**Universidade Federal de São Paulo**

Instituto De Ciências Ambientais,

Químicas E Farmacêuticas

**Campus Diadema**


Mestrado Profissional em Matemática

em Rede Nacional - PROFMAT

# Cripto Alien: Criptografando com Álgebra Abstrata. Aplicativo para Dispositivo Móvel.

Samanta Próspero Martins da Costa

Orientador: Profª. Drª. Paola Andrea Gaviria Kassama

**Diadema**

**Dezembro, 2021**


Título: *Cripto Alien: Criptografando com Álgebra Abstrata. Aplicativo para Dispositivo Móvel.*

Dissertação apresentada ao Instituto De Ciências Ambientais, Químicas E Farmacêuticas da UNIFESP, campus Diadema/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

**Diadema**

**Dezembro, 2021**

Costa, Samanta Próspero Martins da

**Cripto Alien: Criptografando com Álgebra Abstrata. Aplicativo para Dispositivo Móvel.** , Samanta Próspero Martins da Costa – Diadema, 2021.

ii, 73f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto De Ciências Ambientais, Químicas E Farmacêuticas. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Alien Crypto: Encrypting with Abstract Algebra. Application for Mobile Device.

1. Cripto Alien. 2. Cifras de Hill. 3. Matriz. 4. Aplicativo. 5. Aritmética Modular.

Serviço Público Federal
Ministério da Educação
**Universidade Federal de São Paulo**

PROGRAMA MESTRADO PROFISSIONAL DE MATEMÁTICA

ATA DE DEFESA DISSERTAÇÃO E TESE nº 0932995/2021/PROGRAMA MESTRADO PROFISSIONAL DE MATEMÁTICA

Diadema, 17 de dezembro de 2021.

Aos dezessete dias do mês de dezembro do ano de dois mil e vinte e um, reuniu-se através da Plataforma Google Meet às 14:00 horas, a Comissão Julgadora para a DEFESA DE DISSERTAÇÃO DE MESTRADO, solicitada por **SAMANTA PRÓSPERO MARTINS DA COSTA**, aluno(a) do Programa de Pós-Graduação **Mestrado Profissional em Matemática - PROFMAT**, que apresentou dissertação sob o Título: "**CRIPTO ALIEN: CRIPTOGRAFANDO COM ÁLGEBRA ABSTRATA. APLICATIVO PARA DISPOSITIVO MÓVEL"**.

A referida Comissão esteve constituída pelos Professores Doutores:

Profa. Dra. Sandra Maria Zapata Yepes - Universidade Federal do ABC;

Profa. Dra. Roseli Künzel - Universidade Federal de São Paulo;

Profa. Dra. Verilda Speridião Kluth - Universidade Federal de São Paulo.

O(a) Presidente Prof(a). Dr(a). **Paola Andrea Gaviria Kassama** inicia a sessão dando a palavra ao(a) candidato(a), que dispõe de um período de tempo entre trinta e cinquenta minutos, para expor sua tese. A seguir dá a palavra aos Professores para a arguição. Cada examinador(a) dispõe de trinta minutos, no máximo, para arguição, bem como o(a) candidato(a) para as respostas. Tendo o(a) candidato(a) respondido todas as arguições em tempo hábil os membros da Banca Examinadora, emitiram seus Pareceres:

| | |
|---|---|
| Prof(a). Dr(a). Sandra Maria Zapata Yepes | **( x )APROVADO ( ) REPROVADO** |
| Prof(a). Dr(a). Roseli Künzel | **( x )APROVADO ( ) REPROVADO** |
| Prof(a). Dr(a). Verilda Speridião Kluth | **( x )APROVADO ( ) REPROVADO** |
| Prof(a). Dr(a). Paola Andrea Gaviria Kassama | **Orientador(a) / Presidente** |

Em face dos referidos pareceres, a Comissão Julgadora considera o(a) Sr(a) **SAMANTA PRÓSPERO MARTINS DA COSTA**

( x )**Habilitado**

( )**NÃO** habilitado

a receber o título de MESTRADO PROFISSIONAL EM MATEMÁTICA pela UNIVERSIDADE FEDERAL DE SÃO PAULO.

E por estarem de acordo, assinam a presente ata.

Diadema, 17 de dezembro de 2021.

| |
|---|
| Sugestões e Observações: |

Documento assinado eletronicamente por **Sandra Maria Zapata Yepes**, **Usuário Externo**, em 17/12/2021, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Verilda Speridiao Kluth**, **Docente**, em 17/12/2021, às 16:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Roseli Kunzel**, **Docente**, em 17/12/2021, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Paola Andrea Gaviria Kassama**, **Docente**, em 17/12/2021, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida clicando aqui, ou pelo endereço: "https://sei.unifesp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0" informando o código verificador **0932995** e o código CRC **44662B93**.

**UNIVERSIDADE FEDERAL DE SÃO PAULO**

**Instituto De Ciências Ambientais, Químicas E Farmacêuticas**

**Mestrado Profissional em Matemática em Rede Nacional**

**PROFMAT**

**Chefe de departamento:**

Prof. Dr. Renato Marcone José de Souza

**Coordenador do Programa de Pós-Graduação:**

Prof. Dr. Renato de Sá Teles

SAMANTA PRÓSPERO MARTINS DA COSTA

# CRIPTO ALIEN: CRIPTOGRAFANDO COM ÁLGEBRA ABSTRATA. APLICATIVO PARA DISPOSITIVO MÓVEL.

**Presidente da banca:** Profª. Drª. Paola Andrea Gaviria Kassama

**Banca examinadora:**

Prof. Drª. Sandra Maria Zapata Yepes

Prof. Drª. Roseli Künzel

Prof. Drª. Verilda Speridião Kluth

**Data da Defesa:** 17 de Dezembro de 2021

*"Sonho que se sonha só, é só um sonho que se sonha só,*

*mas sonho que se sonha junto é realidade".*

*Raul Santos Seixas*

# AGRADECIMENTOS

Agradeço primeiramente ao meu marido Carlos Alberto Cardoso de Godoy, por todo apoio desde sempre, pelo amor e carinho, e por ser o melhor exemplo de caráter que poderia existir.

Agradeço ao meu filho, Felipe Martins de Godoy e a minha nora, Maria Angélica da Silva Passador pelo apoio, incentivo e por fazerem parte da minha vida.

Aos meus colegas e professores do PROFMAT 2018. Me sinto privilegiada por ter feito parte dessa turma. Obrigada a todos!

Um grande agradecimento a minha orientadora, Dra. Paola Andrea Gaviria Kassama, pela paciência, dedicação e por me alentar em momentos que achei que não conseguiria. Saiba que sua competência e seu amor pela profissão inspiram não só a mim, mas a todos os seus alunos.

Agradeço ao Matheus Gaviria Kassama a quem eu chamo carinhosamente de designer mirim e ao Leandro pelas grandes dicas de design, uma habilidade impossível pra mim.

Ao grande médico Dr. Tuffi Hachul, que tratou da minha saúde mental em um período muito difícil. Sem seus cuidados, provavelmente eu não teria nem começado este trabalho.

Agradeço também aos professores de programação, em especial aos professores Gustavo Guanabara, Diego Schell Fernandes, Luiz Otávio Miranda, Fernando Daciuk e Jamilton Damasceno, entre tantos outros, por todos os valiosos ensinamentos.

Agradeço também à CAPES pelo apoio financeiro a este trabalho.

Enfim, agradeço a todos que de alguma forma contribuíram para a minha formação acadêmica, e também na elaboração desse trabalho e na conclusão do PROFMAT.

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

# RESUMO

O avanço tecnológico, seguido do intenso fluxo de informações e, aliado ao panorama de desigualdade social evidenciado pela pandemia da COVID-19, sugere a necessidade de novas alternativas em prol do ensino. Neste contexto, este trabalho arquitetou um aplicativo para dispositivo móvel, a fim de, proporcionar um jogo com desafios matemáticos no qual o público alvo, alunos do ensino médio, relembrem operações matriciais e implicitamente trabalhem com aritmética modular. Realiza-se então, uma pesquisa de natureza qualitativa e de caráter exploratório, no contexto do ensino de matemática para o ensino médio. Pesquisa-se sobre criptografia, em particular, a técnica denominada Cifra de Hill. Concomitantemente busca-se pelos conhecimentos tecnológicos específicos e indispensáveis para desenvolver um aplicativo. Como resultado, foi concebido um aplicativo que recebeu o nome de Cripto Alien, é gratuito e de código aberto, disponível para download e cópia sem fins comerciais através do link: <https://github.com/samantaProspero/criptoalien_final>, estando também disponível para download no Google Play Store.



**Palavras-chave:** 1. Cripto Alien. 2. Cifras de Hill. 3. Matriz. 4. Aplicativo. 5. Aritmética Modular.

## ABSTRACT

Technological advances, followed by the intense flow of information and, together with the panorama of social inequality evidenced by the COVID-19 pandemic, suggests the need for new alternatives in favor of education. In this context, this work designed an application for mobile device, in order to provide a game with mathematical challenges in which the target audience, high school students, remember matrix operations and implicitly work with modular arithmetic. A qualitative and exploratory research is carried out, in the context of teaching mathematics for high school. Research is being done on cryptography, in particular, the technique called Hill Cipher. At the same time, the search for specific and indispensable technological knowledge to develop an application. As a result, an application named Crypto Alien was designed, it is free and open source, available for download and copy without commercial purposes through the link: <https://github.com/samantaProspero/criptoalien_final>, it is also available for download from the Google Play Store.



**Keywords:** 1. Cripto Alien. 2. Hill System. 3. Matrix. 4. app. 5. Modular arithmetic.

# LISTA DE TABELAS

# LISTA DE FIGURAS

SUMÁRIO

# 1

# INTRODUÇÃO

No contexto atual, após quase dois anos da pandemia gerada pelo corona vírus (SARS-COV-2) a inserção e acessibilidade às tecnologias digitais mostrou-se indispensável na educação. A vulnerabilidade dos alunos de baixa renda ficou mais evidente, visto a dificuldade de se ter dispositivos e internet de boa qualidade para mediar os trabalhos desenvolvidos no ambiente familiar. Segundo dados do IBGE (BARROS, 2021), em 2019, 98,4% dos estudante da escolas privadas tinham acesso à internet, enquanto no ensino público, eram 83,7%. No mesmo ano, o celular foi o equipamento mais usado para acesso à internet, 98,6% das pessoas usaram o telefone móvel para troca de mensagens de texto, voz ou imagens por aplicativos (não e-mails). Outra questão diz respeito às tecnologias digitais não assegurarem a aprendizagem ou o surgimento de ideias inovadoras, segundo Sonego;Behar: "Para tanto, considera-se necessário desenvolver oportunidades viáveis com os dispositivos móveis, de forma que, possam promover situações desafiadoras para os professores e estudantes." (SONEGO; BEHAR, 2015). Partindo da ideia que a tecnologia móvel oportuniza momentos para intensificar a aprendizagem e considerando que, celulares de baixo custo são dispositivos tecnológicos ao alcance da uma boa parte da população, esta pesquisa teve como objetivo geral o desenvolvimento de um aplicativo para dispositivo móvel que proporcione a prática de conceitos aprendidos em aula. Também, foram delineados os seguintes objetivos específicos: conceituar criptografia, detalhar Cifra de Hill, desenvolver o aplicativo Cripto Alien e disponibilizá-lo de forma gratuita.

O presente trabalho possui a seguinte estrutura de capítulos:

Inicialmente, apresenta-se a origem e o desenvolvimento histórico da criptografia bem como as principais técnicas desenvolvidas. Em seguida, apresenta-se a Cifra de Hill, sua origem, seus conceitos matemáticos bem como seus algoritmos para codifica-

ção e decodificação. E, finalmente, apresenta-se o aplicativo Cripto Alien, tecnologias utilizadas, narrativa do jogo, descrição de suas telas e dos desafios de cada fase.

## METODOLOGIA

O presente estudo consiste em pesquisa aplicada, de caráter exploratório, visando construir uma base de conhecimento que possibilite a construção do aplicativo.

A pesquisa surge no contexto do ensino de matemática para o ensino médio. A escolha do público alvo, segundo ano, se deu por ser o ano no qual são oferecidas as noções básicas de operações matriciais.

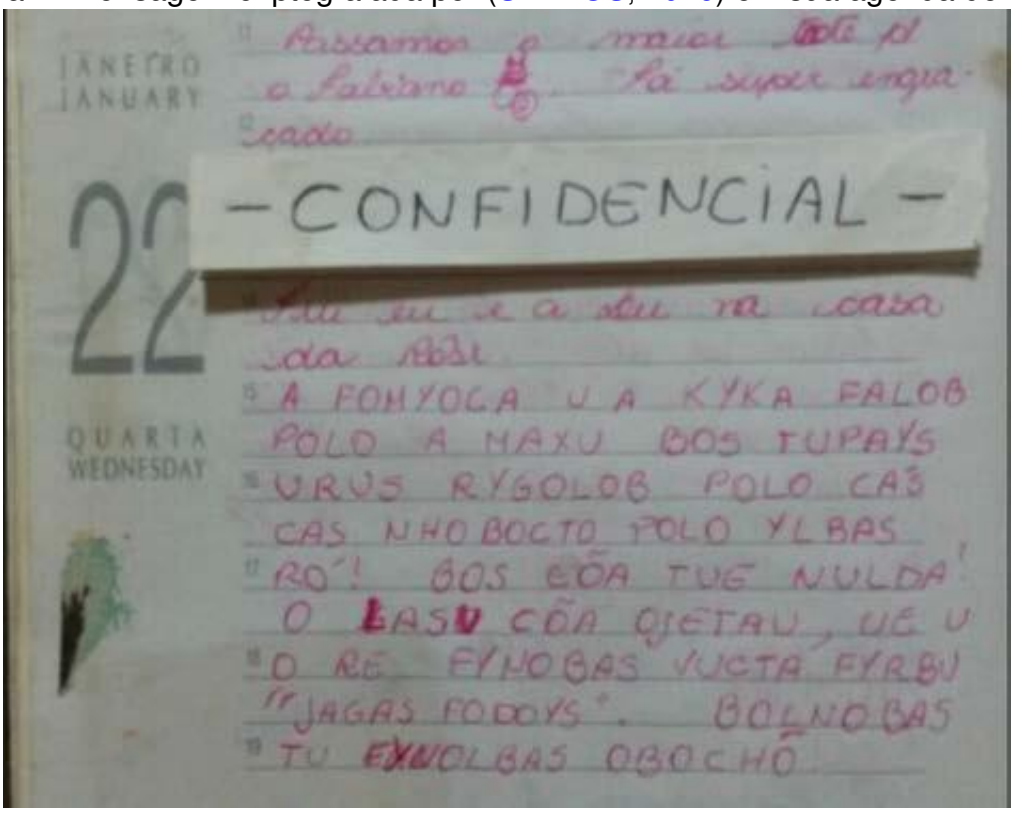
O problema que deu origem à pesquisa, parte da necessidade de dar continuidade, de maneira prática, aos conceitos iniciais de álgebra linear.

Na tentativa de criar outra possibilidade para a prática extraclasse, de assuntos trabalhados em sala de aula, emerge a ideia de um aplicativo como potencial ferramenta para abordar conceitos dentro e fora da sala de aula. Tendo em vista que o aplicativo não poderia ser meramente um software para resolução de exercícios, era necessário levantar alguma conjectura sobre o comportamento e as relações entre os adolescentes, público alvo para o presente trabalho.

