INSTITUTO FEDERAL DA PARAÍBA
CAMPUS CAJAZEIRAS
CURSO DE ESPECIALIZAÇÃO EM MATEMÁTICA

CARLA JOSEFA GONÇALO DE OLIVEIRA

PROTOCOLO DIFFIE-HELLMAN: CONTEXTO HISTÓRICO, MATEMÁTICO E APLICAÇÕES EM SALA DE AULA

CAJAZEIRAS
2021

CARLA JOSEFA GONÇALO DE OLIVEIRA

PROTOCOLO DIFFIE-HELLMAN: CONTEXTO HISTÓRICO, MATEMÁTICO E APLICAÇÕES EM SALA DE AULA

Monografia apresentada junto ao **Curso de Especialização em Matemática** do **Instituto Federal da Paraíba**, como parte dos requisitos à obtenção do título de **Especialista em Matemática**.

Orientador(a):

Prof(a). Dr(a). Vinicius Martins Teodosio Rocha.

Cajazeiras

2021

CARLA JOSEFA GONÇALO DE OLIVEIRA

PROTOCOLO DIFFIE-HELLMAN: CONTEXTO HISTÓRICO, MATEMÁTICO E APLICAÇÕES EM SALA DE AULA

Monografia apresentada ao **Curso de Especialização em Matemática** do **Instituto Federal da Paraíba**, como parte dos requisitos à obtenção do título de **Especialista em Matemática**.

Data de aprovação: 13/08/2021

Banca Examinadora:

Prof. Dr. Vinicius Martins Teodosio Rocha
Instituto Federal da Paraíba - IFPB

Prof. Me. Geraldo Herbetet de Lacerda
Instituto Federal da Paraíba - IFPB

Prof. Me. José Doval Nunes Martins
Instituto Federal da Paraíba - IFPB

Campus Cajazeiras
Coordenação de Biblioteca
Biblioteca Prof. Ribamar da Silva
Catalogação na fonte: Daniel Andrade CRB-15/593

O48p

Oliveira, Carla Josefa Gonçalo de

Protocolo Diffie-Hellman: contexto histórico, matemático e aplicações em sala de aula / Carla Josefa Gonçalo de Oliveira; orientador Vinicius Martins Teodosio Rocha.- 2021.
55 f.: il.

Orientador: Vinicius Martins Teodosio Rocha.
TCC (Especialização em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Cajazeiras, 2021.

1. Criptografia 2. Protocolo Diffie-Hellman 3. Logaritmos discretos. I. Título

CDU 51(083.73)(0.067)

Dedico este trabalho aos meus pais Enádio Elias de Oliveira (in memoriam) e Rosinha Gonçalo de Oliveira, pelo incentivo ao estudo e a meu esposo Francisco Petronio Nobre Lopes pelo apoio à construção do mesmo.

AGRADECIMENTOS

A Deus, pelo dom da vida e por me conceder saúde e força para a realização de mais um projeto;

Aos meu pais, que sempre me incentivaram a estudar;

Ao meu esposo Petronio, pela paciência nos momentos em que precisei me ausentar e pelo grande incentivo à construção desse projeto;

Ao meu orientador, Vinícius Martins Teodosio Rocha, pela paciência, dedicação, pelos ensinamentos e grande colaboração à elaboração do mesmo;

Aos colegas e amigos por todos os momentos vividos juntos e compartilhados, em especial a Cristiano, pelo incentivo para cursar a Especialização e à Fatinha pelo apoio e ajuda durante todo o curso e incentivo para que eu não desistisse do mesmo.

E a todos que compõem o Instituto Federal da Paraíba - Campus de Cajazeiras.

"A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."

Albert Einstein

RESUMO

Atualmente, a segurança da comunicação entre os meios digitais é imprescindível, por isso a utilização da criptografia torna-se cada vez mais necessária. O conceito de chave pública, que surgiu em 1976, através de dois pesquisadores, Bailey Whitfield Diffie e Martin Edward Hellman, proporcionou um grande avanço na criptografia abrindo precedentes para o surgimento de técnicas muito utilizadas nos dias atuais. Neste trabalho, enunciamos definições e teoremas sobre divisibilidade, números primos, grupos e logaritmos discretos; apresentamos um breve histórico da evolução da criptografia; diferenciamos criptografia simétrica da criptografia assimétrica; descrevemos o algoritmo do protocolo de troca de chaves de Diffie-Hellman, analisando-o como o problema do logaritmo discreto; e na parte final, propomos três atividades para serem aplicadas na sala de aula.

Palavras-chave: criptografia, Diffie-Hellman, grupos, logaritmos discretos.

ABSTRACT

In recent times, security in digital communication is crucial, therefore the use of cryptography has become increasingly necessary. The concept of public key in cryptography, introduced in 1976 by researchers Bailey Whitfield Diffie and Martin Edward Hellman, has allowed a big advance in cryptography, setting the stage for the creation of the many techniques used nowadays. In this text we present concepts and results about divisibility, prime numbers, groups and discrete logarithms; we expose a brief description of the evolution of cryptography, distinguish between symmetric and asymmetric cryptosystems and describe Diffie-Hellman key exchange protocol, regarding it as an application of the discrete logarithm problem. We conclude by proposing related problems that that can be applied for students as exercises regarding basic concepts of arithmetic and algebra.

Keywords: cryptography, Diffie-Hellman, groups, discrete logarithms.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Com o surgimento da escrita, surge também a necessidade da troca de mensagens confidenciais, por motivações políticas, militares e até sentimentais, e essa necessidade motivou a criação da criptografia, que é o estudo de técnicas para modificar mensagens, ocultando seu verdadeiro significado, de forma que somente remetente e destinatário sejam capazes de compreendê-las e tornando difícil para possíveis intrusos descobrirem seu teor. Assim, caso as mensagens sejam interceptadas, seu conteúdo não será revelado, ou seja, a criptografia desenvolve métodos de codificar mensagens. Ao longo dos anos, essa técnica vem evoluindo, e boa parte dessa evolução deve-se a Matemática.

Uma situação típica da criptografia ocorre quando duas pessoas desejam se comunicar através de mensagens e precisam combinar uma chave, que é o segredo que as codifica e decodifica. Essa chave precisa ser compartilhada entre essas pessoas para ter acesso ao conteúdo das mensagens, mas se estão distantes, como compartilhar essa chave? Haveria um meio seguro de trocar essa chave? Esses questionamentos impulsionam nosso estudo.

A segurança da comunicação entre os meios digitais é imprescindível nos dias atuais, por isso a utilização da criptografia torna-se cada vez mais necessária. Ao realizarmos uma compra pela internet utilizando o cartão de crédito, por exemplo, as informações do cartão são codificadas pelo nosso computador antes de serem enviadas, entretanto, esse computador não pode usar um código qualquer para codificar as informações, pois a loja precisa decodificá-las, então essa ação é realizada de acordo com o processo de codificação da loja que estamos comprando, mas, se esta troca de informações não for feita num canal seguro, ou seja, de maneira que a informação sobre o processo de codificação ocorra de forma secreta, os dados do cartão de crédito poderiam facilmente ser lidos, colocando a segurança dos dados em risco (COUTINHO, 2015).

Observando a situação descrita acima, nos parece muito inseguro realizar transações pela internet, pois seja qual for o código utilizado, quem codifica, sabe decodificar, mas não é bem assim, já que há uma forma de criptografar uma mensagem, fácil de fazer, porém muito difícil de desfazer, sendo que quem a interceptasse, mesmo sabendo como foi codificada não conseguiria decodificá-la, a depender dos recursos que tivesse. Trata-se da criptografia de chave pública, sendo assim chamada porque a chave de codificação é conhecida por qualquer um, sem que a segurança do código seja comprometida. Tal conceito surgiu em 1976, na publicação de um livro por dois pesquisadores, Bailey Whitfield Diffie e Martin Edward Hellman.

O conceito de chave pública proporcionou um grande avanço na criptografia, já que é uma combinação de função exponencial com aritmética modular, diferentemente das técnicas de substituição e permutação utilizadas até então, e abriu precedentes para o surgimento de criptografias muito utilizadas nos dias atuais, como a RSA, criada em 1977, que recebe esse nome em razão dos seus inventores R. L. Rivest, A. Shamir e L. Adleman, e a assinatura digital.

Tendo por base o princípio de que a criptografia é um assunto muito importante para a atualidade e que a troca de chaves pelo protocolo Diffie-Hellman utiliza conceitos relevantes da Matemática, acredita-se que sua utilização nas aulas dessa disciplina pode proporcionar maior interesse na apropriação de tais conceitos. Dessa forma, este trabalho tem por objetivo geral elencar conhecimentos sobre Criptografia, especificamente sobre o protocolo de troca de chaves de Diffie-Hellman, de forma a subsidiar o professor de Matemática na introdução desses conceitos nas salas de aula do Ensino Fundamental ao Ensino Superior, a fim de dinamizar suas aulas e motivar os alunos no processo de ensino-aprendizagem.

Este trabalho apresenta como objetivos específicos os listados abaixo:

- Apresentar resultados da teoria dos números que servem de base para o protocolo de troca de chaves de Diffie-Hellman;
- Compreender as definições de grupos, raízes primitivas e logaritmos discretos, seus teoremas e demonstrações;
- Introduzir o conceito de criptografia;
- Diferenciar criptografia simétrica de criptografia assimétrica;
- Compreender o protocolo de troca de chaves de Diffie-Hellman;
- Conhecer a importância dos logaritmos discretos na troca de chaves de Diffie-Hellman;
- Propor atividades a serem trabalhadas no Ensino Básico e Superior.

Para uma melhor compreensão deste trabalho, faremos uma breve descrição dos assuntos tratados em cada capítulo.

No Capitulo 1, faremos um estudo resumido dos conceitos matemáticos com os resultados da Teoria dos Números, que servem de base para a troca de chaves através do Protocolo Diffie-Hellman.

No Capítulo 2, abordaremos a evolução da criptografia de forma breve, e o protocolo de troca de chaves de Diffie-Hellman, descrevendo o algoritmo e sua interpretação através da utilização dos Logaritmos Discretos.

No último capítulo, propomos três atividades relacionadas a troca de chaves de Diffie-Hellman, uma para o Ensino Fundamental, uma para o Ensino Médio e uma para o Ensino Superior, respectivamente.

1 RESULTADOS DA TEORIA DOS NÚMEROS

O protocolo de troca de chaves de Diffie-Hellman está diretamente relacionado ao problema do logaritmo discreto no grupo dos inteiros invertíveis módulo p, para a compreensão do qual se faz necessário o conhecimento de elementos da teoria dos números, por isso, iniciaremos nosso trabalho abordando definições e teoremas que constituirão a base para o entendimento do protocolo que será abordado nos capítulos seguintes. Para a elaboração deste capítulo foram utilizadas as referências (GONÇALVES, 1979) , (FILHO, 1981), (FALEIROS, 2011), (SANTOS, 2010), (NASCIMENTO; FEITOSA, 2013) e (SILVA; JURIAANS, 2010).

1.1 DIVISIBILIDADE

Algumas definições e propriedades da divisibilidade possuem grande importância para a compreensão de outros conceitos que servem de base para o protocolo do qual trata este trabalho. Essas definições e propriedades serão apresentadas a seguir.

Definição 1.1.1. *Sejam a e b inteiros, dizemos que a divide b, $(a \neq 0)$ denotado por $a \mid b$, se existir um inteiro c tal que $b = ac$.*

Se a não divide b denotamos por $a \nmid b$.

Listamos algumas propriedades de divisibilidade que serão utilizadas posteriormente.

Proposição 1.1.1. *Sendo a, b e c inteiros $(a \neq 0)$, se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$ então existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ temos $c = k_2 k_1 a$ o que implica que $a \mid c$. ■

Exemplo 1.1.1. *Se $5 \mid 10$ e $10 \mid 50$, então $5 \mid 50$. Como não existe um número inteiro c satisfazendo $12 = 5c$ então $5 \nmid 12$.*

Proposição 1.1.2. *Sendo a, b, c, m e n inteiros e $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração: Se $c \mid a$ e $c \mid b$ então $a = k_1 c$ e $b = k_2 c$. Ao multiplicarmos essas duas equações por m e n respectivamente, teremos $ma = mk_1 c$ e $nb = nk_2 c$. Somando-se membro a membro obtemos $ma + nb = (mk_1 + nk_2)c$, o que implica que $c \mid (ma + nb)$. ■

Exemplo 1.1.2. *Como* $5 \mid 10$ *e* $5 \mid 15$*, então* $5 \mid (3 \times 10 + 4 \times 15)$.

