



AS AVENTURAS DE ALICE NO PAÍS DA CRIPTOGRAFIA


Uma introdução à criptografia...

Luiza Barros Reis Soezima

A green handwritten signature in a cursive script, appearing to read 'luiza'.

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)

O QUE É CRIPTOGRAFIA?



Criptografia é a ciência que estuda e elabora sistemas, técnicas e esquemas para realizar comunicação confiável em canais inseguros

Cript - o - grafia

kryptós

Esconder



gráphein

Escrita

ALGUNS PRINCÍPIOS DA CRIPTOGRAFIA

CONFIDENCIALIDADE

Apenas as partes autorizadas podem acessar as informação.

INTEGRIDADE

Os dados não são alterados ou corrompidos durante a transmissão ou armazenamento.

ALGUNS PRINCÍPIOS DA CRIPTOGRAFIA

NÃO REPUDIÇÃO


Uma entidade não pode negar seus compromissos ou ações prévias e nem a sua autenticidade.

AUTENTICIDADE

Identidade das partes envolvidas em uma comunicação ou transação seja verificada e confirmada.

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)

GLOSSÁRIO



CIFRA

Método utilizado para ocultar informações, transformando-as em algo ilegível para o leitor comum.

TEXTO PLENO

Texto original antes de qualquer transformação.

CIFRAR

Transformar o **texto pleno** em uma forma ilegível através da **cifra**.

GLOSSÁRIO



DECIFRAR

Processo inverso da codificação, onde o texto cifrado é transformado de volta para o **texto pleno**.

CRIPTOANÁLISE


Estuda como quebrar esquemas criptográficos.

CHAVE / CHAVE SECRETA

Informação secreta que permite cifrar e decifrar documentos.

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)



SENTA QUE LÁ
VEM HISTÓRIA...

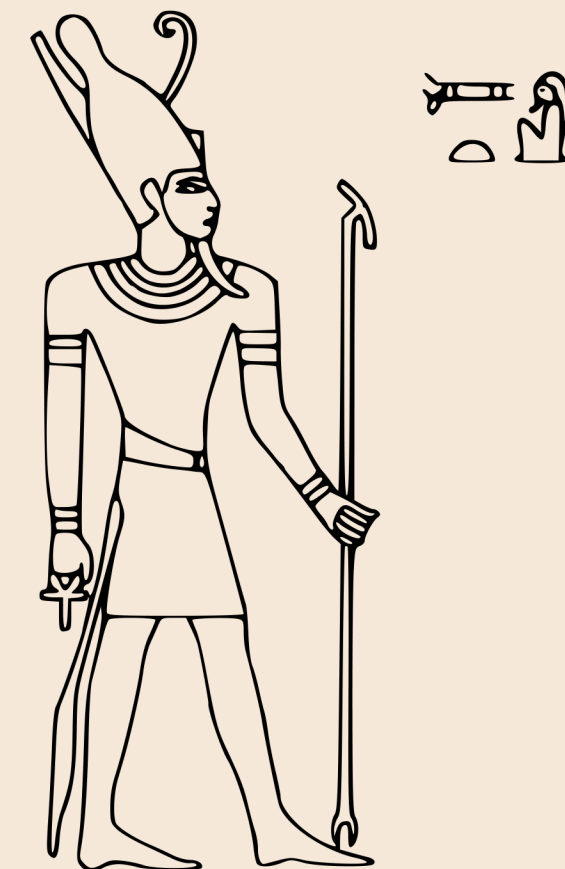
www

UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

HIERÓGLIFOS

Foram as primeiras evidências de criptografia. 4000 anos atrás



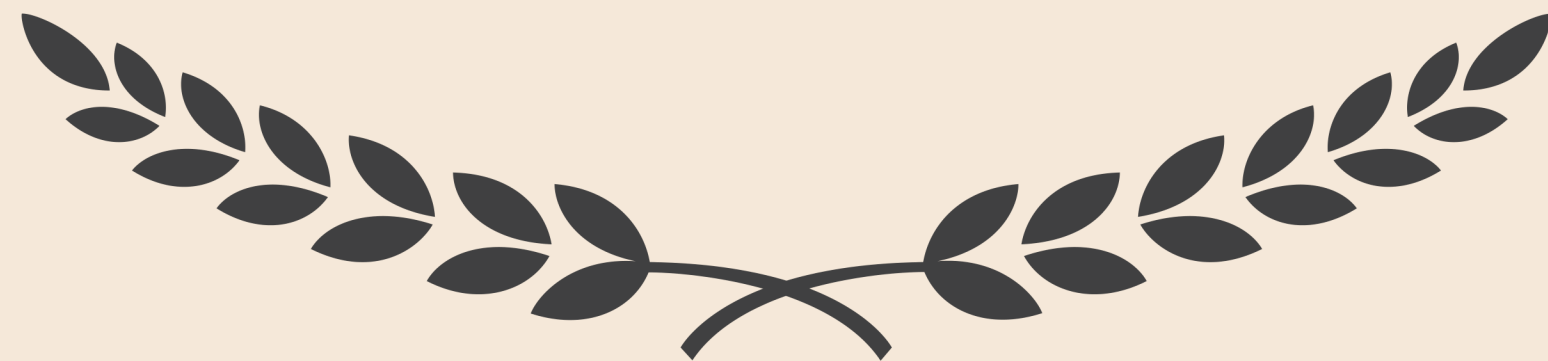
UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