À partir de nossas experiências pessoais, reconhecemos que a adolescência é uma época na qual prima a urgência em se manter a privacidade e, como destacado por (SANTOS, 2016) em sua dissertação, uma forma de esconder as informações na troca de mensagens entre os adolescentes é trocar as vogais por uma letra específica, ou ainda, aparecem novas formas para garantir a segurança do significado de suas mensagens.

> Depois de um tempo, esse artifício começou a ficar muito conhecido e, portanto, perdeu sua utilidade. Começamos então a inventar formas secretas para escrever mensagens umas para as outras ou para escrever em nossos diários era uma forma segura de garantir que nossos segredos ficariam somente entre nós. (SANTOS, 2016)(p.6)

Figura 1: Mensagem criptografada por (SANTOS, 2016) em sua agenda de 1992




Fonte: (SANTOS, 2016)(p.6)

Dado que, a preocupação em manter o sigilo das informações nas trocas de mensagens não é um privilégio dos adolescentes e sim uma necessidade que surgiu nos primórdios da humanidade, chegamos na criptografia, na qual, um dos métodos para codificar mensagens, baseado em transformações matriciais, é conhecido como Cifras de Hill.

Neste ponto se inicia a procura por uma base teórica.

A busca dos trabalhos foi realizada nas bases de dados eletrônicas ScienceDirect, SciELO, Capes, ERIC e Google Scholar. No processo de busca, foram utilizados os seguintes descritores em língua portuguesa e inglesa: Criptografia (Cryptography), Cifra de Hill (Hill System), História da Criptografia (Cryptography History), sempre utilizando operadores lógicos “AND”, “OR” e “AND NOT” para combinação dos descritores e termos utilizados a fim de efetuar o rastreamento das publicações.

Os critérios de inclusão foram artigos científicos e livros referentes ao tema, publicados sem distinção de ano, com ênfase nos trabalhos mais citados, disponíveis

na íntegra nas referidas bases de dados eletrônicas, nos idiomas português e inglês, além de dissertações, teses e documentos oficiais pertinentes para complementação da revisão de literatura do tema em análise. Os critérios de exclusão foram artigos disponíveis apenas na forma de resumo.

Os conceitos matemáticos de Álgebra Abstrata e Álgebra Linear, foram pesquisados em livros.

A etapa da construção do aplicativo iniciou-se com uma busca de quais conhecimentos eram necessários para o desenvolvimento do aplicativo.

Em seguida, começou-se um estudo sobre os fundamentos de HTML, CSS e Javascript, além do aprofundamento dos conceitos de frontend, backend e internet.

Foram realizados vários cursos de algoritmo de programação e desenvolvimento de websites, entre eles:

- Curso em Vídeo: HTML5 Completo e Grátis, disponível em (GUANABARA, 2013)
- Curso em Vídeo: Curso de Lógica da Programação, disponível em (GUANABARA, 2014)
- Curso em Vídeo: Curso de JavaScript e ECMAScript para iniciantes, disponível em (GUANABARA, 2019)
- Desenvolvimento Web Completo- 20 cursos + 20 projetos, professor Jamilton Damasceno, disponível na plataforma Udemy através do endereço (DAMASCENO, 2019)
- Curso JavaScript Ninja (DACIUK, 2020)
- Curso de JavaScript e TypeScript do básico ao avançado, professor Luiz Otávio Miranda, disponível na plataforma Udemy através do endereço (MIRANDA, 2019)
- Bootcamp Launchbase Rocketseat (BRITO, 2020)

Além de vários minicursos gratuitos da Rocketseat e de canais do Youtube.

Durante os cursos, iniciou-se o trabalho de ideação e desenvolvimento do protótipo do aplicativo.

À partir do protótipo, iniciou-se a construção do aplicativo com busca nas documentações oficiais das ferramentas e nos fóruns de ajuda para implantação das funcionalidades, conforme as necessidades iam surgindo.

Após a criação do aplicativo, iniciou-se a fase de testes das funcionalidades e correções dos erros encontrados.

E finalmente, após estudos em tutoriais, foi feita a hospedagem do aplicativo no Google Play Store para uma nova fase de testes, na busca de erros ainda não identificados e sua correção.

# 2

# CRIPTOGRAFIA

A criptografia é uma ciência presente ao longo de toda história da humanidade, desde o desenvolvimento da escrita.

> Em grande medida, a humanidade deve seu progresso à habilidade de se comunicar, e um aspecto fundamental nessa habilidade é a capacidade de comunicação por escrito. Desde os primeiros dias de escrita, ocorreram ocasiões em que os indivíduos desejavam limitar suas informações a um grupo restrito de pessoas. Eles tinham segredos que queriam esconder. Para este fim, tais indivíduos desenvolveram ideias por meios pelos quais suas comunicações poderiam ser tornadas ininteligíveis para aqueles que não receberam as informações especiais necessárias para a decifração. As técnicas gerais usadas para realizar tal propósito, ou seja, ocultar o significado das mensagens, constituem o estudo conhecido como criptografia. (SINKOV; FEIL, 2009)(p.1)

Durante a maior parte deste período, esta ciência ficou restrita aos meios militares, governamentais e religiosos. Segundo (PAAR; PELZL, 2009), somente na década de 1980 que a criptografia se tornou presente também nos setores bancário e de telecomunicação. Sendo que, à partir deste momento, com o desenvolvimento da tecnologia e da internet, gradativamente, foi se tornando necessária em todas as áreas e na vida de todas as pessoas.

A História da criptografia é dividida em duas partes:

- clássica: da sua origem até o século XIX,
- moderna: do século XX até os tempos atuais.

## 2.1 ORIGENS E SIGNIFICADO

A palavra criptografia é derivada das palavras gregas *kriptos* que significa oculto e *graphien* que significa escrever e é definida como: “a ciência de cifragem de mensagens, ou a ciência de esconder o significado de uma mensagem.” (SINGH, 2001), (p 423)

Ela surgiu há milênios, da necessidade de proteger informações sigilosas nas trocas de mensagens escritas.

Vale ressaltar que a criptografia está contida em uma ciência mais ampla, denominada criptologia. Segundo (PAAR; PELZL, 2009), a criptologia se divide em dois ramos:

- Criptografia: "ciência da escrita secreta com o objetivo de ocultar o significado de uma mensagem."
- Criptoanálise: "ciência e às vezes a arte de quebrar criptossistemas. ...A criptoanálise é de importância central para os criptossistemas modernos: sem pessoas que tentem quebrar nossos métodos de criptografia, nunca saberemos se eles são realmente seguros ou não."

> Os decifradores de códigos são os alquimistas linguísticos, uma tribo mística que tenta invocar palavras que tenham significado a partir de uma mistura de símbolos sem sentido. A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de códigos e os decifradores, uma corrida armamentista intelectual que teve um forte impacto no curso da história humana. A batalha contínua entre os criadores e os decifradores de códigos inspirou toda uma série de notáveis descobertas científicas. Os codificadores têm buscado sempre criar códigos cada vez mais fortes, para defender as comunicações, enquanto os decifradores inventam sempre métodos mais poderosos para atacá-los. Em seus esforços para preservar ou destruir o sigilo, ambos os lados se apoiam numa grande variedade de disciplinas e tecnologias, da matemática à linguística, da teoria da informação à teoria quântica. E, em troca, os criadores e os decifradores de códigos enriqueceram estas áreas, acelerando com seu trabalho o desenvolvimento tecnológico, principalmente no caso do computador moderno. (SINGH, 2001)(p. 12)

Este duelo entre quem codifica e quem tenta decifrar proporcionou um ambiente propício para grande evolução em ambos os lados.

Quanto aos primórdios da criptografia, destacam-se dois momentos: o primeiro, em aproximadamente 1900 a.C., que, segundo (KAHN, 1996), um escriba “abriu a história registrada da criptografia” ao substituir hieroglifos comuns por outros, menos comuns. Não foi uma criptografia propriamente dita, pois seu objetivo não era esconder uma mensagem, mas foi um marco importante pela “transformação deliberada da escrita”.

O segundo momento, descrito por (SINGH, 2001), ocorreu no séc. V a.C., durante conflitos entre persas e gregos, nos quais um grego exilado, que vivia na Pérsia, ao saber de um ataque surpresa, enviou uma mensagem secreta, avisando aos gregos e evitando que a Grécia fosse conquistada pelos opressores. Para o envio da mensagem, removeram a cera de uma tabuleta, escreveram a mensagem e cobriram a escrita novamente com cera, fazendo-a parecer com uma tabuleta vazia.

## 2.2 ESTEGANOGRAFIA

A predecessora da criptografia é a esteganografia, “nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever” (SINGH, 2001), (p 21). Esteganografia consiste na ocultação da mensagem, não de seu significado.

Ao longo da história, desenvolveram-se várias técnicas de esteganografia, inclusive a conhecida como tinta invisível, que foram muito úteis para proteção de informações sigilosas, porém, com uma fraqueza, se o inimigo descobrisse a mensagem, logo teria acesso ao seu conteúdo. Desde o surgimento da criptografia, este problema, muitas vezes era resolvido, combinando criptografia com esteganografia, ou seja, ocultando mensagem e significado, proporcionando duas camadas de segurança.

## 2.3 TIPOS DE CRIPTOGRAFIA

A criptografia pode ser dividida em dois tipos, de transposição e de substituição. Na transposição, forma-se uma permutação da palavra, misturando suas letras e ordenando-as de outra forma, técnica de fácil descoberta, principalmente com mensagens curtas ou palavras pequenas.

Na substituição, cada letra é trocada por outra letra ou símbolo, (SINGH, 2001) afirma que: “A transposição faz com que cada letra mantenha sua identidade, mas muda sua posição, enquanto a substituição faz com que as letras mudem de identidade, retendo a posição.”

O primeiro registro da criptografia por substituição é a chamada Cifra de César, usada com objetivos militares pelo líder romano Júlio César (100 a.C.- 44 a.C.). Sua técnica era basicamente substituir cada letra pela terceira letra seguinte do alfabeto, conforme imagem abaixo.

Tabela 1: Cifra de César

| Alfabeto | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alfabeto Cifrado | c | d | e | f | g | h | i | j | k | l | m | n | o |

| Alfabeto | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alfabeto Cifrado | p | q | r | s | t | u | v | w | x | y | z | a | b |

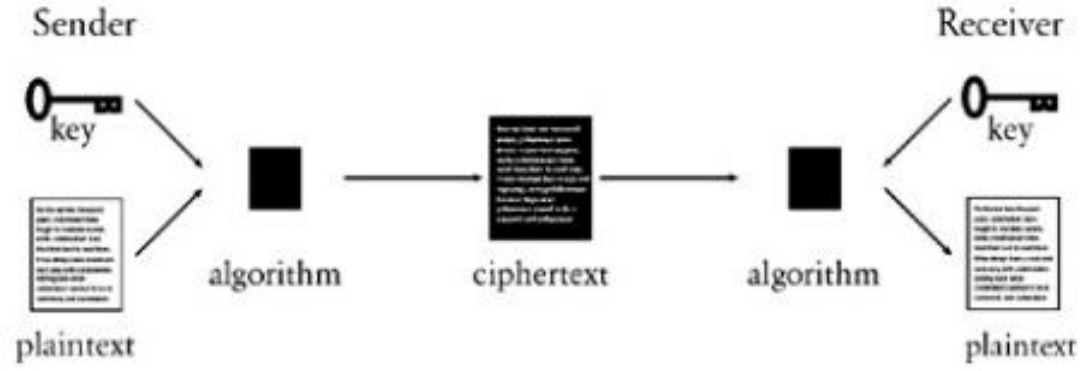
Fonte: a própria autora

Cada letra que substitui a letra do alfabeto original é denominada cifra e, o novo alfabeto formado por essas cifras é denominado alfabeto cifrado.

Todo método criptográfico possui um algoritmo e uma chave.

- O algoritmo é a forma geral, a técnica utilizada.
- A chave é a parte específica, o detalhe de como o algoritmo é implantado.

Figura 2: Chaves na Criptografia




Fonte: Singh, Simon (2021, p. 47)

No caso da Cifra de César, o algoritmo é o método de substituição e a chave é o alfabeto criptografado.

## 2.4 CRIPTOGRAFIA DE SUBSTITUIÇÃO MONOALFABÉTICA

Variações da Cifra de César foram muito usadas por vários séculos, contando com máxima segurança, pois existiam muitas formas de alfabeto cifrado, ao menos $26! \approx 2^{88}$, contando somente as letras, sendo possível aumentar esta quantidade ainda mais, com a inserção de algarismos e/ou outros símbolos.

(SINGH, 2001),(p 29) apresenta uma variação da cifra de César muito difundida, que consiste no uso de uma palavra como chave do alfabeto cifrado.

Para melhor compreensão, a palavra CRIPTOGRAFIA será usada como exemplo. O alfabeto cifrado será iniciado pela letras da palavra CRIPTOGAF, que é a palavra CRIPTOGRAFIA sem letras repetidas. O restante do alfabeto será completado com as demais letras ainda não utilizadas, conforme figura:

Tabela 2: Criptografia de chave

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c | r | i | p | t | o | g | a | f | b | d | e | h |

| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| j | k | l | m | n | q | s | u | v | w | x | y | z |

Fonte: a própria autora

Assim, obtem-se o alfabeto cifrado pela chave CRIPTOGRAFIA.

A criptografia de substituição denominada monoalfabética era muito segura devido a grande quantidade de possíveis chaves, tornando inviável a decifração por busca exaustiva ou ataque de força bruta, sendo que esta técnica ainda é trabalhosa e demorada para os computadores de hoje. Ela só deixou de ser segura com o advento dos criptoanalistas e da análise de frequência.

## 2.5 CRIPTOANALISTAS E A ANÁLISE DE FREQUÊNCIA

Segundo (SINGH, 2001), (p 32), estudiosos árabes, pelo seu alto desenvolvimento em matemática, estatística e linguística, criaram uma técnica para decifrar códigos de cifra de substituição monoalfabética sem o conhecimento da chave, através do estudo de frequência das letras, dando início a criptoanálise.

> Os processos analíticos usados por um criptoanalista requerem um número de técnicas: algumas matemáticas, algumas linguísticas, algumas de uma caractere estranho, e mesmo alguns não prontamente descritíveis, como sorte, talento, sexto sentido, etc. (SINKOV; FEIL, 2009)(p. 2)

A análise de frequência, denominada por (PAAR; PELZL, 2009) como ataque analítico, consiste em analisar um texto normal, desde que seja na mesma língua da que se deseja decifrar. Registrando as letras que mais aparecem, e enumerando-as. Ao pegar o texto criptografado, basta fazer a mesma análise, e substituir a letra mais frequente pela registrada como de número um, a segunda pela de número dois, e assim sucessivamente.

O método permite analisar outras características no texto, como pares ou grupos de letras de uso frequente na lingua adotada.Na língua portuguesa, por exemplo, os

pares "qu", "m"antes de "p"e "b", "rr","ss", entre outros, podem dar dicas para identificação de letras em um texto codificado.

Outra particularidade é a análise de palavras curtas existentes na lingua com "uma", "fim", "os", "as", etc.

Esta técnica, desenvolvida pelo cientista árabe Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi no século IX, permitiu grandes vitórias para a criptoanálise.

Esse desenvolvimento ocorreu bem mais tarde nos demais países, depois de um longo período necessário para desenvolvimento do conhecimento da matemática, da estatística, da linguística, entre outros pré-requisitos. Segundo (SINGH, 2001), o primeiro grande criptoanalista da Europa surgiu somente em 1506, seu nome era Giovani Soro.

