Universidade Federal de Goiás – Campus Catalão

Alunos: Bruno Castilho Rosa

Laura Thaís Lourenço

Géssica Cristina dos Reis

Lucas Borges de Faria

Orientador: Igor Lima

Seminário Semanal de Álgebra

Notas de Aula

- ## Título

Um Pouco de Criptografia

- ## Breve descrição da aula

A aula iniciará com um debate sobre o avanço da internet, onde discutiremos o quanto ela passou a ser útil em nosso dia a dia e que a segurança de usá-la, se dá através da Criptografia, o qual será o tema da aula. De forma resumida e clara, definiremos o que é uma criptografia, um criptossistema e como se trabalha com chaves secretas, tudo isso por meio de definições, exemplos e teoremas. Mostraremos um vídeo sobre a atuação da Criptografia na Segunda Guerra Mundial. Encerraremos aula falando um pouco do programa RSA.

- ## Competência(s) desenvolvida(s)

Ter noções sobre criptografia e criptossistema;

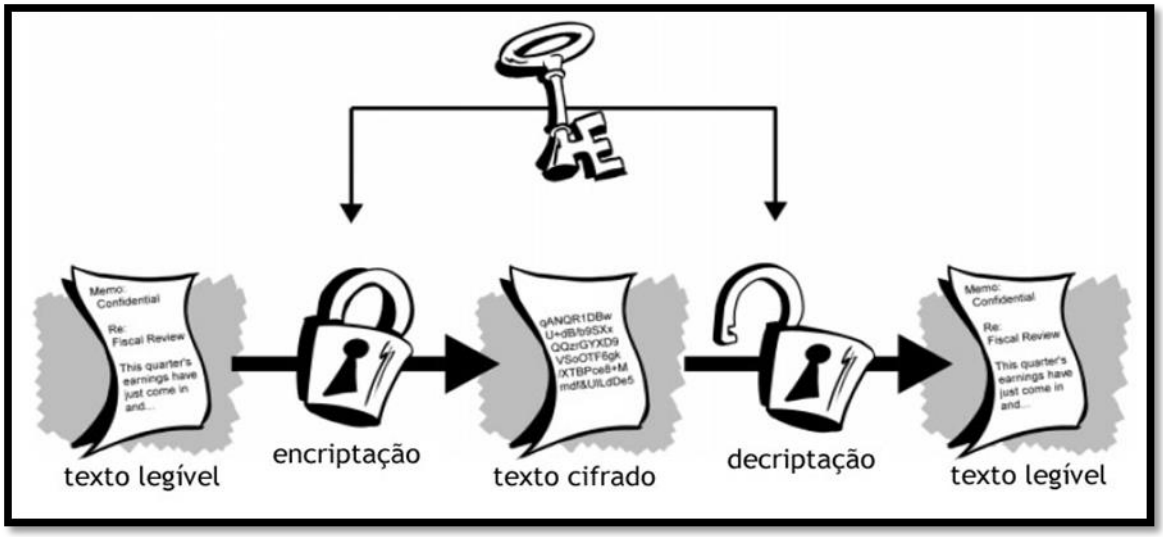
- ## Conteúdo(s) desenvolvido(s).

- **Definição.** A criptografia é um ramo da matemática que lida com princípios de escrever em cifras ou códigos, utilizando um conjunto de técnicas que transformam arquivos legíveis em algo ilegível.

  Na Criptografia:

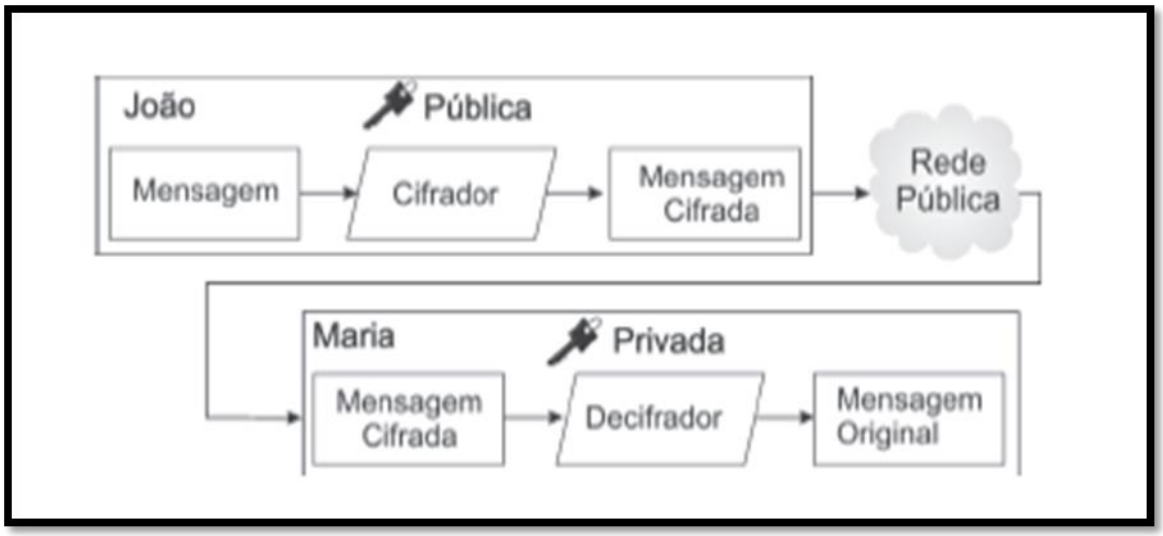
  - Mensagem a ser enviada ⟺ texto-original.
  - Mensagem codificada ⟺ texto-cifrado.
  - Processo de converter um texto-original/texto cifrado ⟺ codificação.