Teorema 1.1.1. *Dados a, n e d inteiros, temos as seguintes propriedades:*

i. $n \mid n$;

ii. $d \mid n \;\Rightarrow\; ad \mid an$;

iii. $ad \mid an \quad e \quad a \neq 0 \Rightarrow d \mid n$;

iv. $1 \mid n$;

v. $n \mid 0$;

vi. $d \mid n \quad e \quad n \neq 0 \;\Rightarrow |d| \leq |n|$;

vii. $d \mid n \quad e \quad n \mid d \;\Rightarrow |d| = |n|$;

viii. $d \mid n \quad e \quad n \neq 0 \;\Rightarrow (n/d) \mid n$.

Demonstração: *(i)* Como $n = 1.n$ por definição segue que $n|n$, inclusive para $n = 0$.*(ii)* se $d|n$, então $n = c.d$ para algum inteiro c, logo $an = c.ad$, o que implica que $ad|an$.*(viii)* Se $d \mid n$ então $n = k_1 d$ e portanto n/d é um inteiro. Como $(n/d).d = n$ segue da definição que $(n/d) \mid n$. As demais demonstrações são consequências imediatas da definição. ■

Teorema 1.1.2. *Sejam a, b, c inteiros:*

i. Se $a \mid b$ *e* $a \mid c$*, então* $a \mid (b + c)$;

ii. Se $a \mid b$*, então* $a \mid bc$;

iii. Se $a \mid b$ *e* $a \mid c$*, então* $a \mid (rb + sc)$*, para todos r, s inteiros;*

iv. Se $a \mid b$ *e* $b > 0$*, então* $a \leq b$;

v. Se $ab = 1$*, então* $a = 1$ *ou* $a = -1$;

vi. Se $a \mid b$ *e* $b \mid a$*, então* $a = b$ *ou* $a = -b$;

vii. Se $ab \mid ac$ *e* $a \neq 0$*, então* $b \mid c$;

viii. Se $0 < a < b$*, então* $b \nmid a$.

Demonstração: (i) Se $a \mid b$ e $a \mid c$, então existem d, e inteiros, tais que $b = da$ e $c = ea$. Logo, $b+c = da+ea = (d+e)a$ e, portanto, $a \mid (b+c)$; **(ii)** Se $a \mid b$, então existe d inteiro tal que $b = ad$. Logo, $bc = adc$ e portanto, $a \mid bc$; **(iii)** Se $a \mid b$ e $a \mid c$, então por (ii), $a \mid rb$ e $a \mid sc$, para quaisquer r e s inteiros. Logo, por (i), $a \mid (rb+sc)$; **(iv)** Como $a \mid b$, então $b = ac$, para algum c inteiro. Se $a < 0$, como $0 < b$ então $a < b$. Se $a > 0$, como $b > 0$, então $c > 0$. Logo $c \geq 1$ e, portanto, $b = ac \geq a.1 = a$; **(v)** Se $a > 0$, como $ab = 1$, então, por definição, $a \mid 1$. Logo, por (iv), $a \leq 1$, isto é, $0 < a \leq 1$ e, portanto, $a = 1$. Se $a < 0$, então $-a > 0$. Como $(-a)(-b) = ab = 1$, do mesmo modo, temos $-a = 1$ e, portanto, $a = -1$.

■

1.2 ALGORITMO DA DIVISÃO DE EUCLIDES

Nesta seção, apresentaremos o algoritmo da divisão de Euclides, um dos resultados mais importantes da teoria dos números, no qual muitas outras definições são baseadas, entre elas as que norteiam este trabalho.

Teorema 1.2.1. *Dados dois inteiros n e d, $d > 0$, existe um único par de inteiros q e r, tais que: $n = qd + r$, com $0 \leq r < d$, onde q é chamado de quociente e r de resto da divisão de n por d.*

Demonstração: (Existência) Considerando inicialmente $n \geq 0$, demonstraremos por indução e pelo princípio da indução finita (PIF). Para $n = 0$, temos que $n = 0 \cdot d + 0$ e, portanto $q = 0 = r$. Pela hipótese de indução, consideremos que dado $n > 0$, o enunciado é válido para todo natural m com $m < n$. Entretanto, se $n \geq d$, como $n \geq d > 0$, então $n > n - d \geq 0$. Pela hipótese de indução, $n - d = qd + r$, com q, r inteiros positivos e $0 \leq r < d$. Sendo assim, $n = n - d + d = qd + r + d = (q+1)d + r$, ou seja, o algoritmo vale para n. Desta forma, pelo PIF, fica provada a existência de q e r para $n \geq 0$. Agora considerando o caso $n < 0$. Sendo assim, $-n > 0$ e portanto, $-n = qd + r$, com $0 \leq r < d$. Logo, $n = (-q) - r$. Se $r = 0$, então $n = (-q)d + r$. Se $r > 0$, então $n = (-q)d - d + d - r = (-q-1)d + (d-r)$ e $0 \leq d - r < d$. **(Unicidade)** Seja $n = qd + r$ e $n = q'd + r'$, com q, q' inteiros e r e r' inteiros positivos com $0 \leq r$, $r' < d$. Supondo, sem perda de generalidade, que $r' < r$. Nesse caso, $0 \leq r - r' = n - qd - (n - q'd) = (q' - q)d$, ou seja, $d \mid (r - r')$. Entretanto, $0 \leq r - r' < d - r' \leq d$. Assim, $d \mid (r - r')$ e $0 \leq r - r' < d$. Logo pelo item (iv) do Teorema 1.7, $r - r' = 0$, ou seja $r = r'$. Sendo assim, $0 = r - r' = (q - q')d$. Como $d \neq 0$, então $q' - q = 0$ e, portanto, $q = q'$. ■

Exemplo 1.2.1. *Temos que $25 = 4 \cdot 6 + 1$ e $-25 = (-5) \cdot 6 + 5$, ou seja, o resto da divisão de 25 por 6 é 1 e resto da divisão de -25 por 6 é 5.*

Corolário 1.2.1. *Dados os números inteiros n e d, com $d>0$, então $d \mid n$ se, e somente se, o resto da divisão de n por d é zero.*

Demonstração: ($\Rightarrow$) Se $d \mid n$, então existe q inteiro tal que $n = q.d = q.d+0$. Sendo assim, o resto da divisão de n por d é zero. ($\Leftarrow$) Pelo algoritmo da divisão, existem e são únicos q, r inteiros, com $0 \leq r < d$ tais que $n = qd+r$. Como, por hipótese, $r = 0$, então, $n = qd$ ou seja, $d \mid n$.

■

Exemplo 1.2.2. *O inteiro $7 \nmid 23$, pois $23 = 3 \cdot 7 + 2$, ou seja, o resto da divisão de 23 por 7 é 2.*

1.3 MÁXIMO DIVISOR COMUM - MDC

Sejam a e b inteiros com pelo menos um deles diferente de zero, o *máximo divisor comum* de a e b, denotado por $mdc(a,b)$, é o inteiro positivo d tal que:

i. $d \mid a$ e $d \mid b$;

ii. se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

A condição (i) afirma que d é um divisor de a e b e a condição (ii) garante que d é o maior divisor comum para a e b e também a unicidade do máximo divisor comum, pois se d e d' são máximos divisores comuns de a e b, então $d \mid d'$ e $d' \mid d$, desta forma, pelo Teorema 1.1.2, $d = d'$.

Teorema 1.3.1. ***(Teorema de Bézout-Bachet)*** *Seja d o máximo divisor comum de a e b, então existem n_0 e m_0 inteiros tais que $d = n_0 a + m_0 b$.*

Demonstração: Sendo B o conjunto de todas as combinações lineares $\{na+mb \mid n,m \in \mathbb{Z}\}$. Percebe-se, de forma clara, que este conjunto contém números positivos, números negativos e o zero. Escolhendo-se n_0 e m_0 de forma que $c = n_0 a + m_0 b$ seja o menor inteiro positivo pertencente a B, pois, pelo Princípio da Boa Ordem (PBO), todo conjunto não-vazio de inteiros positivos contém um elemento mínimo. Precisamos provar que $c \mid a$ e $c \mid b$. Por contradição, supomos que $c \nmid a$. Desta forma, pelo Teorema 1.2.1 existem q e r tais que $a = qc+r$, com $0 < r < c$. Portanto $r = a - qc = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$ o que mostra $r \in B$, pois $(1-qn_0)$ e $(-qm_0)$, o que é uma contradição, pois $0 < r < c$ e c é o menor inteiro positivo do conjunto B. Sendo assim $c \mid a$, como queríamos provar. Analogamente se prova que $c \mid b$. Como d é um divisor comum de a e b, existem inteiros k_1 e

k_2 tais que $a = k_1 d$ e $b = k_2 d$ e, portanto $c = n_0 a + m_0 b = n_0 k_1 d + m_0 k_2 d = d(n_0 k_1 + m_0 k_2)$ implicando que $d \mid c$. Pelo Teorema 1.1.1 (vi) temos que $d \leq c$ (ambos são positivos) e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, conclui-se que $d = n_0 a + m_0 b$. ■

Definição 1.3.1. *Os inteiros a e b são relativamente primos quando* $\text{mdc}(a,b) = 1$.

Teorema 1.3.2. *Se $a \mid bc$ e* $\text{mdc}(a,b) = 1$*, então $a \mid c$.*

Demonstração: Como o $\text{mdc}(a,b) = 1$, pelo Teorema 1.3.1 existem inteiros n e m tais que $na + mb = 1$. Multiplicando ambos os membros por c obtemos $n(ac) + m(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ então pela Proposição 1.1.2 $a \mid c$. ■

1.4 NÚMEROS PRIMOS

Definição 1.4.1. *Um número inteiro $n (n > 1)$ é chamado primo se possuir somente dois divisores positivos n e 1.*

Se $n > 1$ não é primo, então n é chamado de composto.

Teorema 1.4.1. ***(Teorema Fundamental da Aritmética)*** *Todo inteiro maior que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há o que demonstrar. Suponhamos pois, n composto. Seja $p_1 (p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. O que é verdade, pois caso contrário, existiria p, $1 < p < p_1$ com $p \mid n$, o que contradiz a escolha de p_1. Sendo assim, $n = p_1 n_1$. Se n_1 for primo, está provado. Caso contrário, tomamos p_2 como o menor divisor de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$. Repetindo este procedimento, obtemos uma sequência decrescentes de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, ..., p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}.$$

Para mostrar a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumindo que ela seja válida para todos os inteiros maiores que 1 e menores do que n, precisamos provar que ela também é valida para n. Se n é primo, não há o que provar. Supondo então que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r.$$

Precisamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1q_2...q_r$, ele divide ao menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica que $p_1 = q_1$. Logo $nqp_1 = p_2...p_s = q_2...q_r$, Como $1 < nqp_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, ou seja, $s = r$ e, a menos da ordem, as fatorações $p_1p_2...p_s$ e $q_1q_2...q_r$ são iguais. ■

Teorema 1.4.2. ***(Euclides)****A sequência dos números primos é infinita.*

Demonstração: Suponhamos que a sequência dos números primos seja finita. Seja $p_1, p_2, ..., p_n$ a lista de todos os primos. Consideremos o número $R = p_1.p_2...p_n + 1$. O número R não é divisível por nenhum dos p_i da lista e é maior que qualquer p_i. Entretanto, pelo Teorema 1.4.1, ou R é primo ou possui algum fator primo, o que implica na existência de um primo que não está na nossa lista. Sendo assim, a sequência de números primos não pode ser finita. ■

1.5 CONGRUÊNCIA

Apresentaremos aqui a definição de congruência bem como algumas de suas proposições, as quais serão de grande relevância para a compreensão do funcionamento do algoritmo de qual trata este trabalho.

Definição 1.5.1. *Sendo a e b inteiros, dizemos que a é congruente a b módulo m com $m > 0$ se $m \mid (a - b)$. Denotamos por $a \equiv b \pmod{m}$.*

Exemplo 1.5.1. $12 \equiv 5 \pmod{7}$*, pois* $7 \mid (12 - 5)$.

Proposição 1.5.1. *Se a e b são inteiros, temos que $a \equiv b \pmod{m}$, se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b \pmod{m}$, então existe $m \mid (a - b)$ o que significa que existe um k tal que $a - b = km$, ou seja, $a = b + km$. A recíproca é trivial porque da existência de um k que satisfaz $a = b + km$, tem-se que $km = a - b$, ou seja, que $m \mid (a - b)$, isto é, $a \equiv b \pmod{m}$.

■

Proposição 1.5.2. *Sendo a, b, m e d inteiros, com $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a \pmod{m}$;

2. *Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$;

3. *Se* $a \equiv b \pmod{m}$ *e* $b \equiv d \pmod{m}$, *então* $a \equiv d \pmod{m}$.

Demonstração: (1) Como $m \mid 0$, então $m \mid (a-a)$, o que implica que $a \equiv a \pmod{m}$. **(2)** Se $a \equiv b \pmod{m}$, então $a = b + k_1 m$ para algum inteiro k_1. Sendo assim, $b = a - k_1 m$, o que implica, pela Proposição 1.12, $b \equiv a \pmod{m}$. **(3)** Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$ de onde, somando membro a membro as últimas equações, obtém-se $a - d = (k_1 + k_2)m$, o que implica $a \equiv d \pmod{m}$.