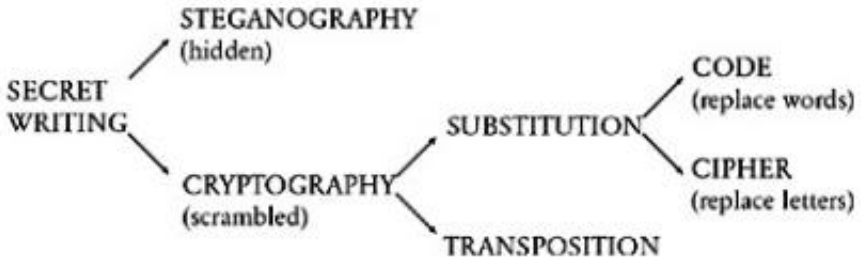
## 2.6 BUSCA POR NOVAS TÉCNICAS

Com as técnicas de criptografia existentes, deixando de ser seguras, tornou-se necessária uma busca por novas alternativas. Muitas foram desenvolvidas, umas fáceis demais para os criptoanalistas, outras difíceis demais tanto para criptoanalistas quanto para sua implantação.

Tentaram dificultar a análise de frequência inserindo e distribuindo ao acaso, no texto, letras ou símbolos sem nenhum significado, os chamados nulos. Outra forma era escrever as palavras com erro de ortografia.

Uma terceira forma foi o uso de palavras-código, neste caso, ao invés de cifrar as letras, cada palavra corresponderia a outra palavra ou símbolo.

Figura 3: Escrita Secreta




Fonte: Singh, Simon (2021, p 47)

Esta técnica apresentava uma grande dificuldade, ao invés de um alfabeto cifrado, tanto o remetente, quanto destinatário deveriam possuir uma espécie de dicionário que continha todas as palavras possíveis. Esse fato tornou a prática inviável, na maioria das vezes, além de ter sua segurança comprometida, visto que, se o inimigo tivesse acesso a este dicionário, todas as mensagens geradas por estes códigos, estariam comprometidas.

Segundo (SINGH, 2001), no século XVI desenvolveram uma forma intermediária entre cifras e palavras-código, os chamados nomenclatores. Este método consistia no uso de uma quantidade limitada de palavras código, e o restante do texto sendo encriptado por um alfabeto cifrado. Esta técnica foi facilmente quebrada pelos criptoanalistas, pelo uso da análise de frequência na maior parte do texto, e o restante sendo deduzido pelo contexto já decifrado.

## 2.7 CRIPTOGRAFIA DE SUBSTITUIÇÃO POLIALFABÉTICA

No final do século XVI, surgem as cifras de substituição polialfabéticas, que consistem no uso de dois ou mais alfabetos cifrados, usados alternadamente. Sua versão final ficou conhecida como quadrado de Vigenère, veja figura:

Figura 4: Quadrado de Vigenère

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

Fonte: Singh, Simon (2021, p 66)

(SINGH, 2001) (p 70), destaca que apesar da qualidade deste sistema, ele não recebeu a devida atenção por mais de 200 anos.

## 2.8 CHAVES SIMÉTRICAS E ASSIMÉTRICAS

Outras alternativas foram desenvolvidas ao longo da era clássica e em parte da era moderna, todas apresentavam algumas características em comum, entre elas destaca-se o fato de que a chave para codificar a mensagem era a mesma para sua decifração, esta característica é denominada Cifra de Chave Simétrica.

Neste caso, o algoritmo pode até ser de conhecimento público mas as chaves devem permanecer secretas, ou seja, se o inimigo, ao conseguir capturar a mensagem, souber o algoritmo usado na criptografia, mas não conhecer a chave (o alfabeto cifrado), ele não conseguirá decifrá-la ou terá grande dificuldade para fazê-la.

Durante muito tempo defendeu-se a ideia de criptografia com algoritmo público e chave privada. Em 1883, o linguista holandês Auguste Kerckhoff postulou o princípio que leva o seu nome:

**Definição 2.1.** *A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave.*

Na verdade, o sigilo transmitia, muitas vezes, uma falsa impressão de segurança. Uma técnica fraca, ao ser guardada em segredo, poderia parecer forte, mas permitiria que outras pessoas decifrassem os textos sem dificuldade, sem o conhecimento dos interessados. Segundo (PAAR; PELZL, 2009), o que não pode ser testado por outros criptógrafos ou criptoanalistas, não possui garantias de segurança.

Segundo (KAHN, 1996), somente em 1976, um estudante de graduação chamado Martin Hellman apresentou um conceito revolucionário, o das chaves assimétricas. Nesta técnica há duas chaves, uma pública para criptografia do texto e uma privada para sua decodificação. Este avanço proporcionou grandes avanços, inclusive a autenticação através de máquinas elétricas e maior facilidade na comunicação e/ou em sua utilização, visto que qualquer um poderia enviar uma mensagem criptografada ao destinatário, e somente quem possuia a chave privada poderia decodificar o texto.

# 3

# CIFRA DE HILL

No capítulo anterior foi apresentado um breve panorama histórico da criptografia, principalmente em seu período clássico. O presente capítulo será dedicado ao estudo da Cifra de Hill, um método desenvolvido na era moderna, cujos conteúdos matemáticos merecem destaque no presente estudo.

Esta técnica foi apresentada em 1929, por Lester S. Hill no artigo intitulado "Cryptography in an Algebraic Alphabet" (HILL, 1929) com continuação publicada em 1931, no artigo "Concerning Certain Linear Transformation Apparatus of Cryptography" (HILL, 1931).

Segundo (KAHN, 1996), Lester S. Hill (1890-1961), quando publicou o artigo, aos 38 anos, era professor assistente de matemática no Hunter College em Nova York, sua técnica é pioneira na aplicação de álgebra abstrata na criptografia e (DOOLEY, 2018), o considera como um dos três gigantes da criptografia moderna do século XX.

Como verificado anteriormente, a maior fragilidade da criptografia de substituição monoalfabética está na facilidade de identificação das letras através do estudo de frequência das mesmas. (ANTON; RORRES, 2001) afirma que, uma forma de reduzir essa fraqueza é desenvolver métodos que codifiquem grupos de letras ao invés de cada letra separadamente. Denomina-se sistema digráfico, sistema cujo agrupamento das letras para codificação é feito dois a dois, trigráfico, três a três e poligráfico, n a n, para qualquer $n \in \mathbb{Z}, n > 1$.

> Um sistema poligráfico é um sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas.(ANTON; RORRES, 2001)(p. 655)

A Cifra de Hill é um sistema poligráfico baseado em matrizes quadradas contendo $n$ linhas e $n$ colunas. E justamente este $n$ define a quantidade de elementos de cada grupo deste sistema.

## 3.1 FUNDAMENTAÇÃO MATEMÁTICA

Esta seção será dedicada à fundamentação matemática para a Cifra de Hill.

A Cifra de Hill utiliza, em todo seu algoritmo, valores de 0 a 25, correspondentes as 26 letras do alfabeto, ou seja, as operações matriciais ocorrem dentro do conjunto $\mathbb{Z}_{26}$.

Para o estudo dos fundamentos matemáticos, percorre-se o seguinte caminho: Partindo do algoritmo da divisão e da definição de congruência, serão apresentadas algumas propriedades básicas das estruturas de anel bem como os teoremas que delas derivam, com atenção especial ao anel $\mathbb{Z}_{26}$. Após a apresentação dos elementos de $\mathbb{Z}_{26}$, serão definidas as operações de soma e produto neste conjunto para posterior estudo de estrutura de domínio de integridade e corpo. Em seguida, serão apresentados os elementos invertíveis e inversos em $\mathbb{Z}_m$ e $\mathbb{Z}_{26}$, para, finalmente, apresentar as matrizes inversíveis e inversas neste conjunto.

As definições aqui apresentadas estão disponíveis nos livros:

- Números, Uma Introdução à Matemática, César Polcino Milies e Sônia Pitta Coelho, (MILIES; COELHO, 2001)
- Introdução à Álgebra, Adilson Gonçalves. (GONÇALVES, 1979)
- Álgebra Linear com Aplicações, Howard Anton e Chris Rorres (ANTON; RORRES, 2001)

**Lema 3.1.** *Sejam $a$ e $b$ inteiros, tais que $a \geq 0$ e $b > 0$, então, existem q e r, tais que a = bq + r e $0 \leq r < b$.*

*Demonstração.* Consideremos o seguinte conjunto S = $\{a - bx \,|\, x \in \mathbb{Z}, a - bx \geq 0\}$.
Quando x = 0, temos que a - bx = a $\geq$ 0 é um elemento de S, logo, S é um conjunto não vazio.
Pelo Princípio da Boa Ordem, existe r = min S. Como r $\in$ S, ele também é da forma r = a - bq $\geq$ 0, para algum q $\in \mathbb{Z}$.
Para mostrar que as condições do enunciado estão verificadas, bastará provar que r < b. De fato, se fosse r $\geq$ b, teríamos: a - b (q+1) = a - bq- b = r- b > 0,
logo, a - b(q+1) também pertenceria a S. Mas a - b (q + 1) = r - b < r = min S, uma contradição. □

**Teorema 3.2** (Algoritmo da Divisão de Euclides)**.** *Sejam $a$ e $b$ inteiros, com $b \neq 0$. Então, existem inteiros $q$ e $r$, únicos, tais que $a = bq + r$ e $0 \leq r < |b|$, ou seja, o resto $r$, da divisão de $a$ por $b$ é um inteiro pertencente ao conjunto $\{0, 1, 2, 3, ..., b - 1\}$.*

*Demonstração.* Mostraremos que podemos determinar $q$ e $r$ para os seguintes casos:

CASO 1: b > 0

$a \geq 0$: Está garantido pelo Lema 3.1.

$a < 0$: Ainda pelo Lema 3.1 pode-se determinar q' e r' tais que |a| = bq' + r' e $0 \leq b$ Se r'= 0, temos -|a| = a = b (-q' ) + 0, e o par q = q', r = 0 verifica as condições do teorema.

Se r' > 0, temos

a= -|a| = b(-q) - r'= b.(-q') - b + b - r' = b.(-q - 1) + (b - r').

Obviamente, 0 < b - r' < b, logo, os inteiros q = -q' - 1 e r = b - r' verificam as condições do enunciado.

CASO 2: b < 0 Qualquer que seja a, pela parte anterior, podemos determinar q' e r' tais que a = |b| q' + r' e 0 $\leq$ r' $<$ |b|.

Quando b < 0, temos que |b|= - b, logo, a = |b|q' + r' = (-b)q' + r' = b(-q') + r', e os inteiros q = -q e r = r' estão nas condições do enunciado.

UNICIDADE: Provaremos que, se (q, r) e (q', r') são dois pares de inteiros verificando as condições do enunciado, então q = q', e r = r'.

De fato, temos que

qb + r = a = q'b + r' $\quad (I)$.

Podemos supor, por exemplo, que $r' \geq r$.

Da igualdade acima, temos

(q - q')b = r' - r. Como | b | > r' também temos r'- r < |b|.

Substituindo, ( q - q' )b < |b| e, tomando módulos, 0 $\leq$ |q - q'| |b| < |b|.

Como | b | > 0, podemos cancelar e obtemos 0 $\leq$ |q - q'| < 1, e portanto,

|q - q'| = 0, isto é, q = q'.

Na igualdade $(I)$, temos agora qb+ r = qb + r'.

Cancelando, segue que r = r'.

□

O algoritmo da divisão afirma que dados inteiros a, m, existem inteiros únicos $q$, $r$, tais que $a = mq + r$. Onde $r$ é o resto da divisão $a$ por $m$, e esse resto pertence ao conjunto de inteiros $\{0, 1, 2, ....m - 1\}$ De $a = mq + r$, tem- se que : $a - r = mq$, isto é o número $a - r$ é um múltiplo de $m$.

**Exemplo 3.3.** *Sejam* $a = 67$ *e* $m = 26$*, pelo algoritmo da divisão, existem* $q$ *e* $r$ *inteiros únicos, com* $0 \leq r < |26|$*, tais que* $67 = 26q + r$*.*
*De fato,*
$67 = 26(2) + 15$*.*
*Segue que:* $67 - 15 = 26(2)$*, ou seja,* $67 - 15$ *é um múltiplo de* $26$*.*

**Definição 3.4.** *Seja* $m \neq 0$ *um inteiro fixo e dois inteiros* $a$ *e* $b$ *quaisquer, dizemos que* $a$ *é congruente a* $b$ *módulo* $m$*, e escrevemos:*

$$a \equiv b \ (mod\ m) \text{ se m divide a diferença } (a - b).$$

Vale ressaltar que, para os fins do presente estudo, será considerado sempre $m > 1$.

Dado um $m$ fixo, podemos relacionar qualquer número $a$ fora do conjunto $\{0, 1, 2, ....m - 1\}$ com um inteiro $r$ dentro deste conjunto. Posto isto, $a$ está relacionado com $r$ quando $a$ dividido por $m$ deixa resto $r$, e dizemos que $a$ é congruente com $r$ modulo $m$. Outra forma de dizer, é que, dados dois números $a$, $r$, eles são congruentes modulo $m$ se $a - r$ é um múltiplo de $m$.

**Exemplo 3.5.** *Tomando* $a = 212$ *e* $m = 26$*:*
$212 = 26.8 + 4$*, tem-se que* $212 - 4$ *é múltiplo de* $26$*, e portanto,* $212 \equiv 4(mod\ 26)$

Para o caso de números inteiros negativos, (SINKOV, 1966) apresenta a seguinte solução:

Seja $a$ um número inteiro negativo, tome o positivo $-a$:
$-a = q.m + r$ com $0 \leq r < |m|$
$-a = q.m + m - m + r$
$-a = m.(q + 1) - (m - r)$
$a = -(q + 1)m + (m - r)$ com $0 \leq m - r < |m|$
$a \equiv (m - r)(mod\ m)$ pois $a - (m - r)$ é múltiplo de m com $(m - r) \in \{0, 1, 2, ....m - 1\}$

Portanto para $a$ um inteiro negativo, basta calcular o resto r que deixa $-a$ quando dividido por m, desta forma, $a$ será congruente a $m - r$ módulo $m$.
Veja o exemplo à seguir:

**Exemplo 3.6.** *Sejam* $a = -58$ *e* $m = 26$*:*
*Calcula-se o resto da divisão de* $58$ *por* $26$*:*
$58 = 2.26 + 6$
*O valor procurado é* $m - r = 26 - 6 = 20$
*Logo,*
$-58 \equiv 20(mod\ 26)$

O próximo passo é estudar classes de congruência:

**Definição 3.7.** *Seja* $a$ *um inteiro. Chama-se* $classe\ de\ congruência$ *de* $a$ *módulo* $m$ *o conjunto formado por todos os inteiros que são congruentes a* $a$ *módulo m. Denotaremos esse conjunto por* $\overline{a}$*. Temos, então,*

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\ (mod\ m)\}$$

*Como* $x \equiv a\ (mod\ m)$*, se e somente se,* $x$ *é da forma* $x = a + tm$*, para algum* $t \in \mathbb{Z}$*, também podemos escrever*

$$\overline{a} = \{a + tm \mid t \in \mathbb{Z}\}$$

A seguir, será apresentado que a relação de congruência entre números se traduz em igualdade no sentido estrito entre classes.