- Processo de reverter ⟺ decodificação ou cifragem.



- **Chaves Criptográficas**

  - **Chaves simétricas**: A criptografia simétrica usa a mesma chave tanto para criptografar como para descriptografar dados.
  - **Chave assimétrica**: A criptografia assimétrica usa duas chaves diferentes, porém matematicamente relacionadas, para criptografar e descriptografar dados.Essas chaves são conhecidas como chaves privadas e públicas.



Exemplos de criptografia que usam chaves assimétricas:

- **Criptografia RSA**
- **Criptografia DAS**
- **Criptografia ECC**
- **Criptografia Diffie-Hellman**

- **Definição de um Criptossistema**

Considere M, o conjunto de todas as possíveis mensagens unitárias x de um texto original e C o conjunto de todas as possíveis mensagens unitárias c do texto cifrado.

Então o processo de codificação é dado pela função bijetora:

$f: M \rightarrow$C, tal que $f(x) = c$

Assim, um *criptossistema* é definido por qualquer bijeção de M em C.

- **Tabela mostrando a bijeção entre o alfabeto e o conjunto**.

  $\mathbb{Z}_{27}$ = {0,1,2, ..., 25,26}.

$$\begin{array}{cccccccc} A & B & C & \cdots & X & Y & Z & u \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 23 & 24 & 25 & 26 \end{array}$$

Onde u representa o “espaço”.

- **Teorema 1.** Seja n ∈ $\mathbb{N}$ e a, b ∈ $\mathbb{Z}_n$ fixados. Se o mdc (a, n) = 1, então a função: $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dada por $f(x) = ax + b$. é um criptossistema.

  Demonstração: Sendo o mdc (a, n) = 1 temos que existe $a' = a^{-1} \in \mathbb{Z}_n^*$ tal que $a \cdot a' = 1$.

  Tome : $g(x) = a'x + b'$, onde $b' = a'b$

Assim $(f \circ g)(x) = f(g(x)) = f(a'x + b') = a(a'x + b') + b = x = I_{\mathbb{Z}_n}$

Analogamente $(g \circ f)(x) = x = I_{\mathbb{Z}_n}$. Logo $g(x) = f^{-1}(x)$ isto é, a função f possui inversa, portanto f é um criptossistema.

- **Alguns Exemplos de Criptossistema:**

Exemplo 1 - Seja $f: \mathbb{Z}_{27} \to \mathbb{Z}_{27}$ dada por $f(x) = x + 4$ uma Cifra de César. Suponha que o emissor irá enviar a mensagem "Guerra" de forma codificada. Então conforme a Tabela abaixo tem-se a seguinte correspondência:

G	→	$f(G) = f(6) = 10$	= K
U	→	$f(U) = f(20) = 24$	= Y
E	→	$f(E) = f(4) = 8$	= I
R	→	$f(R) = f(17) = 21$	= V
R	→	$f(R) = f(17) = 21$	= V
A	→	$f(A) = f(0) = 4$	= E

Logo o receptor irá receber a seguinte mensagem: KYIVVE. Ao receber a mensagem, o receptor irá aplicar a operação inversa em cada letra da mensagem.

Onde a função inversa é dada por:

$f^{-1} = y - 4$.

$$f^{-1}(K) = 10 - 4 = 6 = \text{G}.$$

$$f^{-1}(Y) = 24 - 4 = 20 = \text{U}.$$

.
.
.

E assim sucessivamente até repor a mensagem original completa.

GUERRA

Exemplo 2 - Seja $f: \mathbb{Z}_{27} \to \mathbb{Z}_{27}$ dada por $f(x) = x + 2$, uma Cifra de César. Suponha que o emissor irá enviar a mensagem "ECUC". Logo o receptor irá decodificar a mensagem aplicando a função inversa $f^{-1}(x) = x - 2$, de acordo com a Tabela abaixo:

E	→	$f^{-1}(E) = f^{-1}(4) = 2$	= C
C	→	$f^{-1}(C) = f^{-1}(2) = 0$	= A
U	→	$f^{-1}(U) = f^{-1}(20) = 18$	= S
C	→	$f^{-1}(C) = f^{-1}(2) = 0$	= A

- **Código de Políbio**

As letras são colocadas num tabuleiro de 5x5.