■

Esta proposição diz que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois provou-se que ela é reflexiva, simétrica e transitiva. Os resultados a seguir mostram que a congruência respeita a aritmética, isto é, podemos fazer contas e manipular expressões módulo m de forma análoga a que fazemos para inteiros.

Teorema 1.5.1. *Se a, b, c e m são inteiros tais que* $a \equiv b \pmod{m}$, *então*

1. $a + c \equiv b + c \pmod{m}$;

2. $a - c \equiv b - c \pmod{m}$;

3. $ac \equiv bc \pmod{m}$.

Demonstração: (1) Como $a \equiv b \pmod{m}$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \pmod{m}$. **(2)** Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$, temos que $a - c \equiv b - c \pmod{m}$. **(3)** Como $a - b = km$ então $ac - bc = ckm$ o que implica $m|(ac - bc)$ e, portanto $ac \equiv bc \pmod{m}$. ■

Teorema 1.5.2. *Se a, b, c, d e m são inteiros tais que* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então*

1. $a + c \equiv b + d \pmod{m}$;

2. $a - c \equiv b - d \pmod{m}$;

3. $ac \equiv bd \pmod{m}$.

Demonstração: (1) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = km$ e $c - d = k_1 m$. Somando membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$, o que implica $a + c \equiv$

$b+d \pmod m$. **(2)** Subtraindo membro a membro $a-b=km$ e $c-d=k_1m$ obtendo $(a-b)-(c-d)=(a-c)-(b-d)=(k-k_1)m$ que implica $a-c\equiv b-d \pmod m$. **(3)** Multiplicando ambos os lados de $a-b=km$ por c e ambos os lados de $c-d=k_1m$ por b, obtemos $ac-bc=ckm$ e $bc-bd=ck_1m$. Somando membro a membro as últimas igualdades, obtemos $ac-bc+bc-bd=ac-bd=(ck+bk_1)m$ o que implica $ac\equiv bd \pmod m$.

■

A linguagem de congruência permite fazer certas operações com números muito grandes, obtendo informações sobre eles sem precisar calcular o número em si, isto permite que a congruência seja utilizada na criptografia, como no protocolo de troca de chaves apresentado neste trabalho.

Exemplo 1.5.2. *Calculemos o resto da divisão de* 3^{243} *por* 5. *Observe que*

$$3^{243}=3^{242}\times 3=3^{2\times 121}\times 3=(3^2)^{121}\times 3=9^{121}\times 3$$

Como $9\equiv -1 \pmod 5$, *temos que,* $9^{121}\equiv(-1)^{121}\equiv -1 \pmod 5$. *Portanto*

$$3^{243}\equiv 9^{121}\times 3\equiv(-1)\times 3\equiv 2 \pmod 5.$$

Portanto, o resto da divisão de 3^{243} *por* 5 *é* 2. *O número* 3^{243} *tem mais de* 100 *dígitos, sendo impraticável qualquer manipulação manual de tal número ou mesmo com o auxílio de calculadoras.*

Definição 1.5.2. *Se* h *e* k *são dois inteiros com* $h\equiv k \pmod m$, *dizemos que* k *é um resíduo de* h *módulo* m.

Definição 1.5.3. *O conjunto dos inteiros* $\{r_1,r_2,...,r_s\}$ *é um sistema completo de resíduos módulo* m *se:*

1. r_i *não é congruente a* r_j *módulo* m *para* $i\neq j$
2. *para todo inteiro* n *existe* r_i *tal que* $n\equiv r_i \pmod m$

Exemplo 1.5.3. $\{0,1,2,...,m-1\}$ *é um sistema completo de resíduos módulo* m.

Proposição 1.5.3. *Se* a, b, k *e* m *são inteiros com* $a>0$ *e* $a\equiv b \pmod m$ *então* $a^k\equiv b^k \pmod m$.

Demonstração: Segue imediatamente da identidade:

$$a^k-b^k=(a-b).(a^{k-1}+a^{k-2}b+a^{k-3}b^2+...+ab^{k-2}+b^{k-1})$$ ■

Definição 1.5.4. *Uma solução $\bar{a}$ de $ax \equiv 1 \pmod{m}$ é chamada de um inverso de a módulo m.*

Proposição 1.5.4. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p, se, e somente se, $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.*

Demonstração: Se a é seu próprio inverso, então $a^2 \equiv 1 \pmod{p}$, o que significa que $p \mid (a^2 - 1)$. Mas se $p \mid (a-1)(a+1)$, sendo p primo, $p \mid (a-1)$ ou $p \mid (a+1)$, o que implica que $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$. A recíproca é imediata pois, se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, então $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto $p \mid (a-1)(a+1)$ o que significa que $a^2 \equiv 1 \pmod{p}$ concluindo assim a demostração. ■

Teorema 1.5.3. ***(Pequeno Teorema de Fermat)*** *Seja p primo, se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração: Sabendo que o conjunto formado pelos p números $0, 1, 2, ..., p-1$ constitui um sistema completo de resíduos módulo p, significando que qualquer conjunto contendo no máximo p elementos não congruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto $\{0, 1, 2, ..., p-1\}$. Considerando agora os números $a, 2a, 3a, ..., (p-1)a$, como o mdc $(a, p) = 1$, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles não são congruentes módulo p, pois $aj \equiv ak \pmod{p}$ implica $j \equiv k \pmod{p}$, o que só é possível se $j = k$, pois j e k são ambos positivos e menores que p. Sendo assim, temos um conjunto de $p-1$ elementos que não são congruentes módulo p e não são divisíveis por p. Desta forma, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, ..., p-1$. Multiplicando essas congruências membro a membro, temos:

$$a(2a)(3a)...(p-1)a \equiv 1.2.3...(p-1) \pmod{p}$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Entretanto, como o mdc de $(p-1)!$ e p é igual a 1, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo:

$$a^{p-1} \equiv 1 \pmod{p},$$

como queríamos demonstrar. ■

Corolário 1.5.1. *Se p é um número primo e a é um inteiro positivo, então $a^p \equiv a \pmod{p}$.*

Demonstração: É preciso analisar dois casos, se $p \mid a$ e se $p \nmid a$. Se $p \mid a$, então $p \mid (a(a^{p-1}-1))$ e, portanto, $a^p \equiv a \pmod{p}$. Se $p \nmid a$, pelo Pequeno Teorema de Fermat $p \mid (a^{p-1}-1)$ e, portanto, $p \mid (a^p - a)$ o que significa que em ambos os casos $a^p \equiv a \pmod{p}$. ■

Definição 1.5.5. *Se n é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(n)$ é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Definição 1.5.6. *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, r_3, ...r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então r_i não é congruente a r_j módulo m. Além disso, dado um inteiro n coprimo com m, existe algum $i \in \{1, \ldots, \phi(m)\}$ tal que $r_i \equiv n \pmod{m}$.*

Exemplo 1.5.4. *O conjunto $\{0,1,2,3,4,5\}$ é um sistema completo de resíduos módulo 6. Sendo assim, $\{1,5\}$ é um sistema reduzido de resíduos módulo 6. Para se obter um sistema reduzido de resíduos de um sistema completo módulo m, deve-se retirar os elementos do sistema completo que não são relativamente primos com m.*

Teorema 1.5.4. *Seja a um inteiro positivo tal que o mdc $(a,m) = 1$. Se $r_1, r_2, ..., r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, ..., ar_{\phi(m)}$ também é um sistema reduzido de resíduos módulo m.*

Demonstração: Como temos $\phi(m)$ elementos na sequência $ar_1, ar_2, ..., ar_{\phi(m)}$, temos que mostrar que todos eles são relativamente primos com m e, dois a dois, não congruentes módulo m. Como mdc $(a,1) = 1$ e mdc $(r_i, m) = 1$, temos que o mdc $(ar_i, m) = 1$. Sendo assim, temos que mostrar que ar_i não é congruente a ar_j módulo m se $i \neq j$. Mas como o mdc $(a,m) = 1$, de $ar_i \equiv ar_j \pmod{m}$ temos $r_i \equiv r_j \pmod{m}$, o que implica $i = j$, uma vez que $r_1, r_2, ..., r_{\phi(m)}$, é um sistema reduzido de resíduos módulo m, concluindo assim a demonstração. ■

Teorema 1.5.5. ***(Euler)*** *Se m é um inteiro positivo e a um inteiro com mdc $(a,m) = 1$, então:*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demonstração: Pelo Teorema 1.5.4 podemos concluir que ar_i é congruente a exatamente um dos r_j, com $1 \leq j \leq \phi(m)$, e, portanto, o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é:

$$ar_1.ar_2...ar_{\phi(m)} \equiv r_1.r_2...r_{\phi(m)} \pmod{m}, \text{ ou seja,}$$

$$a^{\phi(m)}r_1.r_2...r_{\phi(m)} \equiv r_1.r_2...r_{\phi(m)} \pmod{m}.$$

Como

$$\text{mdc}\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$$

podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados e obtemos $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

1.6 GRUPOS

A definição de grupos está relacionada à noção de operação binária que é qualquer função:

$$* : G \times G \longrightarrow G.$$

A notação de operação binária é: $*(a,b) = a*b$, ab, $a \times b$ ou $a+b$ e assim por diante, a qual é chamada de produto ou de soma, dependo da notação escolhida.

Diz-se que o par $(G,*)$ no qual G é um conjunto não vazio onde está definida uma operação binária $*$, é um *grupo* se são válidas as seguintes propriedades:

1. Associatividade,
$$a*(b*c) = (a*b)*c, \forall a,b,c \in G.$$
2. Existe $e \in G$ tal que
$$a*e = e*a = a, \forall a \in G.$$
3. Para cada $a \in G$, existe $b \in G$ tal que
$$a*b = b*a = e.$$

Exemplos:

1. $\mathbb{Z}$ é um grupo aditivo infinito.
2. Se $n \geq 1$ é um número inteiro, então o conjunto $\mathbb{Z}_n$ dos inteiros módulo n, é um grupo aditivo que contém exatamente n elementos.

3. $\mathbb{Z}_n^*$ é um grupo, com a multiplicação, finito de tamanho $\phi(n)$ pelo teorema de Euler. Em particular se $n = p$, $\mathbb{Z}_n^* = \{1, ..., p-1\}$, com p primo.

Definição 1.6.1. *Sendo G um grupo, diz-se que um subconjunto não vazio H de G é um subgrupo de G, em símbolos $H \leq G$, quando H munido com a operação binária induzida por G for um grupo.*

Proposição 1.6.1. ***(Critério de Subgrupo)*** *Sejam G um grupo e H um subconjunto não vazio de G. Então H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas:*

1. *$e_G \in H$ com e_G o elemento identidade de G.*
2. *Se $a, b \in H$, então $ab \in H$ (isto é, $HH \subseteq H$). (fechamento)*
3. *Se $a \in H$, então $a^{-1} \in H$ (isto é, $H^{-1} \subseteq H$). (existência de inverso)*

Demonstração: Suponhamos que H seja um subgrupo de G. Seja f o elemento identidade de H. Temos que provar que $e_G = f$. Como $f^2 = f$ e $f \in G$ temos que

$$e_G = f^{-1}f = f^{-1}(f^2) = (f^{-1}f) = e_G f = f.$$

Sendo assim, as condições (1), (2) e (3) são claras.

De forma recíproca, dados a, b e $c \in H$, temos que $a(bc) = (ab)c$, pois $a, b, c \in G$. Logo, pela condição (2), obtemos $a(bc) = (ab)c$ em H. Finalmente, dado $a \in H$, temos, pela condição (3), que $a^{-1} \in H$. Sendo assim, pela condição (2),

$$e = aa^{-1} = a^{-1}a \in H.$$

Portanto, H é um *subgrupo* de G. ■

Proposição 1.6.2. *Seja G um grupo e S um subconjunto não vazio qualquer de G. Então*

$$\langle S \rangle = \left\{ a_1 a_2 \cdots a_n : n \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S \right\}$$

é um subgrupo de G. Além disso, $\langle S \rangle$ é o menor subgrupo de G contendo S.