**Proposição 3.8.** *Sejam* $a$ *e* $b$ *inteiros. Então* $a \equiv b \ (mod\ m)$*, se e somente se,* $\overline{a} = \overline{b}$*.*

*Demonstração:* Suponha que $a \equiv b \ (mod\ m)$, deseja-se provar que $\overline{a} = \overline{b}$, isto é, uma igualdade entre conjuntos.
Dado $x \in \overline{a}$, tem-se, por definição que $x \equiv a \ (mod\ m)$.
Da propriedade transitiva de congruência
$a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m) \implies a \equiv c \ (mod\ m)$, e da hipótese, seguem imediatamente que $x \in \overline{b}$. Logo, $\overline{a} \subset \overline{b}$.
A inclusão de sentido contrário segue de forma análoga.
Reciprocamente, se $\overline{a} = \overline{b}$, como $a \in \overline{a}$, tem-se também que $a \in \overline{b}$, logo, $a \equiv b \ (mod\ m)$.
□

Denota-se pelo símbolo $\mathbb{Z}_m$ o conjunto das classes de congruências módulo $m$ e lê-se como conjunto dos inteiros módulo $m$.

> Sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m são os números 0, 1, ..., m-1, sem repetições e nenhuma ordem qualquer.Portanto, um sistema completo de resíduos módulo m possui m elementos.
> É claro que se $a_1, a_2, ..., a_m$ são m números inteiros, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos $a_i$ por m são dois a dois distintos, o que implica que são números 0,1,...,m-1 em alguma ordem.
> Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m. (HEFEZ, 2013)(p. 167)

Em geral, se $\{\overline{a_1}, \overline{a_2}, \overline{a_3}, ..., \overline{a_m}\}$ é um sistema completo de resíduos módulo $m$, então:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, ..., \overline{m-1}\}$$

**Exemplo 3.9.** *Para* $m = 26$*:*

$$\mathbb{Z}_{26} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}, \overline{23}, \overline{24}, \overline{25}\}$$

À seguir serão introduzidas as operações de soma, produto em $\mathbb{Z}_m$ e suas propriedades:

**Definição 3.10.** *Define-se soma e produto em $\mathbb{Z}_m$ por*

$$\overline{a} + \overline{b} \;=\; \overline{a \;+\; b}$$

$$\overline{a} \;.\; \overline{b} \;=\; \overline{a.b}$$

**Exemplo 3.11.** *Para somar e multiplicar $\overline{18}$ e $\overline{10}$ em $\mathbb{Z}_{26}$ tem-se:*

$$\overline{18} + \overline{10} = \overline{28} = \overline{2}$$

$$\overline{18} \;.\; \overline{10} = \overline{180} = \overline{24}$$

Ou seja, para efetuar a soma de duas classes módulo m, tomam-se representantes (quaisquer) a e b dessas classes, efetua-se a soma a + b em $\mathbb{Z}$ considerando como resultado da soma a classe de a + b módulo m.

Com soma e produto definidos, verifica-se que o conjunto $\mathbb{Z}_m$ satisfaz as seguintes propriedades que, como será visto em breve, caracterizam um conjunto com estrutura de anel.

Tabela 3: Propriedades de $\mathbb{Z}_n$

| **Propriedades dos inteiros módulo n** | **Soma** $\forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ | **Produto** $\forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ |
|---|---|---|
| Fechamento | $\overline{a}, \overline{b} \in \mathbb{Z}_n \implies \overline{a} + \overline{b} \in \mathbb{Z}_n$ | $\overline{a}, \overline{b} \in \mathbb{Z}_n \implies \overline{a}.\overline{b} \in \mathbb{Z}_n$ |
| Associatividade | $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ | $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$ |
| Elemento neutro | $\exists\, \overline{0} \in \mathbb{Z}_n \;/\; \overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$ | |
| Comutatividade | $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ | |
| Oposto Aditivo | $\forall\, \overline{a} \in \mathbb{Z}_n,\ \exists\, \overline{b} \in \mathbb{Z}_n$ único, denotado por $\overline{b} = (-\overline{a})$ tal que: $\overline{a} + (-\overline{a}) = (-\overline{a}) + \overline{a} = \overline{0}$ | |
| Distributiva à esquerda e à direita | $\overline{a}.(\overline{b} + \overline{c}) = \overline{a}.\overline{b} + \overline{a}.\overline{c}$ | $(\overline{b} + \overline{c}).\overline{a} = \overline{b}.\overline{a} + \overline{c}.\overline{a}$ |

Fonte: Atividade - (GPE-FEMIC, )

**Definição 3.12.** *Dizemos que um conjunto não vazio A, tem uma estrutura de anel se nele podem ser definidas duas operações "+" e ".", tais que:*

*i.* $a, b \in A \implies a + b \in A$

*ii.* $a + b = b + a,$ *para* $a, b \in A$

*iii.* $(a+b)+c = a+(b+c),$ *para* $a,b,c \in A$

*iv.* $\exists\ 0 \in A$ *tal que* $a+0=a,\ \forall\ a \in A.$

*v.* $Dado\ a \in A, \exists\ b \in A$ *tal que* $a+b=0$ *(b será denotado por -a)*

*vi.* $a,b \in A \implies a.b \in A$

*vii.* $(a.b).c = a.(b.c),$ *para* $a,b,c \in A$

*viii.* $a.(b+c) = a.b + a.c$ *e* $(b+c).a = b.a + c.a,$ *para* $a,b,c \in A$

Anéis podem ser caracterizados de acordo com suas propriedades.

**Definição 3.13.** $A,+,.$ *é um domínio de integridade se é um anel comutativo, com unidade e sem divisores de zero, ou seja, se possui as três propriedades descritas abaixo:*

1. $\exists 1\ \in A,\ 0 \neq 1,$ *tal que* $x.1 = 1.x = \forall\ x\ \in A$ *(unidade).*
2. $\forall\ x,y \in A,\ x.y = y.x,$ *(comutatividade)*
3. $x,y \in A,\ x.y = 0 \implies x = 0\ ou\ y = 0$ *(sem divisores de zero)*

Finalmente, se um domínio de integridade $A,+,.$ satisfaz a propriedade:

$$\forall\ x \in A,\ x \neq 0,\ \exists\ y \in A \text{ tal que } x.y = y.x = 1$$

então $A,+,.$ é um corpo.

Voltando ao conjunto de classes de equivalencia em $\mathbb{Z}_m$, estamos em condições de responder à pergunta, $\mathbb{Z}_{26}$ é um domínio de integridade ou um corpo? Com um exemplo simples podemos vislumbrar uma possível resposta:

**Exemplo 3.14.** *Considere o conjunto de classes de equivalência* $\mathbb{Z}_4$*.*

Tabela 4: Multiplicação $\mathbb{Z}_4$

| . | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}.\overline{0} = \overline{0}$ | $\overline{0}.\overline{1} = \overline{0}$ | $\overline{0}.\overline{2} = \overline{0}$ | $\overline{0}.\overline{3} = \overline{0}$ |
| $\overline{1}$ | $\overline{1}.\overline{0} = \overline{0}$ | $\overline{1}.\overline{1} = \overline{1}$ | $\overline{1}.\overline{2} = \overline{2}$ | $\overline{1}.\overline{3} = \overline{3}$ |
| $\overline{2}$ | $\overline{2}.\overline{0} = \overline{0}$ | $\overline{2}.\overline{1} = \overline{2}$ | $\overline{2}.\overline{2} = \overline{0}$ | $\overline{2}.\overline{3} = \overline{2}$ |
| $\overline{3}$ | $\overline{3}.\overline{0} = \overline{0}$ | $\overline{3}.\overline{1} = \overline{3}$ | $\overline{3}.\overline{2} = \overline{2}$ | $\overline{3}.\overline{3} = \overline{1}$ |

Fonte: a própria autora

*Note que $\overline{2}.\overline{2} = \overline{0}$ porém $\overline{2} \neq \overline{0}$, então $\mathbb{Z}_4$ não satisfaz a propriedade de anel sem divisores de zero, e portanto não é um dominio de integridade.*

Além disso $\overline{2}$ não possui inverso em $\mathbb{Z}_4$, ou seja, não existe uma classe em $\mathbb{Z}_4$ que se multiplicada por $\overline{2}$ resulte em $\overline{1}$.

Por outro lado, observe a seguir, o conjunto de classes de equivalência $\mathbb{Z}_3$.

**Exemplo 3.15.** *Considere o conjunto de classes de equivalência $\mathbb{Z}_3$.*

Tabela 5: Multiplicação $\mathbb{Z}_3$

| . | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
|---|---|---|---|
| $\overline{0}$ | $\overline{0}.\overline{0} = \overline{0}$ | $\overline{0}.\overline{1} = \overline{0}$ | $\overline{0}.\overline{2} = \overline{0}$ |
| $\overline{1}$ | $\overline{1}.\overline{0} = \overline{0}$ | $\overline{1}.\overline{1} = \overline{1}$ | $\overline{1}.\overline{2} = \overline{2}$ |
| $\overline{2}$ | $\overline{2}.\overline{0} = \overline{0}$ | $\overline{2}.\overline{1} = \overline{2}$ | $\overline{2}.\overline{2} = \overline{1}$ |

Fonte: a própria autora

*Em $\mathbb{Z}_3$, não existem divisores de zero, ou seja, se:*

$$\overline{a}.\overline{b} = \overline{0} \implies \overline{a} = \overline{0}\ ou\ \overline{b} = \overline{0}$$

*Observe também que todos os seus elementos,com exceção dos pertencentes à classe do zero, possuem inverso:*

$\overline{1}.\overline{1} = \overline{1}$

$\overline{2}.\overline{2} = \overline{4} = \overline{1}$

*Logo, $\mathbb{Z}_3$ além de ser um domínio de integridade também é um corpo.*

À seguir, o teorema de Bézout será enunciado, pois ele se faz necessário no teorema seguinte, porém o presente estudo não apresentará sua demonstração.

**Teorema 3.16** (Teorema de Bézout)**.** *Sejam a, b inteiros e d = mdc (a,b). Então, existem inteiros r e s tais que d = ra + sb.*

O teorema a seguir fornece as condições para verificar se $\mathbb{Z}_m$ é um corpo.

**Teorema 3.17.** *O anel $\mathbb{Z}_p$ é um corpo, se e somente se, $p$ é primo.*

*Demonstração:* $\mathbb{Z}_p \text{ é } corpo \Longrightarrow p \text{ é } primo$

Considere por absurdo que p não seja primo, isto é,

$\exists\ a, b,\ \ 1 < a, b < p,$ tal que $p = a.b$, então

$\overline{p} = \overline{a.b} = \overline{a}.\overline{b}$,

mas $\overline{p} = \overline{0} = \overline{a}.\overline{b}$

ou seja, $\mathbb{Z}_p$ é um anel com divisores de zero pois, $\overline{a}.\overline{b} = \overline{0},\ \overline{a} \neq 0$ e $\overline{b} \neq \overline{0}$, isto significa que $\mathbb{Z}_p$ não é um domínio de integridade e, portanto, não é um corpo, o que é uma contradição.

$p \text{ é } primo \Longrightarrow \mathbb{Z}_p \text{ é } corpo$

Seja p um primo, para provar que $\mathbb{Z}_p$ é um corpo, basta mostrar que $\mathbb{Z}_p$ é um anel comutativo, com unidade, sem divisores de zero e que todos seus elementos possuem inverso multiplicativo.

De fato:

- anel com unidade:

  $\forall\ \overline{x} \in \mathbb{Z}_p$

  $\overline{x}.\overline{1} = \overline{x.1} = \overline{x}$

  $\overline{1}.\overline{x} = \overline{1.x} = \overline{x}$

- anel comutativo: $\forall\ \overline{x}, \overline{y} \in \mathbb{Z}_p$

  $\overline{x}.\overline{y} = \overline{x.y} = \overline{y.x} = \overline{y}.\overline{x}$ (pela comutatividade dos inteiros)

- anel sem divisores de zero: $\overline{a}.\overline{b} = \overline{0} \implies \overline{a.b} = \overline{0} \implies ab \equiv 0(mod\ p)$, ou seja, $p|ab$, como p é primo, $p|a$ ou $p|b$, ou seja,

  $a \equiv 0(mod\ p)$ ou $b \equiv 0(mod\ p)$

  Portanto, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

- Todo elemento em $\mathbb{Z}_p$ possui inverso multiplicativo:
  Seja $\overline{x} \in \mathbb{Z}_p$, como p é primo e x está entre 1 e p ($1 \leq x < p$ ), mdc(p, x) = 1
  Pelo Teorema de Bézout,
  1 = ps + xr
  como $\overline{p} = \overline{0}$:
  $\overline{1} = \overline{0} + \overline{xr}$
  $\overline{1} = \overline{xr}$
  Portanto, todo elemento de $\mathbb{Z}_p$ possui inverso multiplicativo.

□

Do teorema anterior pode-se concluir que $\mathbb{Z}_{26}$ não é um corpo, pois 26 não é um número primo, e portanto, nem todos os seus elementos possuem inverso.

De fato, elementos como $\overline{2}, \overline{4}, \overline{6}$ não possuem inverso em $\mathbb{Z}_{26}$, enquanto $\overline{1}, \overline{3}, ...$ possuem.

O resultado a seguir permite encontrar todos os elementos inversíveis em $\mathbb{Z}_{26}$.

**Definição 3.18.** *Um elemento $\overline{x} \in \mathbb{Z}_m$ diz-se inversível se existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x}.\overline{y} = \overline{y}.\overline{x} = 1$. Um elemento $\overline{y}$ diz-se inverso de $\overline{x}$.*

**Proposição 3.19.** *Seja $\overline{a}$ um elemento não nulo de $\mathbb{Z}_m$, então, $\overline{a}$ é inversível se, e somente se, mdc(a,m) = 1.*

*Demonstração:* Suponhamos que mdc (a,m) = 1. O Teorema de Bézout, garante que existem inteiros r e s tais que ar + ms= 1.

Tomando classes segue que:

$\overline{1} = \overline{ar + ms} = \overline{ar} + \overline{ms} = \overline{ar} + \overline{ms} = \overline{ar} + \overline{0}\overline{s} = \overline{ar}$.

Logo, $\overline{r}$ é o inverso de $\overline{a}$.

Reciprocamente, se mdc (a,m) $\neq$ 1, então ã é divisor de zero e existe $\overline{b} \neq 0$ tal que $\overline{a}\overline{b} = 0$. Mostraremos que, nesse caso, $\overline{a}$ não pode ser inversível. Com efeito,

suponhamos que existe $\overline{a'}$ tal que $\overline{aa'} = \overline{1}$. Teríamos, então,
$\overline{b} = \overline{b}.\overline{1} = \overline{b}(\overline{aa'}) = (\overline{a}\overline{b}).\overline{a'} = \overline{0}.\overline{a'} = \overline{0}$, uma contradição.

□

Desta forma, os elementos inversíveis em $\mathbb{Z}_{26}$ são:

$$\overline{1}, \overline{3},\ \overline{5},\ \overline{7},\ \overline{9},\ \overline{11},\ \overline{15},\ \overline{17},\ \overline{21},\ \overline{23},\ \overline{25}$$

pois mdc(1,26) = mdc(3,26) = mdc(5,26) = ... = mdc(25,26) = 1.

Com esses resultados, é possivel apresentar os conceitos de matrizes inversíveis e inversas em $\mathbb{Z}_m$:

**Definição 3.20.** *Seja A uma matriz 2x2 com entradas em $\mathbb{Z}_m$, dizemos que A é inversível se existe uma matriz B com entrada em $\mathbb{Z}_m$ tal que*

*AB = BA = $I$, onde* $I = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$

**Teorema 3.21.** *Seja A uma matriz 2x2 com entradas em $\mathbb{Z}_m$. A é inversível se, e somente se, det(A) é inversível em $\mathbb{Z}_m$.*

*Demonstração:* Seja $A = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$

A é inversível $\Longrightarrow$ det(A) é inversível em $\mathbb{Z}_m$:
Se A é inversível então existe B com entradas em $\mathbb{Z}_m$ tal que
AB = BA = $I$, logo, det(AB) = det(A). det(B) = det($I$) = $\overline{1}$, ou seja, det(A) é inversível em $\mathbb{Z}_m$ ( ou det(B) é o inverso de det(A)).

det(A) é inversível em $\mathbb{Z}_m \Longrightarrow$ A é inversível:
Se det(A) = $\overline{x}$ é inversível, segue que existe $\overline{y} \in \mathbb{Z}_m$ tal que det(A). $\overline{y} = \overline{1}$.

