	$\frac{32}{650} = 0{,}049$	4,9
D	$\frac{35}{650} = 0{,}054$	5,4
E	$\frac{60}{650} = 0{,}092$	9,2
F	$\frac{5}{650} = 0{,}007$	0,7
G	$\frac{6}{650} = 0{,}009$	0,9
H	$\frac{4}{650} = 0{,}006$	0,6
I	$\frac{32}{650} = 0{,}049$	4,9
L	$\frac{9}{650} = 0{,}014$	1,4
M	$\frac{35}{650} = 0{,}054$	5,4
N	$\frac{28}{650} = 0{,}043$	4,3
O	$\frac{52}{650} = 0{,}08$	8
P	$\frac{12}{650} = 0{,}018$	1,8
Q	$\frac{2}{650} = 0{,}003$	0,3
R	$\frac{37}{650} = 0{,}057$	5,7
S	$\frac{41}{650} = 0{,}063$	6,3
T	$\frac{23}{650} = 0{,}035$	3,5
U	$\frac{13}{650} = 0{,}02$	2

V	$\frac{10}{650} = 0{,}015$	1,5
X	$\frac{2}{650} = 0{,}003$	0,3
Z	$\frac{3}{650} = 0{,}005$	0,5

2)

Letras	**Cálculo da Porcentagem**	**Frequência (%)**
B	$\frac{10}{43} = 0{,}23$	23
D	$\frac{6}{43} = 0{,}14$	14
E	$\frac{2}{43} = 0{,}05$	5
F	$\frac{4}{43} = 0{,}09$	9
I	$\frac{2}{43} = 0{,}05$	5
J	$\frac{5}{43} = 0{,}12$	12
N	$\frac{3}{43} = 0{,}07$	7
O	$\frac{3}{43} = 0{,}07$	7
P	$\frac{3}{43} = 0{,}07$	7
S	$\frac{1}{43} = 0{,}02$	2
T	$\frac{2}{43} = 0{,}05$	5
U	$\frac{2}{43} = 0{,}05$	5

3) A MATEMÁTICA É CONHECIDA COMO A RAINHA DAS CIÊNCIAS.