Em particular, se $S = \{a\}$, então

$$\langle S \rangle = \langle \{a\} \rangle = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Demonstração: Seja

$$L = \left\{a_1 a_2 \cdots a_m : m \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S\right\}.$$

$$= \left\{a_1^{t_1} a_2^{t_2} \cdots a_n^{t_n} : n \in \mathbb{N}, a_i \in S \text{ e } t_i \in \{-1, 1\}\right\}$$

$$= \left\{a_1^{t_1} a_2^{t_2} \cdots a_n^{t_n} : n \in \mathbb{N}, a_i \in S \text{ e } t_i \in \mathbb{Z}\right\}.$$

Então $S \subseteq L$ e $e \in L$, pois $e = aa^{-1}$, para todo $a \in S$. Se $x, y \in L$, então existem $m, n \in \mathbb{N}$ tais que

$$x = a_1 a_2 \cdots a_m, a_i \in S \text{ ou } a_i^{-1} \in S,$$

e

$$y = b_1 b_2 \cdots b_n, b_j \in S \text{ ou } b_j^{-1} \in S.$$

Logo,

$$xy^{-1} = a_1 a_2 \cdots a_m b_n^{-1} b_{n-1}^{-1} \cdots b_1^{-1}, (a_i \in S \text{ ou } a_i^{-1} \in S) \text{ e } (b_j \in S \text{ ou } b_j^{-1} \in S).$$

Assim, $xy^{-1} \in L$. Portanto L é um subgrupo de G. Finalmente, seja K qualquer subgrupo de G tal que $S \subseteq K$. Então

$$a_1 a_2 \cdots a_n \in K \text{ com } n \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S.$$

Logo, $L \subseteq K$. Portanto L é o menor subgrupo de G contendo S. Assim, $L \subseteq \langle S \rangle$. Como $S \subseteq L$ temos que $\langle S \rangle \subseteq L$, isto é, $L = \langle S \rangle$. ■

1.7 GRUPOS CÍCLICOS

Seja G um grupo, diz-se que G é um *grupo cíclico* se existir $a \in G$ tal que $G = \langle a \rangle$, isto é:

$$G = \{a^m \mid m \in \mathbb{Z}\}.$$

Exemplo 1.7.1. *O grupo $(\mathbb{Z}_n, +)$ é cíclico, pois temos $\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\} = \langle 1 \rangle$*

Em geral, $(\mathbb{Z}_n^*, \cdot)$ não é cíclico, o que será discutido na seção a seguir.

Proposição 1.7.1. *Seja G um grupo, então:*

1. *Se $a \in G$ tem ordem finita $m > 0$, então $a^n = e$ se, e somente se, m divide n.* [1]
2. *Se $G = \langle a \rangle$ é um grupo cíclico de ordem finita $m > 0$, então $G = \langle a^k \rangle$ se, e somente se,* $\text{mdc}(m, k) = 1$.

[1] Para a definição dos conceitos de Grupos Cíclicos utilizamos (SILVA; JURIAANS, 2010), porém observamos uma imprecisão no item 1 da Proposição 1.7.1

3. *Se $G = \langle a \rangle$ é um grupo cíclico de ordem finita $m > 0$, então para cada $d \in \mathbb{N}$ tal que d divide m, existe um único subgrupo H de G com ordem d. Neste caso,*

$$H = \langle a^k \rangle$$

com $m = dk$.

Demonstração: (2) Suponhamos que $G = \langle a \rangle$. Como $a \in G$, temos que existe $r \in \mathbb{Z}$ tal que $a = (a^k)^r = a^{kr}$. Logo,

$$a^{kr-1} = a^{kr}a^{-1} = aa^{-1} = e.$$

Assim, pelo item (1), $kr - 1 = sm$, para algum $s \in \mathbb{Z}$. Portanto,

$$kr + (-s)m = 1,$$

isto é, $\text{mdc}(m, k) = 1$. Reciprocamente, suponhamos que $\text{mdc}(m, k) = 1$. Então existem $r, s \in \mathbb{Z}$ tais que

$$kr + sm = 1.$$

Logo,

$$a = a^1 = a^{kr+sm} = a^{kr}a^{sm} = \left(a^k\right)^r (a^m)^s = \left(a^k\right)^r \in \langle a^k \rangle.$$

Portanto, $G \subseteq \langle a^k \rangle$, ou seja, $G = \langle a^k \rangle$.

(3) Se $m = kd$, então $H = \langle a^k \rangle$ tem ordem $d = \frac{m}{k}$. De fato, seja $l = |H|$. Então

$$a^{kl} = \left(a^k\right)^l = e \Rightarrow m \mid kl \Rightarrow kd \mid kl \Rightarrow d \mid l \Rightarrow d \leq l.$$

Por outro lado,

$$e = a^m = a^{kd} = \left(a^k\right)^d \Rightarrow l \mid d \Rightarrow l \leq d.$$

Portanto, $l = d$. Seja K um subgrupo qualquer de G de ordem d, então $K = \langle a^n \rangle$, para algum $n \in \mathbb{Z}$. Logo,

$$e = (a^n)^d = a^{nd} \Rightarrow m \mid nd \Rightarrow kd \mid nd \Rightarrow k = n.$$

Assim, existe $r \in \mathbb{Z}$ tal que $n = rk$. Portanto,

$$a^n = a^{rk} = (a^k)^r \in H,$$

isto é, $k \subseteq H$. Como $|H| = |K|$ e $K \subseteq H$ temos que $K = H$.

■

1.8 LOGARITMOS DISCRETOS

O protocolo tratado neste trabalho está diretamente relacionado à ideia de logaritmo discreto , desta forma, abordaremos conceitos importantes para sua compreensão.

Para chegarmos ao conceito de logaritmos discretos é importante apresentarmos as definições de *ordem* e *raiz primitiva*.

Sejam a e $n > 1$ números inteiros tais que o $mdc(a, n) = 1$, chama-se *ordem* de a (mod n) ao menor inteiro positivo k tal que

$$a^k \equiv 1 \pmod{n},$$

ou seja, k é a ordem de a no grupo $\mathbb{Z}_n^*$

A *Raiz primitiva* de um inteiro positivo n é um inteiro a tal que o $mdc(a, n) = 1$ e a ordem de a módulo n é $\phi(n)$, ou seja,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

e a^k não seja congruente a 1 módulo n para todo inteiro positivo $k < \phi(n)$. Isso implica que a raiz primitiva a é um gerador para $\mathbb{Z}_n^*$. Pelo teorema de Euler, $a^{\phi(n)} = 1 \pmod{n}$, para a e n coprimos. No entanto, o $\phi(n)$ não é necessariamente o menor número satisfazendo tal propriedade, como veremos nos exemplos a seguir.

Exemplo 1.8.1. *3 é raiz primitiva de 7, pois* $mdc(3, 7) = 1$ *e a ordem de 3 módulo 7 é* $\phi(n) = 6$. *Observe:*

$$\begin{aligned} 3^1 &\equiv 3 \pmod{7} \\ 3^2 &\equiv 2 \pmod{7} \\ 3^3 &\equiv 6 \pmod{7} \\ 3^4 &\equiv 4 \pmod{7} \\ 3^5 &\equiv 5 \pmod{7} \\ 3^6 &\equiv 1 \pmod{7} \end{aligned}$$

Entretanto, 6 não é raiz primitiva pois sua ordem é 2. Além disso, para determinados módulos não existe nenhuma raiz primitiva, como para o grupo dos invertíveis módulo 8. Veja que $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ e $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$, portanto a ordem de todos os elementos de $\mathbb{Z}_8^*$ é 2, logo, nenhum tem ordem $4 = |\mathbb{Z}_8^*|$. O teorema a seguir classifica quais inteiros admitem raízes primitivas, sua demonstração foi omitida por fugir do objetivo desse texto, mas destacamos que usaremos apenas o caso em que m é um número primo p. A referida demonstração encontra-se em (SANTOS, 2010).

Teorema 1.8.1. *Se* $m \geq 1$ *não é da forma* $1, 2, 4, p^t$ *e* $2p^t$ *com p primo ímpar, m não possui raiz primitiva.*

Consideremos então uma *raiz primitiva* a para algum número primo p. Sabemos que as potências de a de 1 até $(p-1)$ produzem cada inteiro 1 até $(p-1)$ exatamente uma vez. Sabemos também que, qualquer número inteiro b satisfaz

$$b \equiv r \pmod{p}$$

para algum r, onde $0 \leq r \leq (p-1)$, pela definição de aritmética modular. Sendo assim, para qualquer inteiro b e uma raiz primitiva a de um número primo p, podemos encontrar um expoente único i, tal que :

$$b \equiv a^i \pmod{p}$$

onde $0 \leq i \leq (p-1)$. Vejamos tais expoentes para $p = 7$ e $a = 3$.

Exemplo 1.8.2. *Usando o módulo primo $n = 7$. $\phi(n) = 6$ e $a = 3$ sendo a raiz primitiva, temos as diversas potências de a, como visto no exemplo anterior, o que nos fornece os números com determinados logaritmos discretos* (mod 7) *para a raiz $a = 3$, como dispostos na Tabela 1.1.*

Tabela 1.1 – Logaritmos discretos módulo 7

n	1	2	3	4	5	6
$\text{dlog}_{3,7}(n)$	0	2	1	4	5	3

Fonte: Produção própria

Definição 1.8.1. *Dados $a, b \in \mathbb{Z}_p^*$, o logaritmo discreto de b na base a módulo p é o inteiro n, $0 \leq n \leq p-1$ para o qual $a^n \equiv b \pmod{p}$, ou seja,*

$$log_a b \pmod{p} = n \Leftrightarrow a^n \equiv b \pmod{p}.$$

Teorema 1.8.2. *Se a base do logaritmo discreto for uma raiz primitiva de $\mathbb{Z}_p^*$, então o logaritmo discreto de qualquer elemento de $\mathbb{Z}_p^*$ existe.*

Demonstração: Dados $a, b \in \mathbb{Z}_p^*$, como a é uma raiz primitiva de $\mathbb{Z}_p^*$ temos, pela definição anterior, que $\exists n \in \mathbb{Z}$ tal que $b \equiv a^n \pmod{p}$ ou seja, $\text{dlog}_{a,p} b = n$ ■

Os logaritmos discretos únicos (mod m) em alguma base a só existem se a for uma raiz primitiva de m.

Consideremos agora a equação a seguir

$$y = g^x \pmod{p}.$$

Dados g, x, e p, é simples calcular y. Porém, dados y, g e p, encontrar $x = \text{dlog}_{g,p}(y)$ é, em geral, mais custoso computacionalmente, ou seja requer muitos cálculos, sobretudo quando os demais números são grandes.

2 PROTOCOLO DIFFIE-HELLMAN

Neste capítulo, apresentaremos o conceito básico de criptografia e mostraremos os modelos utilizados atualmente, destacando o problema da troca segura de chaves e a solução proposta por Diffie-Hellman, oferecendo dados que possibilitem ao professor de Matemática fazer uso deste assunto do Ensino Básico ao Ensino Superior. As referências utilizadas na elaboração deste capítulo foram: (COSTA; M., 2010), (FIARRESGA, 2010), (STALLINGS, 2015) e (OLIVEIRA, 2012).

2.1 CRIPTOGRAFIA

A criptografia consiste em codificar uma mensagem de forma que somente o destinatário seja capaz de compreendê-la. Para que isso ocorra, é necessário que a mensagem seja modificada de alguma forma, usando uma técnica combinada entre quem envia e quem recebe a mesma, de forma que somente o receptor possa recuperar, obtendo o texto original da mensagem modificada pelo emissor. Dessa forma, a princípio, não haverá revelação da mensagem, caso esta seja interceptada durante o percurso até seu destinatário. Sendo assim, o objetivo básico da criptografia é a segurança da informação.(COSTA; M., 2010)

Há muitos anos são usadas técnicas para manter uma mensagem oculta e transmiti-la de forma secreta. A partir do surgimento da escrita, surgiu também a necessidade de se transmitir mensagens confidenciais, que apenas emissor e receptor compreendessem, fosse por segredos políticos, religiosos, militares, comerciais ou sentimentais. Na Antiguidade foram desenvolvidos dois métodos de ocultar mensagens de um possível interceptador ou espião. O primeiro consistia em esconder a mensagem propriamente dita, técnica chamada de esteganografia. Nesta técnica, a mensagem não sofria alteração, sendo assim, ela não podia ser interceptada, pois poderia ser facilmente decifrada. O segundo método usou processos elaborados em que a mensagem, mesmo tornada pública, não seria entendida pelo interceptador, uma vez que a chave era desconhecida para a leitura, era o surgimento da criptografia. Desde que surgiu, a criptografia utiliza duas técnicas fundamentais: a transposição e a substituição (COSTA; M., 2010). A transposição pode ser observada no scytale ou bastão de Licurgo, que os espartanos usavam por volta do século V a.C, para transmitir mensagens confidenciais.

Neste bastão, era enrolada uma tira de couro ou papiro, na qual estava escrita uma mensagem no sentido do seu comprimento, desenrolava-se a tira e transportava como um cinto, com as letras voltadas para dentro, por um mensageiro até ao destinatário, este então enrolava a tira num bastão de igual diâmetro ao do remetente e ficava conhecedor

Figura 2.1 – Scytale

Fonte: https://aircampgames.com/cryptological-systems-from-history/

da importante informação. Desta forma, as mensagens secretas dos governantes e generais de Esparta eram trocadas com segurança.(FIARRESGA, 2010)

A técnica de substituição foi utilizada pelo imperador Júlio César em sua cifra, na qual letras do alfabeto resultam do avanço da ordem das letras do alfabeto por uma quantidade fixa k de vezes, voltando ao início do alfabeto após a letra Z. Na tabela a seguir ilustramos a posição de cada letra quando $k = 3$.