Agora tomando $B = \overline{y} \begin{bmatrix} \overline{d} & \overline{-b} \\ \overline{-c} & \overline{a} \end{bmatrix}$, obtemos:

$$AB = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} .\overline{y}. \begin{bmatrix} \overline{d} & \overline{-b} \\ \overline{-c} & \overline{a} \end{bmatrix} = \overline{y}. \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} . \begin{bmatrix} \overline{d} & \overline{-b} \\ \overline{-c} & \overline{a} \end{bmatrix} = \overline{y}. \begin{bmatrix} \overline{a}\overline{d} - \overline{b}\overline{c} & -\overline{a}\overline{b} + \overline{b}\overline{a} \\ \overline{c}\overline{d} - \overline{d}\overline{c} & -\overline{c}\overline{d} + \overline{d}\overline{a} \end{bmatrix} =$$

$$= \overline{y}. \begin{bmatrix} det(A) & 0 \\ 0 & det(A) \end{bmatrix} = \begin{bmatrix} \overline{y}.det(A) & \overline{0} \\ \overline{0} & \overline{y}.det(A) \end{bmatrix} = \begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{bmatrix}$$

Portanto, A é uma matriz inversível. □

A seguir, baseado na explanação existente no livro de (ANTON; RORRES, 2001), nas páginas 654 à 663, serão apresentados os algoritmos para criptografia e descriptografia conforme a técnica acima citada.

## 3.2 O ALGORITMO

Como mencionado anteriormente, Cifra de Hill utiliza como chave, uma matriz nxn. Para exemplificar a técnica optou-se por uma matriz de ordem 2, formando assim, um sistema digráfico.

### 3.2.1 *Algoritmo de Codificação*

Inicialmente, serão descritas as etapas para execução da criptografia e posteriormente, o conceito será aplicado em um exemplo.

1. O primeiro passo é agrupar o texto em pares de letras. No caso de quantidade ímpar de letras, é necessário acrescentar uma letra qualquer ao final do texto, para formar o último par.

2. O segundo passo é uma substituição simples de cada letra do texto pelo seu correspondente numérico, conforme tabela:

Tabela 6: Cifra de Hill: Etapa de Substituição

| 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 | 0 |

Fonte: a própria autora

3. Agora basta escolher uma matriz A, de ordem 2, inversível em $\mathbb{Z}_{26}$, que servirá de chave para codificação.

4. Transforme cada par de números, formados na segunda etapa, em uma matriz coluna, ou seja, uma matriz 2x1.

5. Efetue as multiplicações matriciais entre a matriz A, formada na etapa 3, e cada par da etapa anterior.

6. Verifique se todos os valores obtidos são números inteiros não negativos menores do que 26. Caso algum não seja, obtenha seu equivalente mod 26.

7. Finalmente, basta converter os números em letras utilizando a mesma tabela da primeira etapa.

Para exemplificação, será codificada a frase:

C I F R A D E H I L L N O P R O F M A T

Fazendo a separação por pares de letras, tem-se:

CI FR AD EH IL LN OP RO FM AT

Observe que neste caso não foi necessária a inserção de uma letra ao final, por conter vinte letras. O passo seguinte é efetuar a substituição de cada letra por seu número 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 |

Fonte: a própria autora

Resultando em:

| C | I | F | R | A | D | E | H | I | L | L | N | O | P | R | O | F | M | A | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 9 | 6 | 18 | 1 | 4 | 5 | 8 | 9 | 12 | 12 | 14 | 15 | 16 | 18 | 15 | 6 | 13 | 1 | 20 |

Fonte: a própria autora

Para a escolha da matriz A, 2x2, inversível em $\mathbb{Z}_{26}$, basta tomar uma matriz cujo valor do determinante seja inversível em $\mathbb{Z}_{26}$, ou seja, a determinante precisa pertencer à uma das classes do conjunto $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{15}, \overline{17}, \overline{21}, \overline{23}, \overline{25}\}$.

Neste exemplo, usar-se-á a seguinte matriz:

$$A = \begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix}$$

Efetuando as multiplicações matriciais tem-se:

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 3 \\ 9 \end{bmatrix} = \begin{bmatrix} 2.3 + 3.9 \\ 5.3 + 10.9 \end{bmatrix} = \begin{bmatrix} 6 + 27 \\ 15 + 90 \end{bmatrix} = \begin{bmatrix} 33 \\ 105 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 6 \\ 18 \end{bmatrix} = \begin{bmatrix} 2.6 + 3.18 \\ 5.6 + 10.18 \end{bmatrix} = \begin{bmatrix} 12 + 54 \\ 30 + 180 \end{bmatrix} = \begin{bmatrix} 66 \\ 210 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 2.1 + 3.4 \\ 5.1 + 10.4 \end{bmatrix} = \begin{bmatrix} 2 + 12 \\ 5 + 40 \end{bmatrix} = \begin{bmatrix} 14 \\ 45 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 5 \\ 8 \end{bmatrix} = \begin{bmatrix} 2.5 + 3.8 \\ 5.5 + 10.8 \end{bmatrix} = \begin{bmatrix} 10 + 24 \\ 25 + 80 \end{bmatrix} = \begin{bmatrix} 34 \\ 105 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 9 \\ 12 \end{bmatrix} = \begin{bmatrix} 2.9 + 3.12 \\ 5.9 + 10.12 \end{bmatrix} = \begin{bmatrix} 18 + 36 \\ 45 + 120 \end{bmatrix} = \begin{bmatrix} 54 \\ 165 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} 2.12 + 3.14 \\ 5.12 + 10.14 \end{bmatrix} = \begin{bmatrix} 24 + 42 \\ 60 + 140 \end{bmatrix} = \begin{bmatrix} 66 \\ 200 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 2.15 + 3.16 \\ 5.15 + 10.16 \end{bmatrix} = \begin{bmatrix} 30 + 48 \\ 75 + 160 \end{bmatrix} = \begin{bmatrix} 78 \\ 235 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 18 \\ 15 \end{bmatrix} = \begin{bmatrix} 2.18 + 3.15 \\ 5.18 + 10.15 \end{bmatrix} = \begin{bmatrix} 36 + 45 \\ 90 + 150 \end{bmatrix} = \begin{bmatrix} 81 \\ 240 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 6 \\ 13 \end{bmatrix} = \begin{bmatrix} 2.6 + 3.13 \\ 5.6 + 10.13 \end{bmatrix} = \begin{bmatrix} 12 + 39 \\ 30 + 130 \end{bmatrix} = \begin{bmatrix} 51 \\ 160 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix} . \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 2.1 + 3.20 \\ 5.1 + 10.20 \end{bmatrix} = \begin{bmatrix} 2 + 60 \\ 5 + 200 \end{bmatrix} = \begin{bmatrix} 62 \\ 205 \end{bmatrix}$$

Obtendo os seguintes resultados numéricos:

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 33 | 105 | 66 | 210 | 14 | 45 | 34 | 105 | 54 | 165 | 66 | 200 | 78 | 235 | 81 | 240 | 51 | 160 | 62 | 205 |

Fonte: a própria autora

Como todos os valores devem inteiros não negativos menores do que 26, é necessário tomar os respectivos restos das divisões por 26:

$$33 \equiv 7 \ (mod\ 26)$$

$$105 \equiv 1 \ (mod\ 26)$$

$$66 \equiv 14 \ (mod\ 26)$$

$$210 \equiv 2 \ (mod\ 26)$$

$$14 \equiv 14 \ (mod\ 26)$$

$$45 \equiv 19 \ (mod\ 26)$$

$$34 \equiv 8 \ (mod\ 26)$$

$$105 \equiv 1 \ (mod\ 26)$$

$$54 \equiv 2 \ (mod\ 26)$$

$$165 \equiv 9 \ (mod\ 26)$$

$$66 \equiv 14 \ (mod\ 26)$$

$$200 \equiv 18 \ (mod\ 26)$$

$$78 \equiv 0 \ (mod\ 26)$$

$$235 \equiv 1 \ (mod\ 26)$$

$$81 \equiv 3 \ (mod\ 26)$$

$$240 \equiv 6 \ (mod\ 26)$$

$$51 \equiv 25 \ (mod\ 26)$$

$$160 \equiv 4 \ (mod\ 26)$$

$$62 \equiv 10 \ (mod\ 26)$$

$$205 \equiv 23 \ (mod\ 26)$$

Resultando em:

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 1 | 14 | 2 | 14 | 19 | 8 | 1 | 2 | 9 | 14 | 18 | 0 | 1 | 3 | 6 | 25 | 4 | 10 | 23 |

Fonte: a própria autora

Para finalizar basta substituir os números pelas letras conforme tabela:

| 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 | 0 |

Fonte: a própria autora

| 7 | 1 | 14 | 2 | 14 | 19 | 8 | 1 | 2 | 9 | 14 | 18 | 0 | 1 | 3 | 6 | 25 | 4 | 10 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G | A | N | B | N | S | H | A | B | I | N | R | Z | A | C | F | Y | D | J | W |

Fonte: a própria autora

Neste caso, a forma cifrada de ”CIFRA DE HILL NO PROFMAT” é ”GANBNSHABINRZACFYDJW

Analisando os resultados:

| Sem codificação | C | I | F | R | A | D | E | H | I | L | L | N | O | P | R | O | F | M | A | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Texto Cifrado | G | A | N | B | N | S | H | A | B | I | N | R | Z | A | C | F | Y | D | J | W |

Fonte: a própria autora

Observe que letras iguais existentes no texto normal, resultam em letras diferentes na forma cifrada, além de não manterem a mesma frequência, pois o resultado vai depender de sua posição na matriz 2x1 e do valor do outro elemento da mesma matriz.

### 3.2.2 *Algoritmo de Decodificação*

Para decodificação seguem-se as mesmas etapas descritas anteriormente, com exceção do fato de a matriz 2x2 a ser adotada ser a matriz inversa em $\mathbb{Z}_{26}$ da matriz de codificação.

Para exemplificação, será decifrada a frase: "GANBNSHABINRZACFYDJW"

| G | A | N | B | N | S | H | A | B | I | N | R | Z | A | C | F | Y | D | J | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Fonte: a própria autora

| 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 | 0 |

Fonte: a própria autora

| G | A | N | B | N | S | H | A | B | I | N | R | Z | A | C | F | Y | D | J | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 1 | 14 | 2 | 14 | 19 | 8 | 1 | 2 | 9 | 14 | 18 | 0 | 1 | 3 | 6 | 25 | 4 | 10 | 23 |

Fonte: a própria autora

Dada a matriz de codificação A:

$$A = \begin{bmatrix} 2 & 3 \\ 5 & 10 \end{bmatrix}$$

A matriz para decodificação é inversa de A:

$$A^{-1} = (2.10 - 3.5)^{-1}. \begin{bmatrix} 10 & -3 \\ -5 & 2 \end{bmatrix} = (5)^{-1}. \begin{bmatrix} 10 & -3 \\ -5 & 2 \end{bmatrix}$$

Para calcular $(5)^{-1}$:

$5.5^{-1} = 1(mod\ 26)$

Observe que: $5.21 = 1(mod\ 26)$,

logo, $5^{-1} = 21$

$$A^{-1} = 21. \begin{bmatrix} 10 & -3 \\ -5 & 2 \end{bmatrix}$$

portanto, a matriz inversa é:

$$A^{-1} = \begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix}$$

Efetuando as multiplicações matriciais tem-se:

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 7 \\ 1 \end{bmatrix} = \begin{bmatrix} 210.7 - 63.1 \\ -105.7 + 42.1 \end{bmatrix} = \begin{bmatrix} 1470 - 63 \\ -735 + 42 \end{bmatrix} = \begin{bmatrix} 1407 \\ -693 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 14 \\ 2 \end{bmatrix} = \begin{bmatrix} 210.14 - 63.2 \\ -105.14 + 42.2 \end{bmatrix} = \begin{bmatrix} 2940 - 126 \\ -1470 + 84 \end{bmatrix} = \begin{bmatrix} 2814 \\ -1386 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 14 \\ 19 \end{bmatrix} = \begin{bmatrix} 210.14 - 63.19 \\ -105.14 + 42.19 \end{bmatrix} = \begin{bmatrix} 2940 - 1197 \\ -1470 + 798 \end{bmatrix} = \begin{bmatrix} 1743 \\ -672 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 8 \\ 1 \end{bmatrix} = \begin{bmatrix} 210.8 - 63.1 \\ -105.8 + 42.1 \end{bmatrix} = \begin{bmatrix} 1680 - 63 \\ -840 + 42 \end{bmatrix} = \begin{bmatrix} 1617 \\ -798 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 2 \\ 9 \end{bmatrix} = \begin{bmatrix} 210.2 - 63.9 \\ -105.2 + 42.9 \end{bmatrix} = \begin{bmatrix} 420 - 567 \\ -210 + 378 \end{bmatrix} = \begin{bmatrix} -147 \\ 168 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 14 \\ 18 \end{bmatrix} = \begin{bmatrix} 210.14 - 63.18 \\ -105.14 + 42.18 \end{bmatrix} = \begin{bmatrix} 2940 - 1134 \\ -1470 + 756 \end{bmatrix} = \begin{bmatrix} 1806 \\ -714 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 210.0 - 63.1 \\ -105.0 + 42.1 \end{bmatrix} = \begin{bmatrix} 0 - 63 \\ 0 + 42 \end{bmatrix} = \begin{bmatrix} -63 \\ 42 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 210.3 - 63.6 \\ -105.3 + 42.6 \end{bmatrix} = \begin{bmatrix} 630 - 378 \\ -315 + 252 \end{bmatrix} = \begin{bmatrix} 252 \\ -63 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 25 \\ 4 \end{bmatrix} = \begin{bmatrix} 210.25 - 63.4 \\ -105.25 + 42.4 \end{bmatrix} = \begin{bmatrix} 5250 - 252 \\ -2625 + 168 \end{bmatrix} = \begin{bmatrix} 4998 \\ -2457 \end{bmatrix}$$

$$\begin{bmatrix} 210 & -63 \\ -105 & 42 \end{bmatrix} . \begin{bmatrix} 10 \\ 23 \end{bmatrix} = \begin{bmatrix} 210.10 - 63.23 \\ -105.10 + 42.23 \end{bmatrix} = \begin{bmatrix} 2100 - 1449 \\ -1050 + 966 \end{bmatrix} = \begin{bmatrix} 651 \\ -84 \end{bmatrix}$$

Obtendo os seguintes resultados numéricos:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1407 | -693 | 2814 | -1386 | 1743 | -672 | 1617 | -798 | -147 | 168 |
| 1806 | -714 | -63 | 42 | 252 | -63 | 4998 | -2457 | 651 | -84 |

Fonte: a própria autora

Como todos os valores devem ser inteiros não negativos menores do que 26, é necessário tomar os respectivos restos das divisões por 26:

$$1407 \equiv 3 \ (mod\ 26)$$

$$-693 \equiv 9 \ (mod\ 26)$$

$$2814 \equiv 6 \ (mod\ 26)$$

$$-1386 \equiv 18 \ (mod\ 26)$$

$$1743 \equiv 1 \ (mod\ 26)$$

$$-672 \equiv 4 \ (mod\ 26)$$

$$1617 \equiv 5 \ (mod\ 26)$$

$$-798 \equiv 8 \ (mod\ 26)$$

$$-147 \equiv 9 \ (mod\ 26)$$

$$168 \equiv 12 \ (mod\ 26)$$

$$1806 \equiv 12 \ (mod\ 26)$$

$$-714 \equiv 14 \ (mod\ 26)$$

$$-63 \equiv 15 \ (mod\ 26)$$

$$42 \equiv 16 \ (mod\ 26)$$

$$252 \equiv 18 \ (mod\ 26)$$

$$-63 \equiv 15 \ (mod\ 26)$$

$$4998 \equiv 6 \ (mod\ 26)$$

$$-2457 \equiv 13 \ (mod\ 26)$$

$$651 \equiv 1 \ (mod\ 26)$$

$$-84 \equiv 20 \ (mod\ 26)$$

Resultando em:

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 9 | 6 | 18 | 1 | 4 | 5 | 8 | 9 | 12 | 12 | 14 | 15 | 16 | 18 | 15 | 6 | 13 | 1 | 20 |

Fonte: a própria autora

Para finalizar basta substituir os números pelas letras conforme tabela:

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 9 | 6 | 18 | 1 | 4 | 5 | 8 | 9 | 12 | 12 | 14 | 15 | 16 | 18 | 15 | 6 | 13 | 1 | 20 |
| C | I | F | R | A | D | E | H | I | L | L | N | O | P | R | O | F | M | A | T |

Fonte: a própria autora

Finalmente, decifrada a frase ”GANBNSHABINRZACFYDJW” obteve-se ”CIFRADEHILLNOPRO que, depois de separadas as palavras conforme o contexto, resultou em "CIFRA DE HILL NO PROFMAT"

# 4

# APLICATIVO

Este capítulo visa apresentar o software educacional para dispositivos móveis, desenvolvido durante o presente estudo, com o objetivo de exercitar conceitos matemáticos da Educação Básica por meio de atividades que envolvam a criptografia.

