

INTRODUÇÃO A CRIPTOGRAFIA E SEGURANÇA DIGITAL

Alexandre Velloso Pinheiro Filho

2018

O QUE É CRIPTOGRAFIA?

- Cryptography or cryptology is the practice and study of techniques of third parties called adversaries.

- Fonte:

- RIVEST, Ronald L. Cryptography. In: **Algorithms and Complexity**. 1990. p. 717-755.

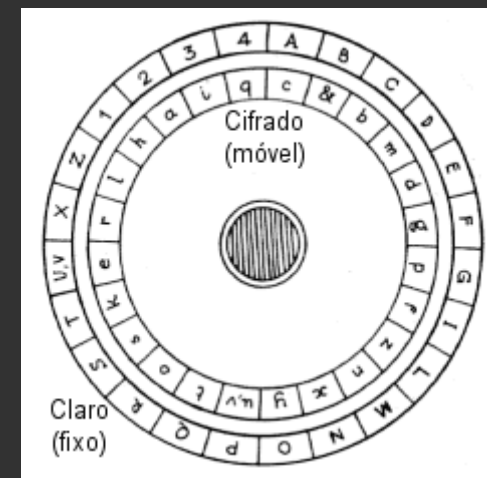
PRINCÍPIOS DA CRIPTOGRAFIA

- Confidencialidade: Garantia que a mensagem criptografada só pode ser lida por quem tem autorização.
- Integridade: Garantia que a mensagem não sofreu alterações no meio do caminho.
- Autenticação: Validar se a pessoa é quem ela diz ser.
- Não-repúdio: Você não pode negar a autoria de uma mensagem.

BREVE HISTÓRIA

- Cifra de cesar(Império romano)
- Vigenère (século XVI)
- Enigma (Exército alemão)
- Blue Code (Marinha japonesa)

	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



BORA PROGRAMAR!

- Faça um programa em qualquer linguagem para cifrar e decifrar mensagens de texto usando os seguintes algoritmos:
- Cifra de cesar
 - $E(x) = (x + n) \bmod 256$
 - $D(x) = (x - n) \bmod 256$
- Cifra de Vigenère
 - $C_i = (P_i + K_i) \bmod 256$
 - $P_i = (C_i + K_i) \bmod 256$

RESPOSTA EM PYTHON

- Cesar

```
def criptografa( mensagem, deslocamento ):  
    mensagemCriptografada = ''  
    for c in mensagem:  
        mensagemCriptografada += chr( ( ord(c) + deslocamento ) % 256 )  
    return mensagemCriptografada
```

- Vigenère

```
def criptografa( mensagem, senha ):  
    mensagemCriptografada = ''  
    pos = 0  
    for c in mensagem:  
        mensagemCriptografada += chr( ( ord(c) + ord(senha[pos])) % 256 )  
        pos = ( pos + 1 ) % len( senha )  
  
    return mensagemCriptografada
```

CLASSE DE ALGORÍTIMOS DE CRIPTOGRAFIA UTILIZADOS HOJE

- Simétricos: Uma única chave para criptografia e descriptografia da mensagem.
- Assimétricos: Esse tipo de criptografia usa 2 chaves, uma chave pública e uma chave privada, onde usando uma para cifrar a mensagem é possível decifrar a mesma mensagem com a outra.

ALGORÍTIMO SIMÉTRICO – AES

- Esse algoritmo usa blocos de tamanhos 128, 192 e 256 bits para cifragem.
- Prós:
 - Rápido, pois só usa operações aritméticas fáceis, como soma e xor.
- Contras:
 - Como vou transmitir a chave simétrica para a outra pessoa?

ALGORÍTIMO ASSIMÉTRICO – RSA (PARTE 1)

- Esse algoritmo usa 2 números primos grandes para calcular as 2 chaves, pública e privada.
- Prós:
 - Você pode distribuir a sua chave pública livremente.
 - Uma mensagem criptografada com uma chave só pode ser descriptografada com a outra.
- Contras:
 - Lento, esse algoritmo pega cada caractere e eleva a um número grande.

ALGORÍTIMO ASSIMÉTRICO – RSA (PARTE 2)

- Algoritmo:
 - Escolha 2 números primos grandes, p e q .
 - Calcule $n = p * q$
 - Calcule $\phi = (p-1) * (q-1)$
 - Escolha um número e de forma que ϕ e e sejam primos entre si.
 - Encontre d de forma que $e * d = 1 \bmod \phi$.
- Chave pública: (e, n)
- Chave privada: d

CIFRAGEM E DECIFRAGEM

- Criptografar a mensagem usando a chave publica n
 - $C(p) = p^e \bmod n$
- Descriptografar a mensagem usando a chave privada m
 - $P(c) = c^d \bmod m$

BORA PROGRAMAR!

- Vamos fazer o algoritmo de criptografia RSA cifrar e decifrar um texto.
- Para facilitar a sua vida, use os seguintes números:
- E: 7
- N: 2869
- D: 1543

RESPOSTA EM PYTHON

- Criptografar

```
def criptografa( mensagem, e, n ):
    mensagemCriptografada = []
    for c in mensagem:
        mensagemCriptografada.append( (ord(c)**e) % n )
    return mensagemCriptografada
```

- Descriptografar

```
def descriptografa( mensagem, d, n ):
    mensagemDescriptografada = ''
    for c in mensagem:
        mensagemDescriptografada += chr( (c**d) % n )
    return mensagemDescriptografada
```

ENTÃO AGORA CONSEGUIMOS RESOLVER O PROBLEMA DAS CHAVES

- Quando criptografamos algo com a chave privada de alguém temos certeza que somente a pessoa dona daquela chave consegue descriptografar a mensagem.
- Assim conseguimos gerar uma chave simétrica e criptografá-la usando a chave pública do destinatário.
- Algoritmo:
 - Gere uma chave de 128, 192 ou 256 bits, depende de qual versão do AES você quer usar.
 - Criptografe a chave usando a chave pública do destinatário.
 - Transmita a chave criptografada pela internet.
 - O usuário vai descriptografar a mensagem usando a sua chave privada, assim conseguindo a chave para o algoritmo AES.

CONCLUSÃO

- Como diversas tecnologias, a criptografia foi criada em tempos de guerra, mas hoje usamos ela no dia a dia para facilitar nossa vida
- Essa palestra foi uma breve introdução a esses conceitos, espero que tenham gostado.

Dúvidas?