Tabela 2.1 – Cifra de César

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

Fonte: Produção própria

Baseando-se na definição de aritmética modular, podemos expressar a cifra de César através de um algoritmo, para isso atribuímos um equivalente numérico para cada letra do alfabeto a = 0, b =1, ..., z = 25, como segue na tabela:

Tabela 2.2 – Equivalente numérico de cada letra

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Produção própria

Para cada letra no texto original, chamado de p, denotado aqui por p, iremos substitui-la pela letra do texto cifrado, que podemos chamar de C.

Ao aplicar a notação da aritmética modular, obtemos:

$$C \equiv (p+3) \pmod{26}$$

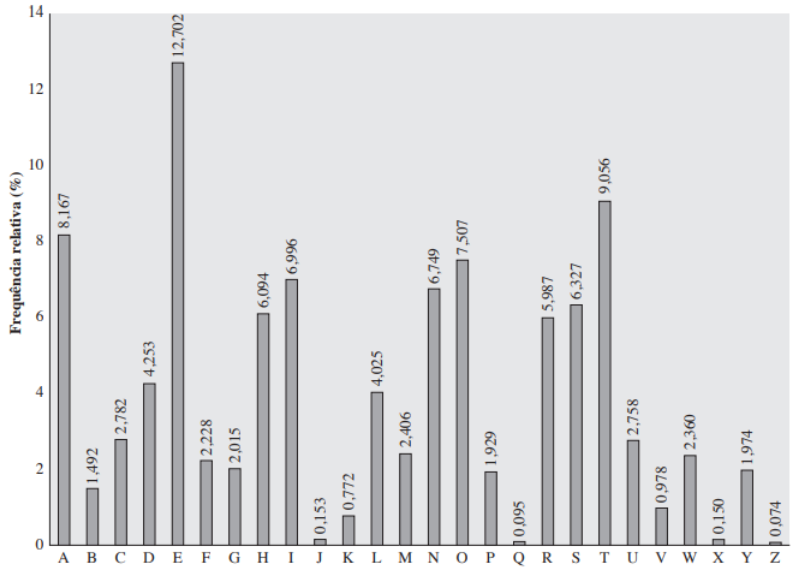
César deslocava as letras em três casas, no caso geral, como mencionamos, esse deslocamento pode ser de qualquer quantidade fixo k. Sendo assim, o algoritmo de César pode ser representado por:

$$C \equiv (p+k) \pmod{26}, \text{ com } k \in \mathbb{Z} \text{ fixo e } 1 \leq k \leq 25$$

Para decodificar o texto é preciso realizar a operação $C \mapsto C-k \pmod{25}$. Pode-se também fazer no máximo, 25 tentativas, já que a possibilidade do texto original é excluída, ou seja, quando k = 0. Essa última forma de decodificação é chamada por (STALLINGS, 2015) de "força bruta".

Por ser monoalfabética, ou seja, usar uma substituição fixa na mensagem inteira, essa cifra é considerada fácil de ser quebrada por apresentar dados de frequência do alfabeto original, pois como bem afirma (STALLINGS, 2015), alguém que intercepte a mensagem sabendo da natureza do texto claro (texto em inglês não compactado, por exemplo) poderá investigar a regularidade da linguagem. Para isso, pode inicialmente determinar e comparar a frequência relativa das letras com uma distribuição padrão para o inglês, como vemos na figura abaixo.

Figura 2.2 – Frequência relativa de letras no texto em inglês



Fonte: Stallings, 2015

Para (STALLINGS, 2015) uma forma de melhorar a técnica monoalfabética é utilizar diferentes substituições monoalfabéticas enquanto se prossegue pela mensagem do texto claro. Essa técnica é chamada de cifra por substituição polialfabética.

Como a cifra de César utiliza apenas 25 chaves possíveis, pode-se dizer que não se trata de uma cifra segura. Entretanto, isso pode ser modificado ao se permitir uma substituição arbitrária, pois uma dificuldade extra de uma cifra por permutação arbitrária é a transmissão e o armazenamento da chave. Enquanto na cifra de César a chave era apenas um número $1 \leq k \leq 25$, na permutação arbitrária é necessário que a chave compartilhada seja a permutação toda, ou seja, uma tabela com a substituição de todas as letras. Muitas das criptografias avançadas até pouco tempo atrás usavam permutações de letras, como por exemplo a realizada na máquina enigma, no entanto a permutação das letras trocava em cada posição, fazendo com que ela deixasse de ser monoalfabética.

Outra cifra bastante conhecida, sendo essa polialfabética, é a cifra de Vigenère. Nesse esquema o conjunto de regras de substituição monoalfabética consiste nas 26 cifras de César, com deslocamentos de 0 a 25 e cada cifra é indicada por uma letra da chave, que é a letra do texto cifrado que substitui a letra do texto.

Figura 2.3 – Cifra de Vigenère

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

Fonte: https://aminoapps.com/c/gravityfalls_ptbr/page/blog/cifra-de-vigenere/qxMm_QkcRuwgmaojmp71527a47E6Np8E5B

Considerando uma sequência de letras em texto claro $P = p_0, p_1, p_2, ..., p_{n-1}$ e uma chave que consiste na sequência de letra $K = k_0, k_1, k_2, ..., k_{m-1}$ em que normalmente $m < n$. A sequência de letras no texto cifrado $C = C_0, C_1, C_2, ..., C_{n-1}$ pode ser calculada

através da equação abaixo

$$C_i = (p_i + k_i \pmod m) \bmod 26$$

Essa cifra se torna forte porque existem múltiplas letras de texto cifrado para cada uma do texto claro, uma para cada letra exclusiva da palavra chave, sendo assim, as informações referentes à frequência das letras ficam ocultas, entretanto, nem todo conhecimento da estrutura do texto claro é perdido (STALLINGS, 2015).

De acordo com (FIARRESGA, 2010), após a Primeira Guerra Mundial, o mundo da criptografia foi revolucionado com a criação da máquina Enigma (**??**) pelo alemão Scherbius. Uma máquina de cifra, utilizada para fins militares pelos alemães, por sua alta complexidade, já que utilizava um número elevado de chaves.

Figura 2.4 – Máquina Enigma

Fonte: https://revistagalileu.globo.com/Sociedade/Historia/noticia/2019/05/maquina-secreta-nazista-para-enviar-mensagens-sera-leiloada.html

Esta máquina é forte não apenas pela quantidade de alfabetos que permite ser usado, 17576 alfabetos de cifra diferentes, mas também no seu número de chaves que é muito grande.

2.1.1 Sistemas Simétricos e Assimétricos

Uma situação típica da criptografia acontece quando duas pessoas, Ana e Beatriz, por exemplo, querem se comunicar através de mensagens, sob o risco da interceptação por uma terceira pessoa, supondo que seja Eva. Ana e Beatriz precisam combinar as chaves que

serão utilizadas durante a troca de mensagens. Na criptografia simétrica a mesma chave usada por Ana para codificar a mensagem, será utilizada por Beatriz para decodificá-la. Mas se Ana e Beatriz estão distantes, não haveria um meio seguro para trocar essa chave. Esta é a principal fragilidade dos algoritmos de chave simétrica.

A distribuição de chaves na encriptação simétrica necessita que dois comunicadores compartilhem, de algum jeito, a chave que foi distribuída para eles e da utilização de um centro de distribuição de chaves. Os matemáticos e criptógrafos Bailey Whitfield Diffie e Martin Edward Hellman que descobriram a encriptação de chave pública, entenderam que o uso de um centro de distribuição de chaves tornava sem efeito a mais importante característica da criptografia, que era assegurar o sigilo total da comunicação.

A encriptação simétrica, também conhecida como encriptação de chave única, é, de acordo com (OLIVEIRA, 2012), o mais antigo modelo de criptografia, no qual a chave, elemento que permite o acesso a mensagem oculta, é igual para as duas partes que se comunicam, devendo esta permanecer em segredo (privada) e era o único tipo utilizado antes da encriptação por chave pública ser desenvolvida na década de 1970. Nesse tipo de sistema, o texto claro, que é a mensagem ou dados originais, serve como entrada do algoritmo de encriptação, que realiza as diversas substituições e transformações no texto claro, possuindo uma chave secreta.

Para que a encriptação simétrica seja segura é necessário um algoritmo de encriptação forte e que emissor e receptor obtenham cópias da chave secreta de forma segura e mantenham-na protegida.

Na encriptação assimétrica são utilizadas duas chaves, uma para encriptar e outra diferente, porém relacionada, para decriptar, uma privada e outra pública, sendo computacionalmente inviável determinar a chave de decriptação conhecendo apenas o algoritmo de criptografia e a chave de encriptação.

Nesse tipo de sistema, o algoritmo de encriptação realiza várias transformações no texto claro através das chaves pública e privada, que é um par de chaves selecionado de modo que se uma for usada na encriptação, a outra é usada na decriptação.

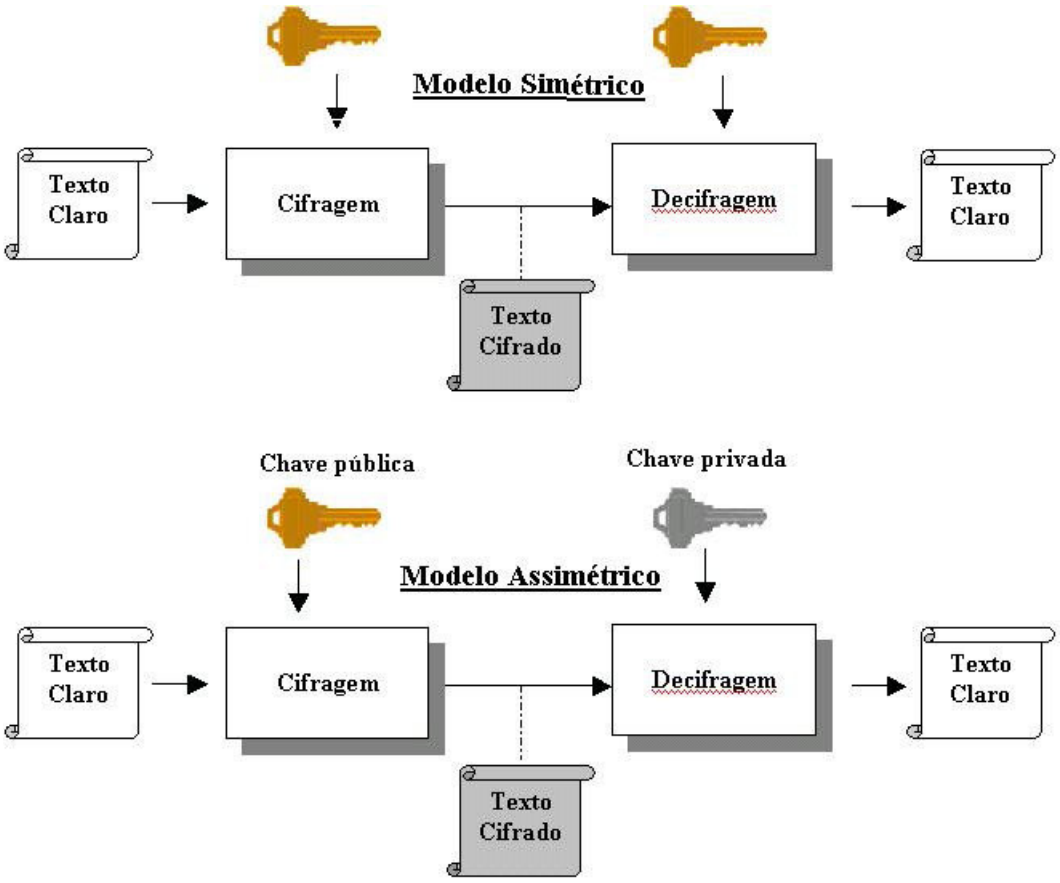
No sistema de encriptação assimétrica, cada usuário gera um par de chaves a ser utilizado para encriptar e decriptar a mensagem. Com essa técnica, todos os participantes têm acesso às chaves públicas. As chaves privadas são geradas localmente por cada participante, e nunca precisarão ser distribuídas, ou seja, a chave pública pode ser disponibilizada para qualquer pessoa que deseja se comunicar com outra de forma segura, mas a chave privada deve ficar apenas em poder de cada titular, pois é com ela que o destinatário

poderá decodificar a mensagem criptografada para ele com sua respectiva chave pública. Estando a chave privada de um usuário secreta, a comunicação estará protegida.

Para compreender melhor a encriptação assimétrica pode-se pensar num cadeado comum protegendo um determinado bem e a mensagem é este bem. O cadeado, que pode ficar exposto, é a chave pública. Somente quem tiver uma chave particular (privada) que consiga abrir o cadeado, terá acesso à mensagem.(OLIVEIRA, 2012)

Na criptografia assimétrica as mensagens codificadas com a chave pública só poderão ser decodificadas com a chave privada correspondente, ou seja, não é possível decifrar a mensagem com a mesma chave que a cifrou, como ocorre na criptografia simétrica.