Na busca de uma forma mais dinâmica, interessante e condizente com os tempos atuais para o estudo da matemática, desenvolveu-se um software em forma de jogo, para dispositivos móveis, com algumas etapas, todas envolvendo raciocínio matemático e conceitos muito presentes no Ensino Médio.

Em sua essência, o grande objetivo é apresentar ou relembrar ao jogador, conceitos de matrizes, determinantes, aritmética modular (de forma implícita), entre outros, através da Cifra de Hill, técnica de criptografia muito útil para o estudo desses conceitos.

Para o seu desenvolvimento e sua implantação foram usadas as seguintes ferramentas tenológicas: React Native, Typescript, Expo Go, Visual Studio Code, Git, Github, Google Market Place.

O aplicativo é gratuito e de código aberto, disponível para download e cópia sem fins comerciais através do link: <https://github.com/samantaProspero/criptoalien_final>. Estando também disponível para download no Google Play Store através do link: <https://play.google.com/store/apps/details?id=com.samanta.criptoalien>.

## 4.1 O JOGO

O jogo possui como pano de fundo a tentativa de invasão alienígena ao planeta Terra. O jogador tem como missão, enfrentar vários desafios para impedir os ataques contando com a ajuda de um espião que está infiltrado entre os inimigos, que, para se comunicar, precisa do sigilo das informações, lançando mão da criptografia para garantir essa segurança.

O método de criptografia escolhido foi o das Cifras de Hill, que, como descrito anteriormente, é fundamentalmente composto por operações com matriciais no conjunto dos números Inteiros, além da aritmética modular.

O jogo possui 32 telas, as quais serão descritas à seguir. As três primeiras se referem à apresentação do jogo, as boas vindas ao jogador e a tela com as fases existentes.

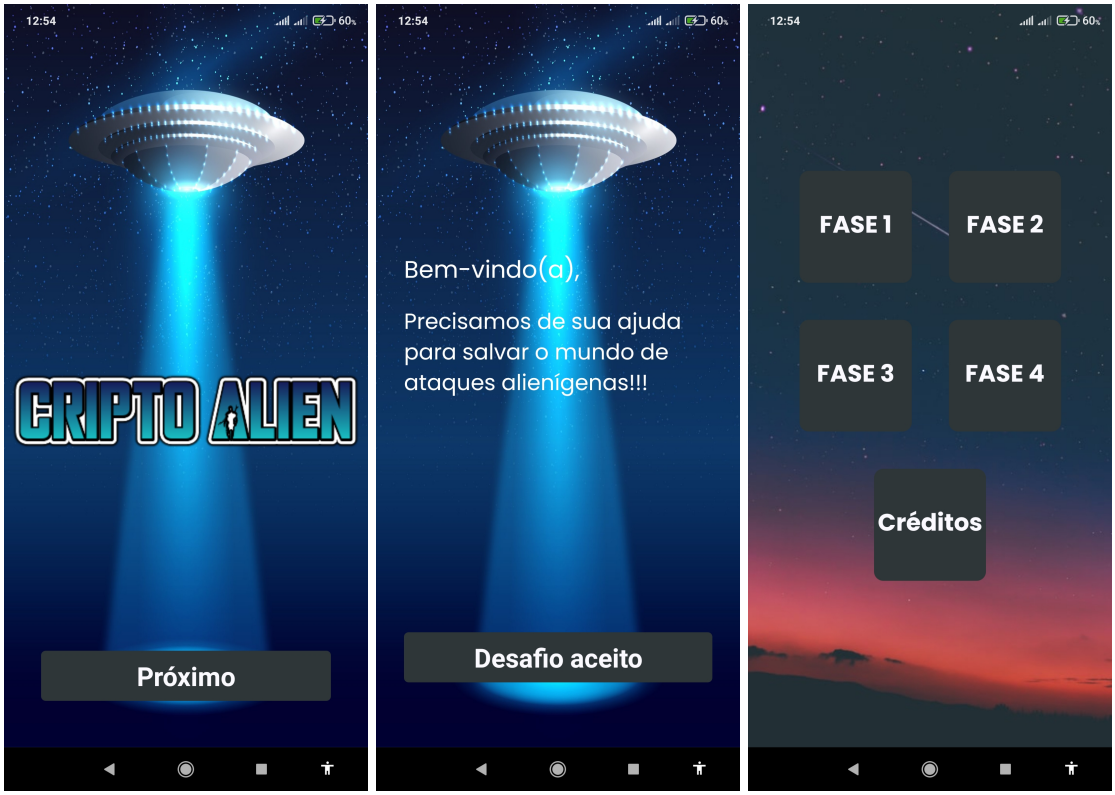



Figura 5: Telas Iniciais do Jogo

Fonte: Aplicativo Cripto Alien

### 4.1.1 *Primeira Fase*

Nas duas telas seguintes, o jogador é apresentado à primeira fase e recebe sua missão pois, o espião enviou uma pista do primeiro ataque dos alienígenas.

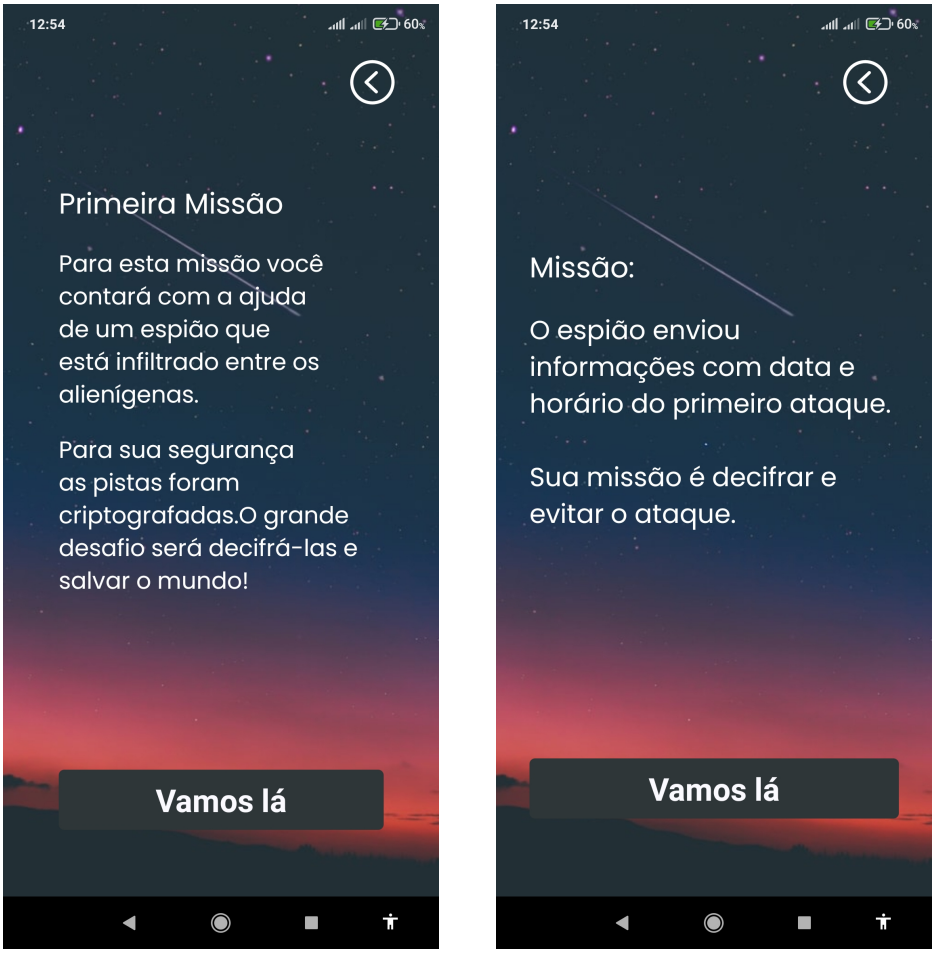



Figura 6: Telas Iniciais da fase 1

Fonte: Aplicativo Cripto Alien

Com o objetivo de impedir o primeiro ataque o jogador precisa descobrir o dia da semana previsto para explosão, para isto ele contará com uma data codificada: dia 156 e da informação sobre o primeiro dia do ano(figura: 7).


Figura 7: Primeiro desafio

Fonte: Aplicativo Cripto Alien

Como é uma data com mais de trinta ou trinta e um dias, o jogador deverá perceber que este número se refere aos dias do ano e não do mês. Mas, como saber a qual dia da semana ela se refere? O jogador poderá resolver de duas formas:

- A mais sofrida: pegar o calendário de 2021, e contar um por um à partir de primeiro de janeiro;
- O esperado: observar que o ano é composto por ciclos de sete dias, e que basta pegar o número da data fornecido, dividi-lo por 7, e obter o resto.

Dado que o primeiro dia do ano de 2021 ocorreu em uma sexta-feira, então, os ciclos semanais serão:

$$\text{resto} = 1 \implies \text{Sexta-feira}$$

resto = 2 $\Longrightarrow$ Sábado

resto = 3 $\Longrightarrow$ Domingo

resto = 4 $\Longrightarrow$ Segunda-feira

resto = 5 $\Longrightarrow$ Terça-feira

resto = 6 $\Longrightarrow$ Quarta-feira

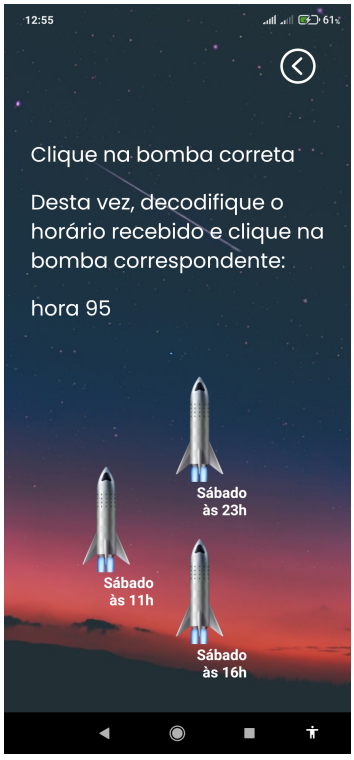
resto = 0 $\Longrightarrow$ Quinta-feira

O jogador deverá clicar na imagem da bomba com a data correta.

Caso falhe na primeira tentativa, ele pode acessar a tela de dica (figura: 4.1.1), e nela haverá a imagem de um calendário do mês de janeiro de 2021, com destaque visual ao dia primeiro de janeiro, e um destaque adicional aos sete primeiros dias do mês.

Na tela seguinte, o jogador terá um desafio semelhante, agora envolvendo a hora 95. E para ter sucesso, o jogador precisará encontrar o resto da divisão deste número por 24, que corresponde às vinte quatro horas contidas em um dia (figura: 8).

Figura 8: Tela do Desafio do Horário




Fonte: Aplicativo Cripto Alien

### 4.1.2 *Segunda Fase*

Neste momento, o jogador precisará avisar ao espião do seu sucesso na fase anterior, e para isso, ele deverá seguir algumas etapas, que serão descritas à seguir, para cifrar a palavra “DESATIVADA” por meio das Cifras de Hill.

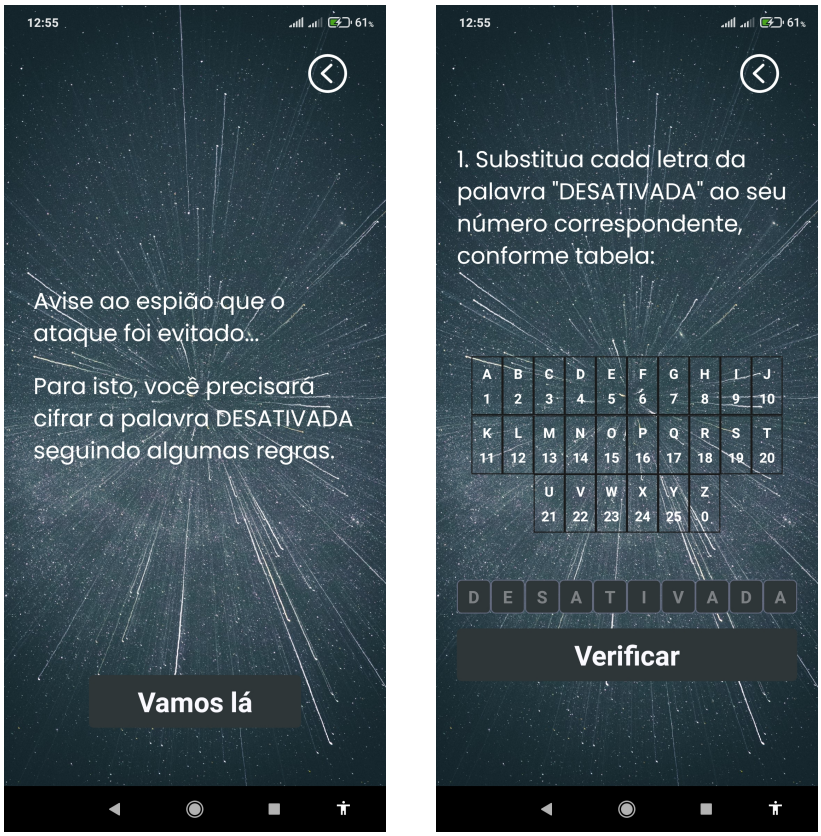



Figura 9: Inicio da Segunda Missão

Fonte: Aplicativo Cripto Alien

1. O primeiro passo é substituir cada cada letra da palavra DESATIVADA pelo seu correspondente numérico conforme a tabela apresentada na tela [figura: 9.2],

2. Na Figura 10.2 o jogador precisa digitar uma matriz inversível em $\mathbb{Z}_{26}$ mas, alunos aprendem, na Educação Básica, matriz inversível no conjunto dos números reais, não no conjunto dos inteiros. Para evitar confusão, o termo matriz inversível não fez parte do enunciado da missão e, apesar do conceito ter sido utilizado na lógica do jogo e nos códigos de programação (Figura: 21), optou-se por solicitar uma matriz cuja determinante fosse um dos valores existes em uma lista fornecida.