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

Cada letra é representada pela combinação dos dois números que correspondem à posição ocupada pela letra e a mensagem clara é transformada em uma sequência de números que variam de 11 a 15, 21 a 25, 31 a 35, 41 a 45 e 51 a 55. Veja alguns

- **Exemplos do uso do Código de Políbio.**

1. Texto Original: Tochas de Políbio

Texto Cifrado: 44 35 13 23 11 43 14 15 41 35 32 24 12 24 35

2. Texto Original: AlgebraModerna

Texto Cifrado: 11 32 22 15 12 42 11 33 35 14 15 42 34 11

3. Texto Original: A Matemática é Linda

Texto Cifrado: 11 33 11 44 15 33 11 44 24 13 11 15 32 24 34 14 11

4. Texto Original: Criptografia

Texto Cifrado: 13 42 24 41 44 35 22 42 11 21 24 11

- **Ave Maria de Trithemius**

Este sistema é composto por 14 alfabetos nos quais a cada letra corresponde uma palavra ou grupo de palavras. O resultado da encriptação acaba sendo um texto coerente, em Latim, como se fosse uma oração ou glorificação religiosa.

Veja a seguir um dos algabetos de Ave Maria traduzido para Português:

A: no céu

B: para todo o sempre

C: um mundo sem fim

D: numa infinidade

E: perpetuamente

F: por toda a eternidade

G: durável

H: incessantemente

I - J: irrevogavelmente

K: eternamente

L: na sua gloria

M: na sua luz

N: no paraíso

O: hoje

P: na sua divindade

Q: em Deus

R: na sua felicidade

S: no seu reino

T: na sua majestade

U-V-W: na sua beatitude

X: na sua magnificência

Y: ao trono

O inconveniente do sistema é o tempo necessário para a transposição de um texto de qualquer tamanho e o grande aumento do texto esteganografado resultante. Por outro lado, como a mensagem cifrada se apresenta como um conjunto normal de palavras, os eventuais decifradores, teriam que acumular uma massa enorme de material antes de encontrar as semelhanças necessária para obter a chave.

- **Criptografia RSA** é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da actual empresa RSA Data Security, Inc.), Ronald Rivest, Adi Shamir e Leonard Adleman, que inventaram este algoritmo — até a data (2008), a mais bem sucedida implementação de sistemas de chaves assimétricas

  - **Funcionamento**

    O RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave privada

- Geração das Chaves

No RSA as chaves são geradas desta maneira:

1. Escolha de forma aleatória dois números primos grandes p e q, da ordem de 10^{100} no mínimo.
2. Compute $n = pq$
3. Compute a função totiente em n: $\phi(n) = (p-1)(q-1)$
4. Escolha um inteiro e tal que $1 < e < \phi(n)$, de forma que e e $\phi(n)$ sejam primos entre si.
5. Compute d de forma que $de \equiv 1 \pmod{\phi(n)}$, ou seja, d seja o inverso multiplicativo de e em $\pmod{\phi(n)}$.

- No passo 1 os números podem ser testados probabilisticamente para primalidade
- No passo 5 é usado o algoritmo de Euclides estendido, e o conceito de inverso multiplicativo que vem da aritmética modular

Por final temos:

A chave pública: o par de números n e e
A chave privada: o par de números n e d

- **Cifragem**

Para transformar uma mensagem m, onde $0 < m < n$, numa mensagem c cifrada usando a chave pública do destinatário n e e basta fazer uma potenciação modular:

$$c = m^e \mod n$$

A mensagem então pode ser transmitida em canal inseguro para o receptor. Há um algoritmo para realizar esta potência rapidamente.

- **Decifragem**

Para recuperar a mensagem m da mensagem cifrada c usando a respectiva chave privada do receptor n e d, basta fazer outra potenciação modular:

$$m = c^d \mod n$$

- **Recursos /Materiais Utilizado**

  Quadro e giz.

- **Bibiografia**

SMOLE, Kátia Stocco e DINIZ, Maria Ignez. Matemática: Ensino Médio 1ª série. 3ª Ed reformulada. São Paulo, 2003.

CUNHA, A.L, SAMPAIO,A.C, BRANDÃO, C.R, SANTOS,D.P, RIOS,E.M, MACHADO,I.A, PARREIRA, J.R.P, LIMA, M.D, PIRES, M.M, FERNANDES,R.A.C, VIEIRA, S.P.N, SAMPAIO, U.T . Caderno educacional – Matemática-3º bimestre. Goiás.