Figura 2.5 – Modelo Simétrico e Assimétrico de Criptografia



Fonte: https://www.researchgate.net/figure/Figura-14-Modelo-simetrico-e-assimetrico-de-criptografia_fig4_266912212

2.2 TROCA DE CHAVES E O ALGORITMO DIFFIE-HELLMAN

A compreensão de que uma única chave era necessária foi considerada uma verdade durante muitos anos até a criação do conceito de chave pública, através do qual, Ana e Beatriz poderiam combinar uma chave por meio de uma troca de mensagens utilizando um sistema de comunicação aberto que, no final, terminasse como conhecimento exclusivo

delas. Esse conceito surgiu em 1976, na publicação de um livro, por dois pesquisadores, Bailey Whitfield Diffie e Martin Edward Hellman que descreveram o primeiro método para trocar uma chave secreta entre dois agentes usando um canal público. Em outras palavras pode-se dizer que, num código de *chave pública*, usuários trocam uma chave com segurança, pois estes calculam a chave do sistema criptográfico de forma independente. Na prática pode-se dizer que a criptografia de chave pública não utiliza a mesma chave para os processos de cifragem e decifragem dos conteúdos e a segurança matemática oferecida neste tipo de criptografia, torna segura a distribuição das chaves, já que o processo de decifragem só pode ser feito pela chave privada correspondente à chave pública que cifrou o conteúdo.

Segundo (STALLINGS, 2015, Pág.199), "o desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução na história da criptografia", pois praticamente todos os sistemas criptográficos, dos mais antigos até os modernos, se baseavam em ferramentas elementares da substituição e da permutação e a criptografia de chave pública proporciona uma mudança radical no que havia sido feito até então, pois se baseia em funções matemáticas, e, principalmente, é assimétrica, utilizando-se de duas chaves separadas, diferentemente da criptografia simétrica, que faz uso de apenas uma chave.

O conceito de criptografia de chave pública foi resultado da evolução de tentativas em resolver dois dos problemas mais difíceis da encriptação simétrica: a distribuição de chaves e o de assinaturas digitais. Para (STALLINGS, 2015, Pág. 201) "Diffie e Hellman fizeram uma descoberta incrível em 1976, surgindo com um método que resolvia os dois problemas e que era radicalmente diferente de todas as técnicas anteriores de criptografia".

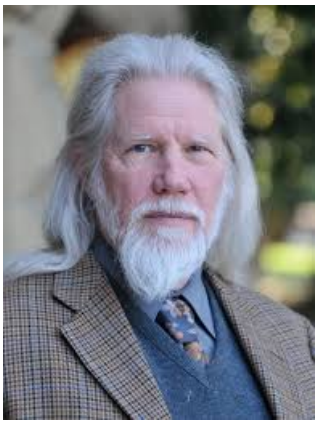
O sistema proposto por Diffie-Hellman permite a troca de chaves criptográficas entre dois usuários sobre uma linha de comunicação insegura, entretanto, este não é um método para cifrar mensagem, ou seja, o algoritmo Diffie-Hellman não realiza nenhuma técnica de cifragem de dados.

2.2.1 Descrição do algorítmo de Diffie-Hellman

A função usada por Diffie e Hellman é uma combinação de função exponencial com aritmética modular, e era considerada como uma *função de mão única*, ou seja, fácil de ser calculada porém difícil de ser revertida, havendo um grande percurso entre teoria e prática. Entretanto, esse percurso conduziu a um dos resultados mais impressionantes da criptografia.

Nesse método, suponha que Ana e Beatriz pretendam trocar uma chave secreta

Figura 2.6 – Bailey Whitfield Diffie



Fonte: https://cisac.fsi.stanford.edu/people/whitfield_diffie

Figura 2.7 – Martin Edward Hellman

Fonte: https://pt.wikipedia.org/wiki/Martin_Hellman

usando um canal público, ambas combinam inicialmente usar um número primo p e uma raiz primitiva g do grupo multiplicativo dos invertíveis módulo p, $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$, os quais não precisam ser mantidos em sigilo, podendo ser conhecido por todos.

Ana então efetua o seguinte procedimento:

1. Escolhe de forma aleatória um número inteiro x_A no intervalo $1 < x_A < p-1$ e o mantém em sigilo;
2. Calcula
$$y_A \equiv g^{x_A} \pmod{p}.$$
3. Envia y_A para Beatriz usando um canal público.

Beatriz efetua o mesmo procedimento:

1. Escolhe de forma aleatória um número inteiro x_B no intervalo $1 < x_B < p-1$ e o mantém em sigilo;
2. Calcula
$$y_B \equiv g^{x_B} \pmod{p}.$$
3. Envia y_B para Ana usando um canal público.

Como Ana recebeu y_B, ela calcula

$$(y_B)^{x_A} \pmod{p} \equiv (g^{x_B})^{x_A} \pmod{p} \equiv g^{x_A x_B} \pmod{p} = k.$$

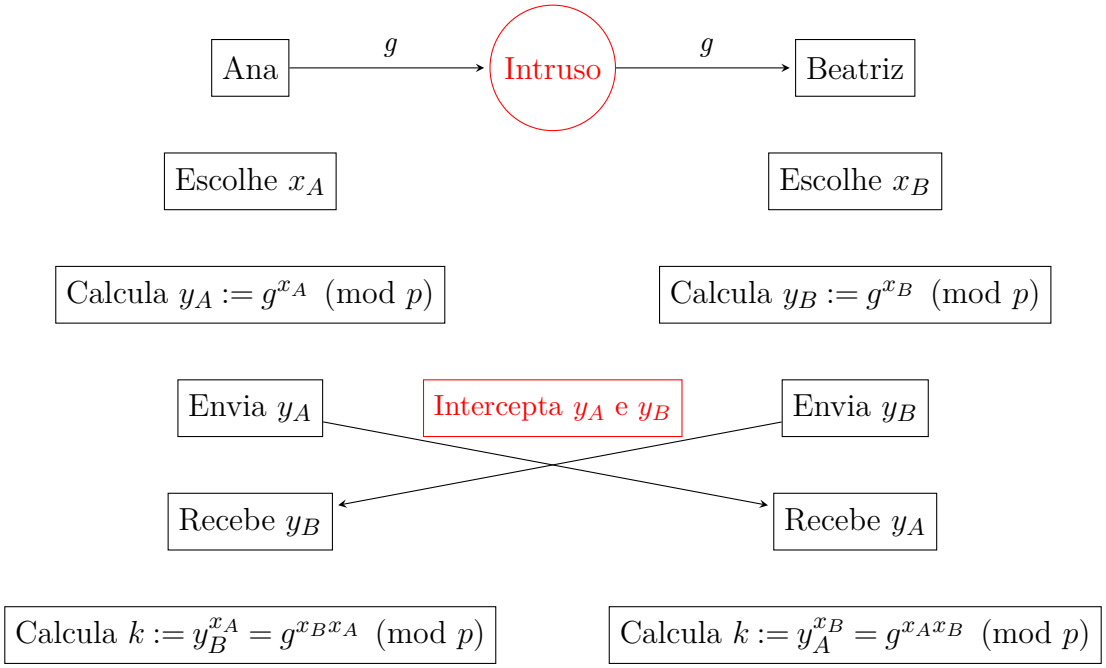
Como Beatriz recebeu y_A, ela calcula

$$(y_A)^{x_B} \pmod{p} \equiv (g^{x_A})^{x_B} \pmod{p} \equiv g^{x_A x_B} \pmod{p} = k,$$

assim, ambas passam a compartilhar da mesma chave. O diagrama na Figura (2.8) mostra os passos envolvidos no protocolo.

As operações envolvidas são facilmente computáveis, porém muito difíceis de serem revertidas e possibilita que dois interlocutores calculem a chave, sem precisar compartilhá-la de forma direta.

Figura 2.8 – Algoritmo de Diffie-Hellman



Fonte: Produção própria

Vejamos na prática como funciona o protocolo Diffie-Hellman utilizando os exemplos abaixo:

Exemplo 2.2.1. *A troca de chaves é baseada no número primo* $p = 353$ *e de uma raiz primitiva de 353, neste caso* $g = 3$*. A e B selecionam, respectivamente, chaves secretas* $x_A = 97$ *e* $x_B = 233$*. Cada um calcula sua chave pública:*

A calcula $y_A = 3^{97} \ mod\ 353 = 40$*.*

B calcula $y_B = 3^{233} \ mod\ 353 = 248$

Depois de trocarem as chaves públicas, cada um poderá calcular a chave secreta comum.

A calcula $k = (y_B)^{x_A} \ mod\ 353 = 248^{97} \ mod\ 353 = 160$*.*

B calcula $k = (y_A)^{x_B} \ mod\ 353 = 40^{233} \ mod\ 353 = 160$*.*

Considerando que um intruso tivesse à sua disposição as informações abaixo

$$p = 353, \quad g = 3, \quad y_A = 40 \quad e \quad y_B = 248$$

Através da força bruta seria possível encontrar a chave secreta 160, bastando para isso, calcular potências de 3 $(\text{mod } 353)$*, parando quando o resultado for igual a* 40 *ou* 248*. Entretanto, com números grandes isso se torna impraticável. Sendo assim, por razões de segurança, os números primos escolhidos são enormes.*

Quando g não é uma raiz primitiva, ou seja, as potências $g, g^2, g^3, \ldots$ não assumem todos os valores $\{1, 2, ..., p-1\}$, ainda é possível usar o algoritmo, mas a quantidade de chaves possíveis diminuirá. Vejamos a seguir um exemplo onde o g escolhido não é uma raiz primitiva.

Exemplo 2.2.2. *Ana e Beatriz combinam usar o número primo* $p = 53$ *e* $g = 11$ *em comum acordo, que podem ser públicos.*

Ana escolhe, sem divulgar, um número natural x_A *igual a 7 e calcula* $y_A < p$ *tal que* $g^{x_A} \equiv y_A \pmod{p}$*, ou seja, o resto da divisão de* 11^7 *por* 53 *é* $y_A = 25$*. Ana envia* y_A *para Beatriz.*

Beatriz escolhe, sem divulgar, um número natural x_B *igual a 5 e calcula* $y_B < p$ *tal que* $g^{x_B} \equiv y_B \pmod{p}$*, ou seja, o resto da divisão de* 11^5 *por* 53 *é* $y_B = 37$*. Beatriz envia* y_B *para Ana.*

Ana calcula $k < p$ *como o resto da divisão de* $y_B^{x_A}$ *por p, ou seja, o resto da divisão de* 37^7 *por* 53 *é* 4*, pois como* $y_B \equiv g^{x_B} \pmod{p}$*, temos que* $y_B^{x_A} \equiv (g^{x_B})^{x_A} \equiv g^{x_B x_A} \equiv k \pmod{p}$*.*

Beatriz calcula $k < p$ como o resto da divisão de $y_A^{x_B}$ por p, ou seja, o resto da divisão de 25^5 por 53 é 4, pois como $y_A \equiv g^{x_A} \pmod{p}$, temos que $y_A^{x_B} \equiv (g^{x_A})^{x_B} \equiv g^{x_A x_B} \equiv k \pmod{p}$.

Como pode-se perceber, Ana e Beatriz chegam ao mesmo número $k = 4$.

Através do exemplo anterior, observa-se que o algoritmo funciona apesar do $g = 11$ escolhido não ser raiz primitiva, uma vez que que a ordem do 11 módulo 53 é 26. Assim, ataques via força bruta tem uma facilidade maior para funcionar, uma vez que as possíveis chaves $k = g^{x_A x_B} \pmod{p}$ só assumem $26 = \frac{53-1}{2}$ valores.

2.2.2 Diffie-Hellman e o problema do logaritmo discreto

O problema do logaritmo discreto (PLD) sobre um grupo finito $(G, *)$ de ordem t pode ser descrito da seguinte forma: Dado um elemento $a \in G$ e $y \in \langle a \rangle$, encontre $x \in \mathbb{N}$ tal que $a^x = y$, ou seja,

$$y = \underbrace{a * a * a * \ldots * a}_{x \text{ vezes}} = a^x,$$

justificando a nomenclatura de logaritmo, denotamos usualmente $\log_a(x) = y$. Se o grupo G for cíclico e $a \in G$ é um gerador, então y pode ser um elemento qualquer do grupo. Naturalmente, $1 \leq x \leq t-1$, uma vez que t é a ordem de G.

No contexto apresentado anteriormente, podemos interpretar o protocolo Diffie-Hellman como uma aplicação do PLD no grupo $G = \mathbb{Z}_p^*$, onde p é um primo, e a operação é a multiplicação usual módulo p. Nesse caso, pode-se provar pelo Teorema 1.8.1 que G é um grupo cíclico, seus geradores são chamados de raízes primitivas.