Nesta tela o jogador tem a disposição um campo de dica, caso ele considere necessário (Figura: 10.1), onde encontrará uma explicação para o cálculo do determinante.


Figura 10: Matriz Inversível

Fonte: Aplicativo Cripto Alien

3. Esta etapa consiste em efetuar as multiplicações entre a matriz inversível, obtida na etapa 2 desta fase, com matrizes 2x1, formadas por pares de números da palavra DESATIVADA da etapa 1, totalizando cinco multiplicações (Figura: 11). Para para não ser uma atividade muito desgastante, o nível de dificuldade foi aumentando gradativamente. Em uma tela, a primeira multiplicação foi apresentada como exemplo, totalmente resolvida, na tela seguinte, as demais multiplicações foram apresentas:

    - a primeira multiplicação também totalmente resolvida;
    - a segunda, continha a matriz inversível, a matriz 2x1, composta pelos terceiro e quarto números da palavra, um campo com as multiplicações de cada linha, restando ao jogador, efetuar as operações e digitar o resultado;

- na terceira, além do resultado, foram omitidos os resultados das multiplicações;
- e na última, o jogador precisa identificar e digitar na matriz 2x1, os dois últimos valores da palavra, além de digitar o resultado da multiplicação.

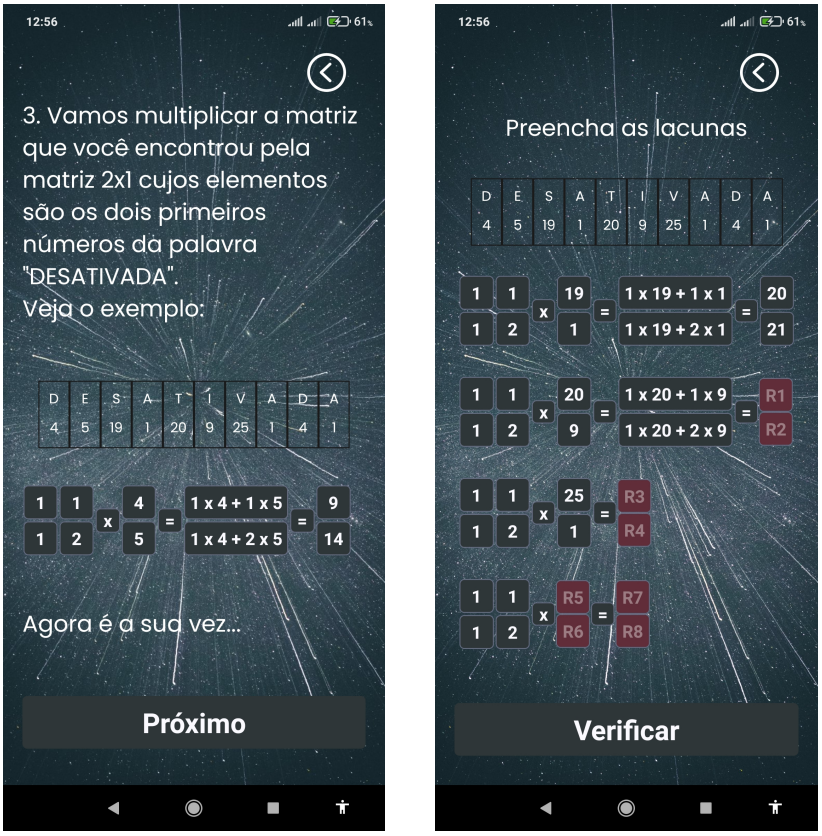



Figura 11: Multiplicação Matriciais

Fonte: Aplicativo Cripto Alien

4. O próximo passo é pegar a sequência dos dez números resultantes da etapa anterior, e garantir que todos sejam menores do que 26 (Figura 12). Nesta versão do aplicativo, o programa entregará a lista original, com os resultados das multiplicações, seguida de uma lista “corrigida”, ou seja, para cada número, o programa devolverá o resto de sua divisão por 26 (trecho do código disponível na figura: 22).

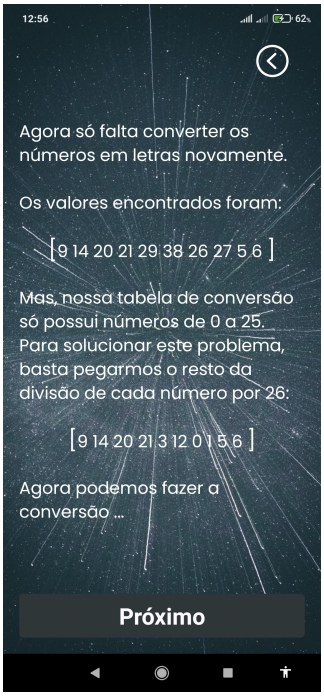



Figura 12: Restos módulo 26

Fonte: Aplicativo Cripto Alien

5. Finalmente, na tela é apresentada a lista dos números obtidos na etapa anterior, o jogador deverá substituir os valores numéricos por seus respectivos correspondentes no alfabeto, fazendo o inverso da primeira etapa, obtendo assim, a palavra cifrada.

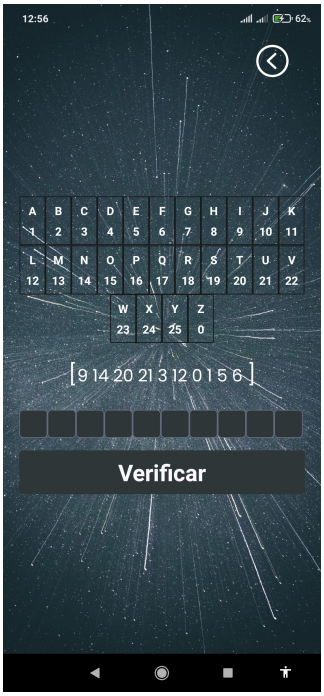



Figura 13: Substituição por letra

Fonte: Aplicativo Cripto Alien

### 4.1.3 *Terceira Fase*

O espião foi informado que a primeira bomba foi desativada, neste momento o jogador repetirá as etapas da fase anterior para codificar a palavra DICA, e assim, ter acesso à próxima missão, figura 14.

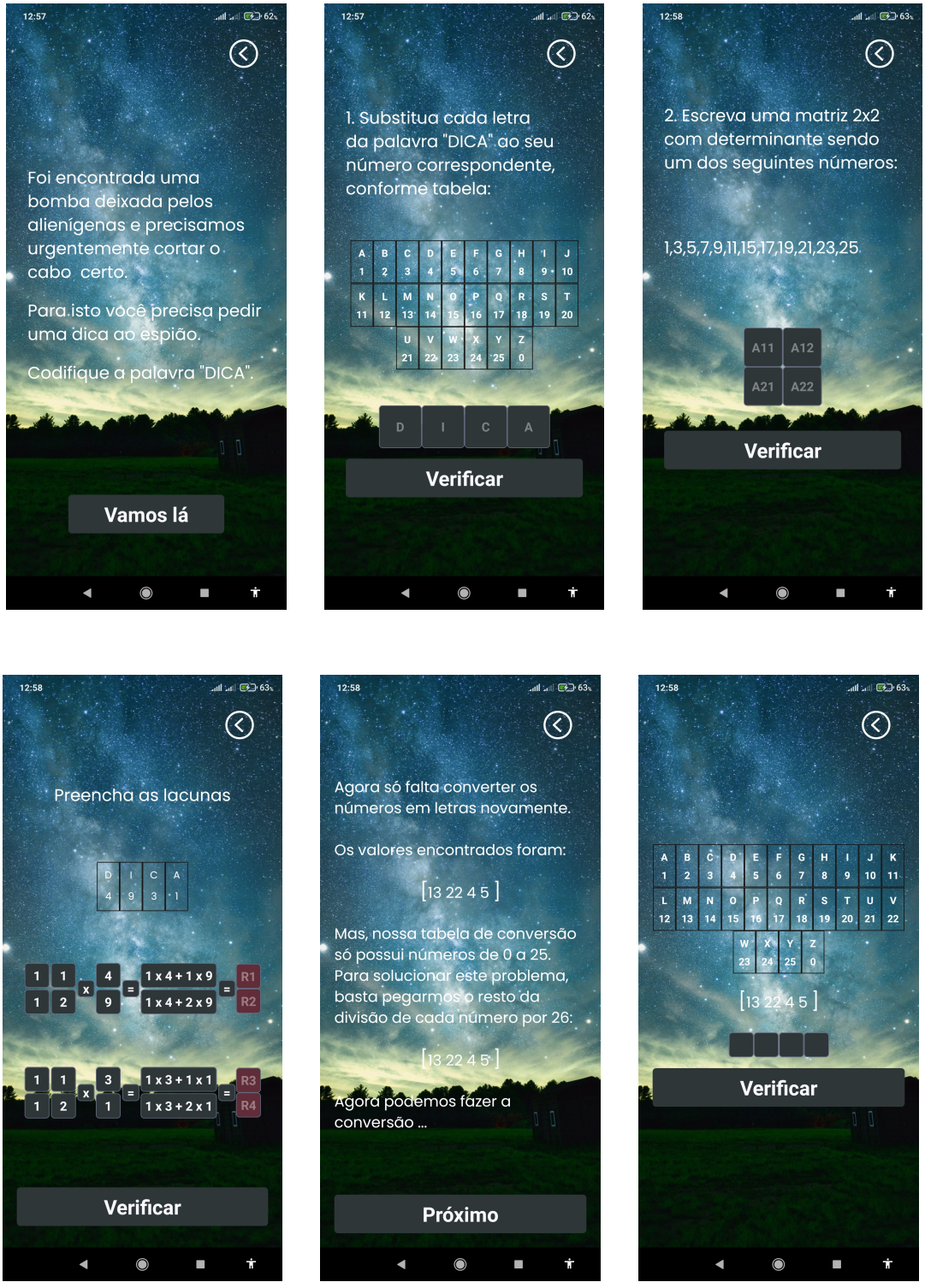



Figura 14: Terceira Fase

Fonte: Aplicativo Cripto Alien

### 4.1.4 *Quarta Fase*

Ao cifrar a palavra DICA na fase anterior, o jogador recebeu do espião uma palavra cifrada e uma matriz 2x2.

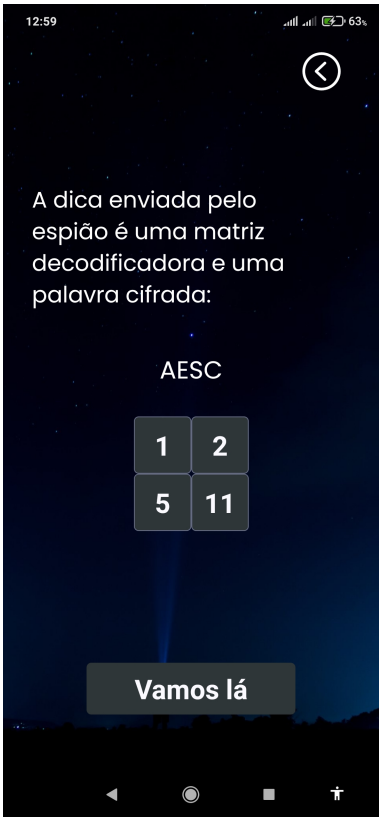



Figura 15: Dicas recebidas
Fonte: Aplicativo Cripto Alien

Nesta fase, a missão é cortar o cabo com a cor correta e evitar um novo ataque. Com as informações enviadas pelo espião, o jogador precisa decodificar a palavra "AESC" para descobrir a cor do cabo, seguindo as seguintes etapas:

1. Substituir as letras por números conforme tabela exibida na tela (Figura: 16);

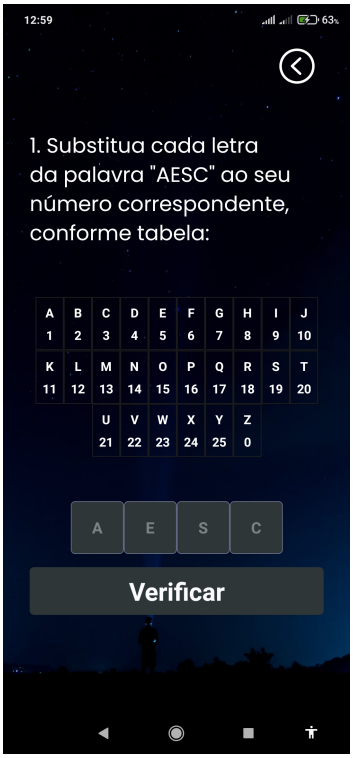



Figura 16: Substituição por números

Fonte: Aplicativo Cripto Alien

2. Calcular a matriz inversa da matriz fornecida pelo espião, figura 17

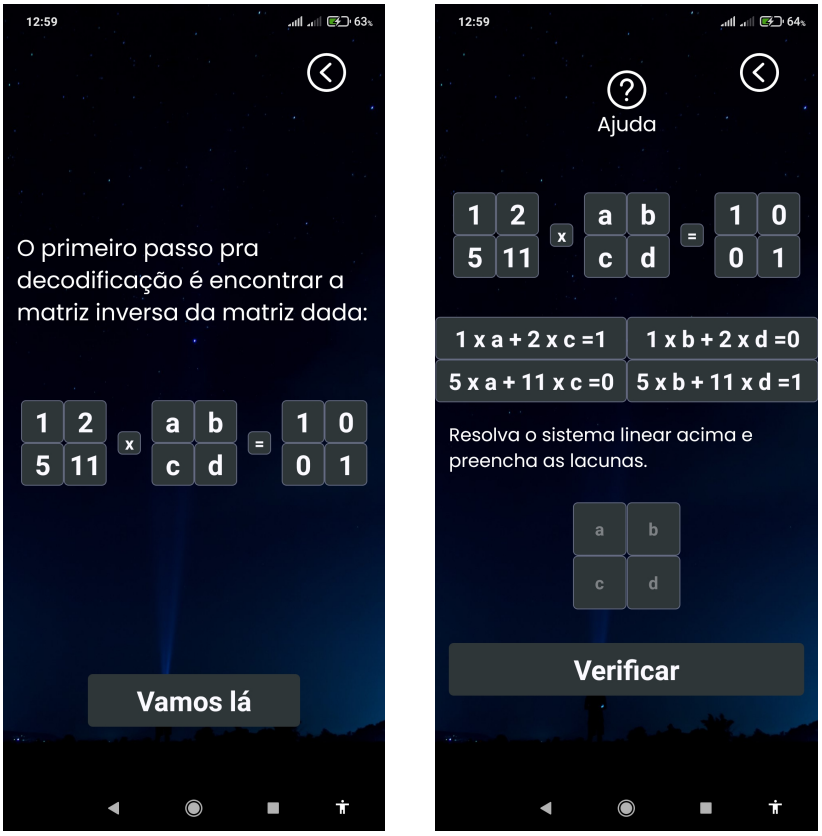



Figura 17: Cálculo da Matriz Inversa

Fonte: Aplicativo Cripto Alien

3. Efetuar as duas multiplicações entre matrizes;

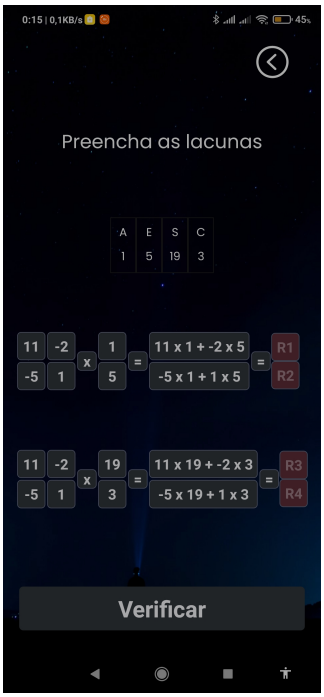



Figura 18: Multiplicação Matricial

Fonte: Aplicativo Cripto Alien

4. Para cada número obtido, calcular o resto da divisão por 26;

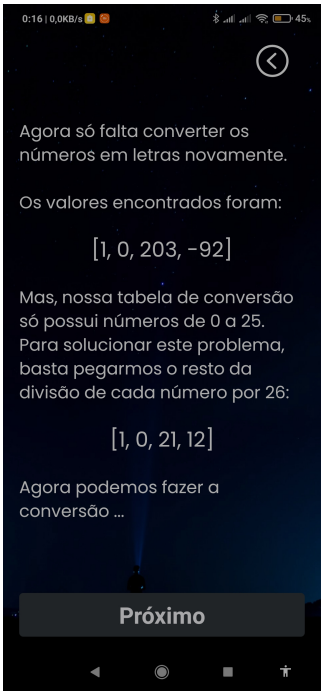



Figura 19: Restos Módulo 26

Fonte: Aplicativo Cripto Alien

5. Converter esses números novamente em letras;

Figura 20: Substituição por letra


Fonte: Aplicativo Cripto Alien Fonte: Aplicativo Cripto Alien

Decodificada, a resposta será a cor do cabo que o jogador deverá cortar para impedir a últma tentativa de ataque e salvar o mundo.