O problema do logaritmo discreto pode não ser eficiente para um grupo genérico. Por exemplo, no grupo modular aditivo o PLD não fornece dificuldades uma vez que pode ser resolvido por uma simples divisão. Em contraste, no grupo multiplicativo módulo p, a dificuldade na resolução do PLD garante a segurança do protocolo Diffie-Hellman. A segurança da troca de chaves Diffie-Hellman reside no fato de que, embora seja relativamente fácil calcular exponenciais módulo um primo, calcular logaritmos discretos para números primos grandes é uma tarefa considerada inviável computacionalmente. Após a introdução do protocolo Diffie-Hellman, matemáticos propuseram outros grupos onde o mesmo comportamento pode ser observado. Um dos principais exemplos onde isso acontece é o grupo de curvas elíticas. Apresentamos superficialmente esse exemplo a seguir.

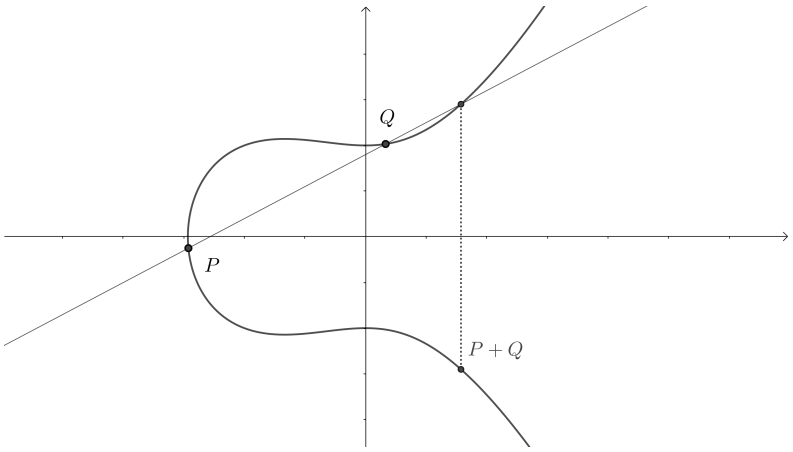
2.2.3 PLD para curvas elíticas

Uma curva plana suave de grau 3 com coeficientes em um corpo k (de característica > 3) pode ser transformada, via mudança de variáveis, em uma curva com equação na forma

$$y^2 = x^3 + ax + b, \Delta = 4a^3 + 27b^2 \neq 0. \quad (1)$$

A definição formal de curva elítica utiliza conceitos que fogem do objetivo desse trabalho, no entanto podemos tratar intuitivamente de curvas elíticas considerando o conjunto dos pontos (x, y) no conjunto k^2 que satisfazem a equação (1), adicionado de um ponto extra, denotado O, que consideramos o ponto no infinito [1]. O interesse no estudo das curvas elíticas vem do fato que o conjunto das soluções da equação adicionado do ponto O, denotamos tal conjunto por $E(k)$, forma um grupo com a operação binária chamada de corda-tangente, ilustrada na Figura 2.9.

Figura 2.9 – Operação de grupo da Curva elítica



Fonte: Produção Própria

Dados dois pontos P, Q na curva elítica, é possível verificar que a reta passando por P e Q intersecta a curva em um terceiro ponto (possivelmente igual a P ou Q, no caso em que a reta é tangente à curva), digamos que esse ponto tem coordenadas (x_0, y_0). Observe que, pela natureza da equação, a curva é simétrica com relação ao eixo x, portanto a troca de y_0 por $-y_0$ também fornece um ponto na curva, denominado $P + Q$. Verifica-se que, com essa operação, o conjunto dos pontos situados na curva adicionado do ponto O define um grupo abeliano. Uma introdução geral à teoria das curvas elíticas, incluindo a definição algébrica formal da operação de grupo, pode ser encontrada em (SILVERMAN,

[1] Formalmente, uma curva elítica deve ser definida não no espaço euclidiano usual, mas no espaço projetivo, onde há um ponto no infinito para cada direção do plano. Curvas elíticas possuem apenas um ponto no infinito, a saber, o ponto no infinito da direção vertical.

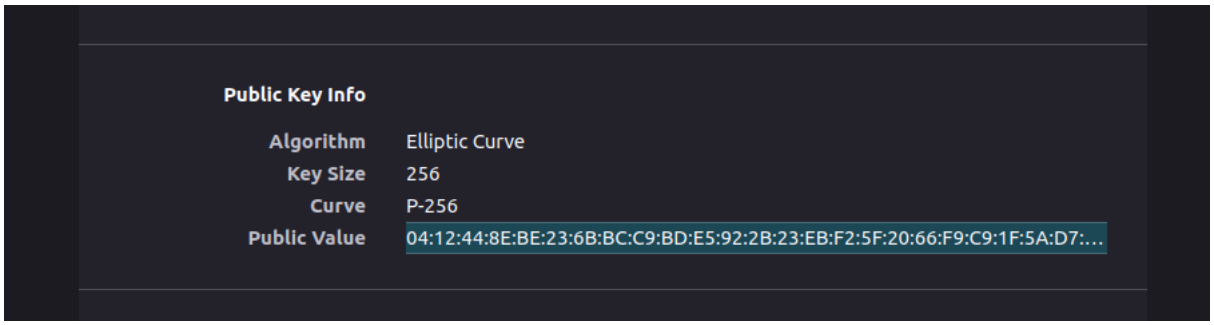
2009). Observamos que, apesar de ilustrar a curva elítica no plano $\mathbb{R}^2$ usual, a mesma operação é definida para coeficientes em um corpo qualquer, inclusive nos corpos finitos. Nesse caso perdemos a intuição geométrica mas a definição algébrica da operação ainda funciona.

Se considerarmos um primo p e $k = \mathbb{Z}_p$, o conjunto $E(k)$ é um grupo finito pois é um subconjunto de $(\mathbb{Z}_p)^2 \cup \{O\}$. Para fins de aplicações, consideramos p grande o suficiente e $P \in E(k)$ um ponto de forma que o subgrupo gerado por P tenha também uma ordem grande. Aplica-se, então o algoritmo de Diffie-Hellman considerando o grupo $G = E(k)$ e $g = P$.

Exemplo 2.2.3. *Curva de Montgomery:* $y^2 = x^3 + 48666x^2 + x$ *sobre o corpo primo com* $p = 2^{255} - 19$. *O ponto* P *com* $x = 9$ *gera um subgrupo cíclico com ordem* $2^{252} + 27742317777372353535851937790883648493$.

Na prática, se usa o algoritmo de Diffie-Hellman nesse contexto, para curvas elípticas, chamado de *ECDH*, a Figura 2.10 mostra informações sobre o algoritmo de troca de chaves do site *Facebook*, detalhadas nas configurações.

Figura 2.10 – Informações sobre troca de chaves usando curvas elíticas



Fonte: Produção Própria

3 PROTOCOLO DIFFIE-HELLMAN NA SALA DE AULA

Como visto no capítulo anterior, o protocolo Diffie-Hellman baseia-se em conceitos importantes da Matemática como divisão, potenciação, números primos entre outros. Sendo assim, este capítulo tem como objetivo propor atividades relacionadas ao protocolo que possam ser aplicadas em salas de aula do Ensino Fundamental, Médio e Superior, utilizando a criptografia como forma de motivação na apropriação desses conceitos. Em cada uma das seções propomos atividades para cada nível escolar, descrevendo-as na forma que seriam apresentadas aos estudantes e, em seguida, inserimos algumas informações auxiliares ao instrutor, como metodologia e desdobramentos possíveis.

3.1 ATIVIDADE 1 - ENSINO FUNDAMENTAL

De acordo com (MARQUES, 2013), a atividade sobre o protocolo Diffie-Hellman proposta abaixo pode ser aplicada no Ensino Fundamental, pois permite serem trabalhados conteúdos como divisão e potenciação.

Atividade

A *criptografia* (do grego *kiptos*, "escondido"e *graphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas pelo remetente e destinatário da mensagem por meio de uma chave. Dois estudiosos americanos chamados Whitfield Diffie e Martin Hellman publicaram em 1976 um novo método de duas pessoas trocarem mensagens de modo seguro utilizando o protocolo da troca de chaves de Diffie-Hellman, baseado, de maneira simplificada, no resto da divisão entre números naturais.

Supondo que Alice e Bob são duas pessoas que desejam se comunicar utilizando uma mensagem secreta, mas para isso deverão compartilhar uma chave secreta. O protocolo Diffie-Hellman funciona da seguinte maneira:

1. Alice e Bob trocarão informações utilizando os restos das potências de base 4 com relação ao número primo 7;
2. Alice deverá escolher um valor natural entre 1 e 7, que vamos chamar de x, e calcular o resto da divisão de 4^x por 7 que denotaremos por a e enviar para Bob;
3. Bob deverá escolher um valor natural entre 1 e 7, que vamos chamar de y, e calcular o resto da divisão de 4^y por 7 que denotaremos por b e enviar para Alice;

4. Agora, Alice irá calcular o resto da divisão de b^x por 7 e chamar de k_1;
5. Bob irá calcular o resto da divisão de a^y por 7 e chamar de k_2;
6. Note que $k_1 = k_2$ e será a chave da comunicação secreta entre eles, que denotaremos por k.

Após esse procedimento ser feito, Bob deseja enviar uma palavra secreta para Alice, supondo que seja a palavra **amor**. Então, por exemplo, se o valor de k obtido for o número 5, então Bob irá codificar a palavra **amor** substituindo cada letra dessa palavra pela sua representante na linha 5 da tabela abaixo.

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

Fonte: Marques, 2013

Sendo assim, ele substituirá a letra A por N, M por H, O por A e R por Z, obtendo a palavra **nhaz**. Alice receberá essa mensagem e decodificará utilizando a linha 5 com relação a linha do alfabeto da Língua Portuguesa. Dessa forma, ela substituirá a letra N por A, H por M, A por O e Z por R, obtendo a mensagem original **amor**.

Reúnam-se em dupla de forma que um desempenhe a função de Alice e o outro a de Bob, sigam os passos do exemplo acima e troquem uma chave secreta utilizando o protocolo Diffie-Hellman para enviar uma palavra secreta um para o outro.

Objetivo Geral

Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos em relação à divisão e potenciação de números naturais.

Objetivos Específicos

- Identificar o dividendo, divisor, quociente e resto de uma divisão;
- Saber a definição de números primos;
- Calcular potências de números naturais;
- Relacionar o resto de uma divisão com a codificação e decodificação de mensagens.

Público Alvo: Estudantes do Ensino Fundamental a partir do 6º ano.

Materiais: Lápis, borracha, calculadora e a folha contendo a atividade.

Metodologia: Atividade a ser aplicada em sala de aula ao final do conteúdo de potenciação para a verificação da aprendizagem dos alunos em relação a esse conteúdo. Os alunos formarão duplas para verificar, utilizando a calculadora para o cálculo das potências, se conseguiram chegar a mesma chave e codificar e decodificar as mensagens transmitidas. Ao final desta atividade, o professor deverá discutir os resultados obtidos com os discentes, verificando se as mensagens foram trocadas com êxito.

Dificuldades Previstas: As dificuldades, que poderão surgir durante a aplicação desta atividade, são referentes à divisão, conteúdo usualmente considerado difícil pelos alunos. O professor perceberá essa dificuldade ao orientar e observar o andamento das atividades.

Possíveis Continuações ou Desdobramentos: O docente poderá utilizar outros valores para o número primo e a base da potência, bem como mudar o alfabeto utilizado na codificação e decodificação das mensagens.

3.2 ATIVIDADE 2 - ENSINO MÉDIO

Neste trabalho foi feito um breve relato histórico da criptografia mostrando algumas cifras utilizadas ao longo de sua evolução, entre elas a cifra de Viginère. A atividade a seguir faz uso dessa cifra, relacionando-a com a chave obtida através do protocolo Diffie-Hellman por meio de funções, conteúdo abordado no Ensino Médio.

Atividade

A criptografia consiste em técnicas de modificar uma mensagem de forma que somente o destinatário seja capaz de compreendê-la. Para isso é preciso utilizar uma chave combinada entre quem envia e quem recebe. Essa chave é a forma que deve ser usada para decifrar a mensagem, portanto deve ser mantida em sigilo para aqueles que não devem compreender a mesma. Mas se os que desejam se comunicar estiverem distantes, como será possível combinar a chave para decifrar a mensagem? Em 1976, dois estudiosos americanos chamados Whitfield Diffie e Martin Hellman publicaram um novo método de duas pessoas trocarem mensagens de forma segura utilizando um protocolo de troca de chaves chamado de Diffie-Hellman em homenagem aos mesmos, o qual tem como base o resto da divisão entre números naturais.