## 4.2 SUGESTÕES DE TRABALHOS FUTUROS

Algumas funcionalidades podem ser adicionadas em versões futuras do aplicativo.

- Fases adicionais com codificação de palavras escolhidas pelo jogador,
- Inserção da etapa para o jogador calcular os restos das divisões por 26,
- Melhorias estéticas no aplicativo,
- Estudo aprofundado da metodologia Design Science Research (DSR) para possíveis melhorias.

# 5

# CONSIDERAÇÕES FINAIS

Acredita-se na potencialidade que os aplicativos móveis têm para o ensino, no quesito portabilidade e baixo custo, estes artefatos tecnológicos podem ser mediadores entre o professor e os conceitos matemáticos. Apesar deste trabalho não abordar metodologias específicas de ensino para a elaboração de artefatos educativos, foi projetado um aplicativo com o compromisso de atingir o objetivo: dar continuidade, de forma prática, aos conceitos iniciais de álgebra linear. Buscando algum elemento no comportamento dos adolescentes para guiar a geração de um protótipo e posteriormente, a criação do aplicativo. O software para dispositivos móveis, aqui apresentado, é composto por um jogo com atividades dinâmicas envolvendo conceitos matemáticos existentes na Cifra de Hill, uma técnica que efetua criptografia de textos através de operações matriciais. O aplicativo é gratuito e de código aberto, disponível no Google Play Store através do endereço: <https://play.google.com/store/apps/details?id=com.samanta.criptoalien>, e seu código está disponível para cópia, sem fins comerciais, no endereço: <https://github.com/samantaProspero/criptoalien_final> Destaca-se também que a construção do aplicativo, estimula e aprimora a produção de novos conhecimentos e habilidades.

Artefatos tecnológicos por si, não viabilizam o ensino e a aprendizagem, é necessário uma abordagem epistemológica-metodológica. Infelizmente deparou-se de forma tardia com a metodologia Design Science Research (DSR), que segundo (PIMENTEL; FILIPPO; SANTORO, 2019) na abordagem Design Science Research (DSR) que encontramos fundamentos que legitimam o desenvolvimento de artefatos como um meio para a produção de conhecimentos científicos do ponto de vista epistemológico. Espera-se que um futuro não distante, embasados na metodologia DSR ou em outra que venha ser conveniente, possam ser revistas e melhoradas as fases do aplicativo.

# REFERÊNCIAS BIBLIOGRÁFICAS


ANTON, H.; RORRES, C. ***Álgebra linear com aplicações***. [S.l.]: Bookman Porto Alegre, 2001. v. 8.

BARROS, A. ***Internet chega a 88,1% dos estudantes, mas 4,1 milhões da rede pública não tinham acesso em 2019***. 2021. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2021-04/acesso-de-estudantes-internet-aumenta-para-881-em-2019-diz-ibge>.

BRITO, M. ***Bootcamp Launchbase Rocketseat***. 2020. Disponível em: <https://app.rocketseat.com.br/>.

DACIUK, F. ***Curso JavaScript Ninja***. 2020. Disponível em: <https://www.udemy.com/course/curso-javascript-ninja/>.

DAMASCENO, J. ***Desenvolvimento Web Completo- 20 cursos + 20 projetos***. 2019. Disponível em: <https://www.udemy.com/course/web-completo/>.

DOOLEY, J. F. ***History of Cryptography and Cryptanalysis: Codes, Ciphers, and their algorithms***. [S.l.]: Springer, 2018.

GONÇALVES, A. ***Introdução à álgebra***. [S.l.]: Impa, 1979.

GPE-FEMIC, G. de Pesquisa e Estudos Filosóficos em Educação Matemática e Interfaces com outras C. **A semiótica de Husserl: contribuições para a educação matemática no âmbito da formação inicial de professores de matemática**. p. 16.

GUANABARA, G. ***Curso de HTML5 Completo e GRÁTIS***. YouTube, 2013. Disponível em: <https://youtube.com/playlist?list=PLHz_AreHm4dlAnJ_jJtV29RFxnPHDuk9o>.

GUANABARA, G. ***Curso em Vídeo: Curso de Lógica da Programação***. 2014. Disponível em: <https://youtube.com/playlist?list=PLHz_AreHm4dmSj0MHol_aoNYCSGFqvfXV>.

GUANABARA, G. ***Curso de JavaScript e ECMAScript para iniciantes***. 2019. Disponível em: <https://youtube.com/playlist?list=PLHz_AreHm4dlsK3Nr9GVvXCbpQyHQl1o1>.

HEFEZ, A. ***Aritmética***. [S.l.: s.n.], 2013.

HILL, L. S. **Cryptography in an Algebraic Alphabet**. *The American Mathematical Monthly*, Taylor & Francis, v. 36, n. 6, p. 306–312, 1929.

HILL, L. S. **Concerning Certain Linear Transformation Apparatus of Cryptography**. *The American Mathematical Monthly*, Taylor & Francis, v. 38, n. 3, p. 135–154, 1931.

KAHN, D. ***The Codebreakers: The comprehensive history of secret communication from ancient times to the internet***. [S.l.]: Simon and Schuster, 1996.

MILIES, F. C. P.; COELHO, S. P. ***Números: uma introdução à matemática***. [S.l.]: Edusp, 2001.

MIRANDA, L. O. ***Curso de JavaScript e TypeScript do básico ao avançado***. 2019. Disponível em: <https://www.udemy.com/course/curso-de-javascript-moderno-do-basico-ao-avancado/>.

PAAR, C.; PELZL, J. ***Understanding cryptography: a textbook for students and practitioners***. [S.l.]: Springer Science & Business Media, 2009.

PIMENTEL, M.; FILIPPO, D.; SANTORO, F. M. **Design Science Research: fazendo pesquisas científicas rigorosas atreladas ao desenvolvimento de artefatos computacionais projetados para a educação**. *Metodologia de Pesquisa em Informática na Educação: Concepção da Pesquisa. Porto Alegre: SBC*, 2019.

SANTOS, A. P. F. d. ***A criptografia no ensino fundamental II : contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas outras curiosidades***. Tese (Doutorado) — Universidade Estadual do Norte Fluminense Darcy Ribeiro, 2016.

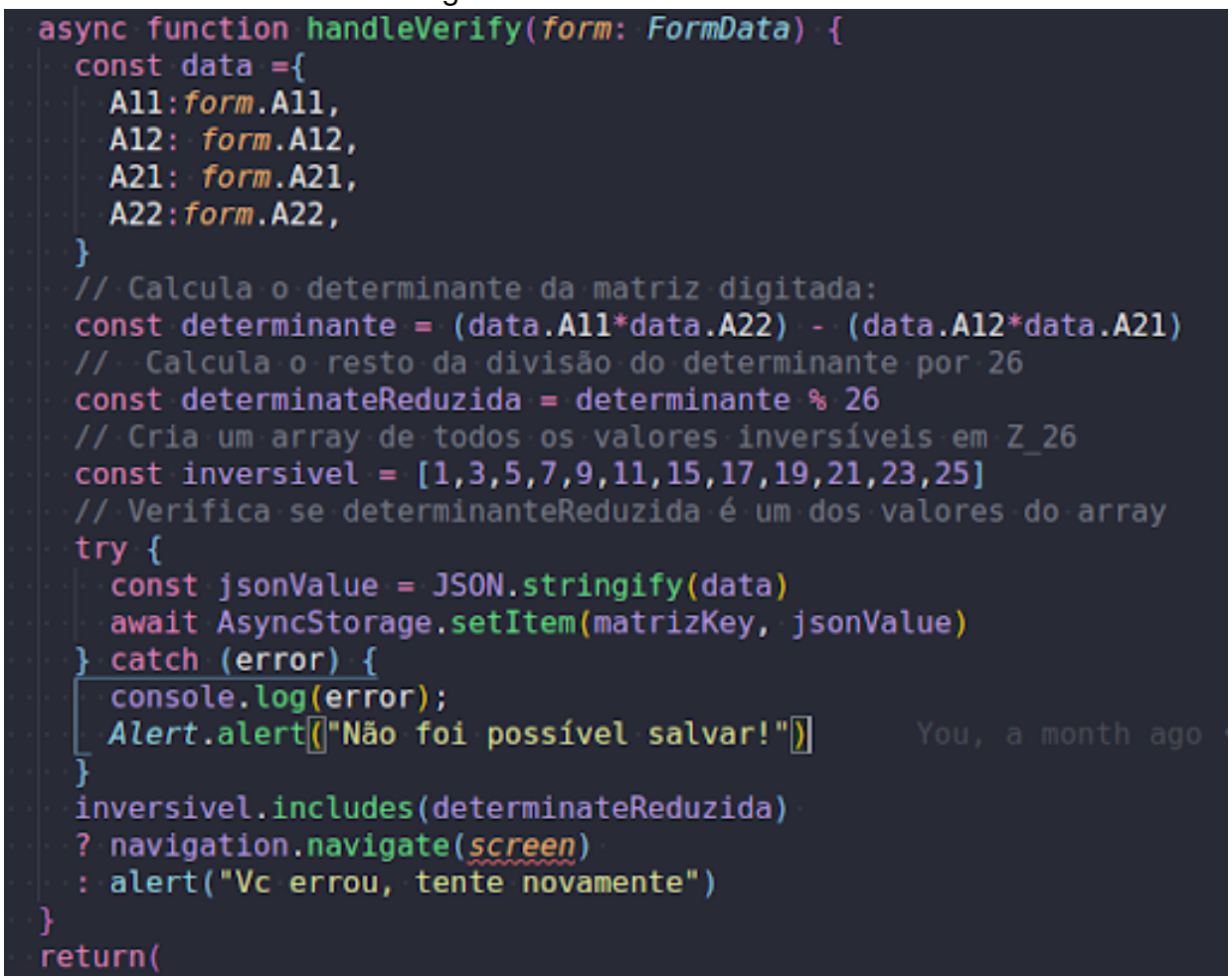
SINGH, S. ***O Livro dos Códigos: A Ciências do Sigilo-do Antigo Egito à Criptografia Quântica***. [S.l.: s.n.], 2001.

SINKOV, A. ***Elementary Cryptanalysis: a Mathematical Approach***. [S.l.: s.n.], 1966. v. 22.

SINKOV, A.; FEIL, T. ***Elementary cryptanalysis***. [S.l.]: MAA, 2009. v. 22.

SONEGO, A. H. S.; BEHAR, P. A. **M-Learning: Reflexões e Perspectivas com o uso de aplicativos educacionais**. p. 521–526, 2015.

Figura 21: Matriz inversível



```
async function handleVerify(form: FormData) {
    const data ={
      A11:form.A11,
      A12: form.A12,
      A21: form.A21,
      A22:form.A22,
    }
    // Calcula o determinante da matriz digitada:
    const determinante = (data.A11*data.A22) - (data.A12*data.A21)
    //  Calcula o resto da divisão do determinante por 26
    const determinateReduzida = determinante % 26
    // Cria um array de todos os valores inversíveis em Z_26
    const inversivel = [1,3,5,7,9,11,15,17,19,21,23,25]
    // Verifica se determinanteReduzida é um dos valores do array
    try {
      const jsonValue = JSON.stringify(data)
      await AsyncStorage.setItem(matrizKey, jsonValue)
    } catch (error) {
      console.log(error);
      Alert.alert("Não foi possível salvar!")      You, a month ago
    }
    inversivel.includes(determinateReduzida)
    ? navigation.navigate(screen)
    : alert("Vc errou, tente novamente")
}
return(
```

Fonte: Código Aplicativo Cripto Alien

## CÓDIGO PARA CÁLCULO DOS RESTOS MÓDULO 26

Figura 22: Restos módulo 26

```
      <Title>
        [
        {contasFinais.map((conta: number, index: number) => (
          <DescriptionText key={index}>{conta} </DescriptionText>
        ))}
        ]
      </Title>
      <DescriptionText>
        Mas, nossa tabela de conversão só possui números de 0 a 25. Para
        solucionar este problema, basta pegarmos o resto da divisão de cada
        número por 26:
      </DescriptionText>
      <Title>
        [
        {contasFinais.map((conta: number, index: number) => (
          <DescriptionText key={index}>{conta % 26} </DescriptionText>
        ))}
        ]
      </Title>
      <DescriptionText>Agora podemos fazer a conversão ...</DescriptionText>
    </PrincipalContainer>
    <Button description="Próximo" onPress={handleRespostas} />
  </Container>
```

Fonte: Código Aplicativo Cripto Alien

## CÓDIGO PARA MULTIPLICAÇÃO DE MATRIZES

Figura 23: Multiplicação de matrizes

```
function handleConta(){
  const contasFinais = [
    data.A11 * vetor[0] + data.A12 * vetor[1],
    data.A21 * vetor[0] + data.A22 * vetor[1],
    data.A11 * vetor[2] + data.A12 * vetor[3],
    data.A21 * vetor[2] + data.A22 * vetor[3],
  ]
  return contasFinais
}

function handleVerify(form: FormData) {
  const resps = {
    resp1: form.resp1,
    resp2: form.resp2,
    resp3: form.resp3,
    resp4: form.resp4,
  }
  setResps(resps)
  const contasFinais = handleConta()

  const testeResps =
  resps.resp1 == handleConta()[0] &&
  resps.resp2 == handleConta()[1] &&
  resps.resp3 == handleConta()[2] &&
  resps.resp4 == handleConta()[3]

  testeResps ? navigation.navigate('Screen14a', {contasFinais})
  : alert("Vc errou, tente novamente")
}
```

Fonte: Código Aplicativo Cripto Alien