Vamos supor que Alice e Bob são duas pessoas que desejam se comunicar utilizando

uma mensagem secreta, mas para isso deverão compartilhar uma chave secreta. O protocolo Diffie-Hellman funciona da seguinte maneira:

1. Alice e Bob trocarão informações utilizando os restos das potências de base 4 com relação ao número primo 11;
2. Alice deverá escolher um valor natural entre 1 e 11, que vamos chamar de x, e calcular o resto da divisão de 4^x por 11 que denotaremos por a;
3. Bob deverá escolher um valor natural entre 1 e 11, que vamos chamar de y, e calcular o resto da divisão de 4^y por 11 que denotaremos por b;
4. Agora, Alice irá calcular o resto da divisão de b^x por 11 e chamar de k_1;
5. Bob irá calcular o resto da divisão de a^y por 11 e chamar de k_2;
6. Note que $k_1 = k_2$ e será a chave da comunicação secreta entre eles, que denotaremos por k.

Após esse procedimento ser feito, Bob deseja enviar uma mensagem para Alice, supondo que seja a mensagem **VOU ESTUDAR**. Então, por exemplo, se o valor de k obtido for o número 8, então Bob irá calcular a função $f(k)$ ou seja, $f(8)$ na função $f(x) = 2x + 3$, na qual irá obter $f(8) = 19$ e irá codificar a mensagem **VOU ESTUDAR** substituindo cada letra dessas palavras pela sua representante na linha 19 da cifra de Vigenère abaixo.

Dessa forma, ele substituirá a letra V por O, O por H, U por N, E por X, S por L, T por M, U por N, D por W, A por T e R por K, obtendo **OHN XLMNWTK**. Alice receberá essa mensagem e decodificará utilizando a linha 19 com relação a linha do alfabeto da Língua Portuguesa. Sendo assim, ela substituirá a letra O por V, H por O, N por U, X por E, L por S, M por T, N por U, W por D, T por A e K por R, obtendo a mensagem original **VOU ESTUDAR**.

Formem três grupos na sala e troquem mensagens utilizando o protocolo Diffie-Hellman.

Objetivo Geral

Motivar o estudo de funções utilizando a criptografia.

Objetivos Específicos

Figura 3.1 – Cifra de Vigenère

Fonte: https://efacildemais.blogspot.com/2011/08/um-trabalho-de-faculdade-que-jamais-li.html?m=0

- Compreender e aplicar o conceito de função;
- Calcular o valor numérico de uma função;
- Relacionar funções com a codificação e decodificação de mensagens.

Público Alvo: Estudantes do Ensino Médio a partir do 1º ano.

Materiais: Lápis, borracha, calculadora e a folha da atividade.

Metodologia: Essa atividade deve ser aplicada após o conteúdo sobre funções. Os alunos formarão grupos de forma que o grupo 1 (Alice) será responsável por codificar a mensagem e enviá-la para o grupo 2 (Bob), que será o destinatário, o qual decifrará a mensagem e o grupo 3 é o interceptador e tentará decifrá-la sem conhecer a chave. O professor deverá verificar as dificuldades encontradas por cada grupo e promover uma discussão ao final da atividade.

Pré-requisitos: Para a realização desta atividade é necessário o conhecimento sobre função e seu valor numérico, além do funcionamento da cifra de Vigenère que pode ser explicado durante a realização da atividade.

Possíveis Continuações ou Desdobramentos: O professor poderá utilizar outros valores para o número primo e a base da potência, além de outras funções, cujos

valores numéricos estejam dentro das linhas da cifra de Vigenère.

3.3 ATIVIDADE 3 - ENSINO SUPERIOR

Em relação ao Ensino Superior pode-se utilizar o protocolo Diffie-Hellman na abordagem de conteúdos como congruência, logaritmos discretos entre outros. A atividade proposta a seguir pode ser utilizada ao abordar congruência.

Atividade

A criptografia consiste em técnicas de modificar uma mensagem de forma que somente o destinatário seja capaz de compreendê-la. Para isso é preciso utilizar uma chave combinada entre quem envia e quem recebe. Essa chave é a forma que deve ser usada para decifrar a mensagem, portanto deve ser mantida em sigilo para aqueles que não devem compreender a mesma. Mas se os que desejam se comunicar estiverem distantes, como será possível combinar a chave para decifrar a mensagem? Em 1976, dois estudiosos americanos chamados Whitfield Diffie e Martin Hellman publicaram um novo método de duas pessoas trocarem mensagens de forma segura utilizando um protocolo de troca de chaves chamado de Diffie-Hellman em homenagem aos mesmos, o qual tem como base a aritmética modular.

Nesse método, supondo que Alice e Bob pretendam trocar uma chave secreta usando um canal público, ambos combinam inicialmente usar um número primo p e um gerador g do grupo multiplicativo $Z_p^* = \{1, 2, ..., p-1\}$, os quais não precisam ser mantidos em sigilo, podendo ser conhecido por todos.

Alice então efetua o seguinte procedimento:

1. Escolhe de forma aleatória um número inteiro x_A no intervalo $1 < x_A < p-1$ e o mantém em sigilo;
2. Calcula
$$y_A \equiv g^{x_A} \pmod{p}$$
3. Envia y_A para Bob usando um canal público.

Bob efetua o mesmo procedimento:

1. Escolhe de forma aleatória um número inteiro x_B no intervalo $1 < x_B < p-1$ e o mantém em sigilo;

2. Calcula

$$y_B \equiv g^{x_B} \pmod{p}$$

3. Envia y_B para Alice usando um canal público.

Como Alice recebeu y_B, ela calcula

$$(y_B)^{x_A} \pmod{p} \equiv (g^{x_B})^{x_A} \pmod{p} \equiv g^{x_A x_B} \pmod{p} = k$$

Como Bob recebeu y_A, ele calcula

$$(y_A)^{x_B} \pmod{p} \equiv (g^{x_A})^{x_B} \pmod{p} \equiv g^{x_A x_B} \pmod{p} = k$$

e assim, ambos passam a compartilhar da mesma chave.

Agora, supondo que Alice e Bob desejem trocar uma chave usando o algoritmo Diffie-Hellman, combinando usar o número primo $p = 13$ e o gerador $g = 5$ e sabendo que $y_A = 12$, marque a alternativa que indica o valor de x_A.

a) 89 b) 97 c) 142 d) 267 e) 453

Para resolver esse problema, como foi dado o valor de $y_A = 12$, temos que verificar qual das alternativas satisfaz $12 \equiv 5^{x_A} \pmod{13}$.

Como exemplo, verificaremos se é 89 (letra a).

$5^{89} = 5^{88} \times 5 = (5^2)^{44} \times 5 = 25^{44} \times 5$.

Como $25 \equiv -1 \pmod{13}$ temos que:

$25^{44} \equiv (-1)^{44} \equiv 1 \pmod{13}$

Logo, $5^{89} \equiv 25^{44} \times 5 \equiv 1 \times 5 \equiv 5 \pmod{13}$, não satisfaz o y_A que deve ser igual a 12.

Com base no exemplo acima, encontre a solução para o problema dado.

Objetivo Geral

Motivar o estudo de congruência utilizando a criptografia

Objetivos Específicos

- Compreender grupos e seus geradores;
- Conceituar e aplicar congruência modular, teoremas de Fermat e Euler;
- Relacionar grupos, congruência modular, teoremas de Fermat e Euler com a codificação e decodificação de mensagens.

Público Alvo: Estudantes dos cursos de Licenciatura e/ou Bacharelado em Matemática e de áreas afins.

Materiais: Lápis, borracha e a folha da atividade.

Metodologia: Será proposto o problema acima para os alunos, de modo que eles percebam que um intruso conhecendo g e y_A, poderia encontrar x_A através de

$$y_A = g^{x_A} \pmod{p},$$

o que significaria resolver o problema do logaritmo discreto, e consequentemente descobrir a chave. Por força bruta, a técnica do intruso seria testar todos os $x_A \in \{1, ..., p-1\}$ até achar o resultado. Ao propor uma atividade de múltipla escolha, em que há apenas algumas alternativas para testar, indicamos que o ideal na criptografia é utilizar números primos p muito grandes para que a força bruta se torne inviável.

Pré-requisitos: Para a realização desta atividade é necessário o conhecimento sobre grupos, teoremas de Fermat e Euler e congruência modular.

Possíveis Continuações ou Desdobramentos: O professor poderá utilizar outros valores para o número primo e para o gerador, bem como permitir o uso da calculadora para facilitar o cálculos com números mais elevados. Poderá ainda criar um grupo de alunos para representar Alice, outro para Bob e conduzi-los para o cálculo de k, que é a chave secreta, enquanto outro grupo age como o intruso, tentando encontrar a chave secreta.

CONSIDERAÇÕES FINAIS

Através do exposto neste trabalho, constatou-se que a criptografia é um assunto relevante para os dias atuais, haja vista que as novas tecnologias fazem cada vez mais parte do nosso cotidiano e que nossas informações precisam estar bem seguras, sendo as técnicas utilizadas pela criptografia capazes de tornar isso possível.

Pela importância que o assunto tem para a atualidade, o presente estudo teve como objetivo principal listar conhecimentos sobre a Criptografia, em especial o Protocolo de troca de chaves de Diffie-Hellman, fornecendo possibilidades para professores de Matemática que desejem dinamizar suas aulas através deste conteúdo, já que o referente protocolo faz uso de conceitos importantes dessa disciplina e que apesar de não ser um método de cifrar mensagens, provocou uma verdadeira revolução na criptografia ao permitir que pessoas pudessem trocar uma chave num meio inseguro, objetivo este, que acredita-se ter sido atingido ao passo que abordou aspectos significativos para a compreensão de tais conhecimentos.

Acredita-se também, que os objetivos específicos deste trabalho foram atingidos, já que o mesmo apresenta os conceitos de teoria dos números com seus teoremas e demonstrações, que servem de base para o entendimento do protocolo de troca de chaves em questão, fazendo um breve relato histórico da evolução da criptografia, que apesar de não profundo, contempla os fatos pertinentes ao seu entendimento, além de propiciar à realização de uma abordagem sobre esse assunto em salas de aula do Ensino Básico ao Superior com a proposta de três atividades prontas para serem ministradas nestas etapas de ensino, uma para cada nível especificamente.

Sobre o processo de construção do presente estudo pode-se relatar um aspecto negativo, que foi a limitação de acesso a bibliografia necessária, já que muitas das disponíveis na internet estavam em outra língua, principalmente as que tratam do protocolo.

Um aspecto positivo refere-se à existência do programa LaTex, que apesar de apresentar uma certa complexidade no seu manuseio é bastante funcional para a realização da escrita na linguagem matemática.

Em virtude da dificuldade ocorrida para realização deste trabalho, recomenda-se uma ampliação a respeito do tema proposto no mesmo, tais como o estudo do sistema criptográfico RSA, um dos mais utilizados na atualidade, que recebeu forte influência do algoritmo proposto por Diffie e Hellman,

REFERÊNCIAS

COSTA, C.; M., F. L. **Introdução à Criptografia - Vol.1**. UFF / CEP – EB, 2010. ISBN 85-7648-303-3. Disponível em: <https://canal.cecierj.edu.br/recurso/4687>.

COUTINHO, S. C. Notas de aula, **Criptografia**. 2015.

FALEIROS, A. C. **Critografia**. [S.l.]: SBMAC, 2011. ((Notas em Matemática Aplicada; v. 52)). ISBN 78-85-86883-54-5.

FIARRESGA, V. M. C. **Criptografia e Matemática**. Tese (Dissertação (Mestrado em Matemática para Professores)) — Faculdade de Ciências da Universidade de Lisboa, 2010.

FILHO, E. de A. **Teoria elementar dos números**. Nobel, 1981. ISBN 9788521300403. Disponível em: <https://books.google.com.br/books?id=Z5z5tgAACAAJ>.

GONÇALVES, A. **Introdução à Álgebra**. Rio de Janeiro: Impa, 1979.

MARQUES, T. V. **Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula**. Tese (Dissertação (Mestrado PROFMAT)) — UFPB/CCEN, 2013.

NASCIMENTO, M. C. d.; FEITOSA, H. d. A. Notas de Aula, **Elementos da teoria dos números**. 2013.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. **Revista Online Segurança Digital**, p. 11–15, 2012.

SANTOS, J. D. **Introdução à teoria dos números**. IMPA, 2010. (Coleção matemática universitária). ISBN 9788524401428. Disponível em: <https://books.google.com.br/books?id=mL6mAAAACAAJ>.

SILVA, A. d. A.; JURIAANS, O. S. Notas de Aula, **Álgebra Abstrata**. 2010.

SILVERMAN, J. **The Arithmetic of Elliptic Curves**. Springer New York, 2009. (Graduate Texts in Mathematics). ISBN 9780387094946. Disponível em: <https://books.google.com.br/books?id=Z90CA_EUCCkC>.

STALLINGS, W. **Criptografia e segurança de redes. Princípios e práticas**. São Paulo: Pearson Prentice Hall, 2015.