CIFRA DE CÉSAR

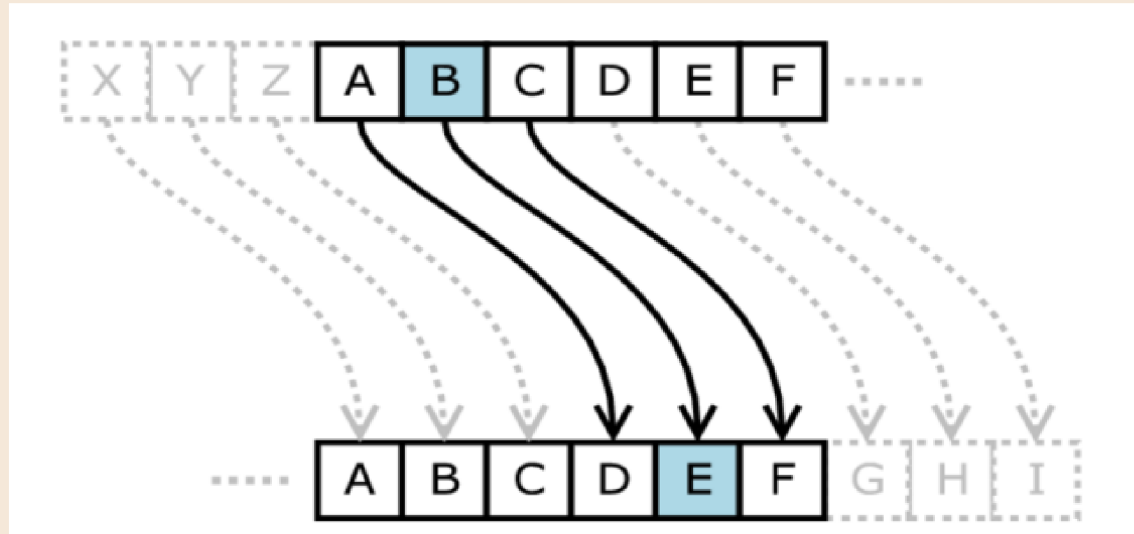


Técnica grega simples, baseada no deslocamento (shifting) de letras em uma mensagem. A quantidade de “casas” deslocadas é uma quantidade definida pelas partes.

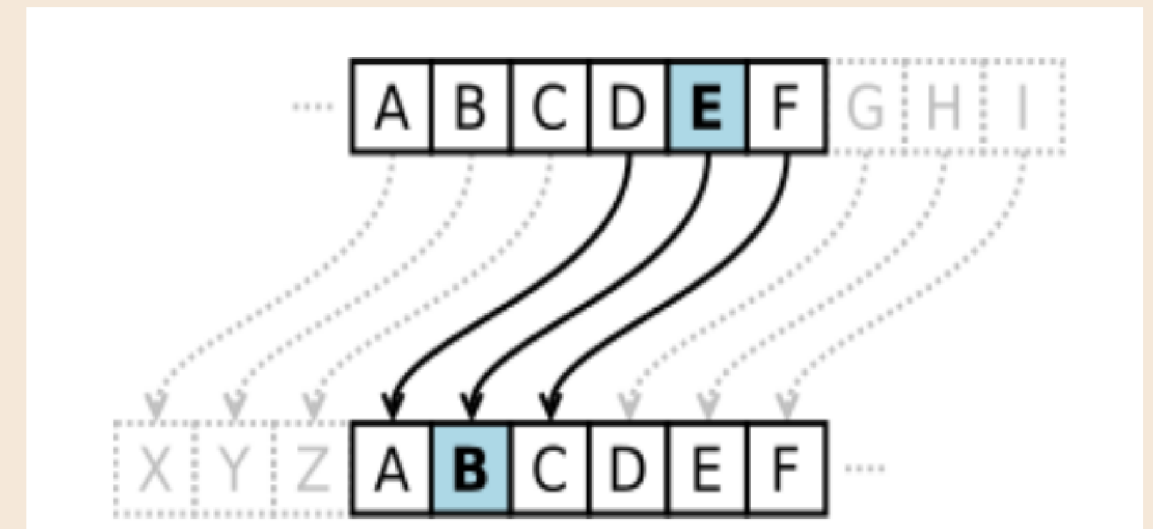


UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)



ENCRIPTAÇÃO



DECRIPTAÇÃO

UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

CIFRA DE VIGENÈRE

Sequência de várias cifras de César com diferentes valores de deslocamento.

Usamos uma tabela de alfabetos.

As 26 linhas correspondem às 26 possíveis cifras de César.

	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

UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

TEXTO: SOMOSINFORMATICA

CHAVE: LIMAOLIMAOLIMAOL

TEXTO ENCRIPADO:

DWYOGTVROFXIFIQL

A PRIMEIRA LETRA DO TEXTO, S, É CIFRADA USANDO O ALFABETO NA LINHA L, QUE É A PRIMEIRA LETRA DA CHAVE.

BASTA OLHAR PARA A LETRA NA LINHA L E COLUNA S NA TABELA DE VIGENÈRE, QUE É UM D.

PARA A SEGUNDA LETRA DO TEXTO, VER A SEGUNDA LETRA DA CHAVE: LINHA I E COLUNA O, QUE É W,

CONTINUANDO SEMPRE ATÉ OBTER: DWYOGTVROFXIFIQL

	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

UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

ENIGMA

Foi criada no final da primeira guerra para criptografar e descriptografar mensagens e serviu ao exército alemão para comunicações militares.



UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

A Enigma era um sistema mecânica que oferecia uma grande quantidade de configurações.

A cada dia, as configurações da Enigma eram alteradas, o que significava que os Aliados precisavam diariamente encontrar novas maneiras de quebrar o código.

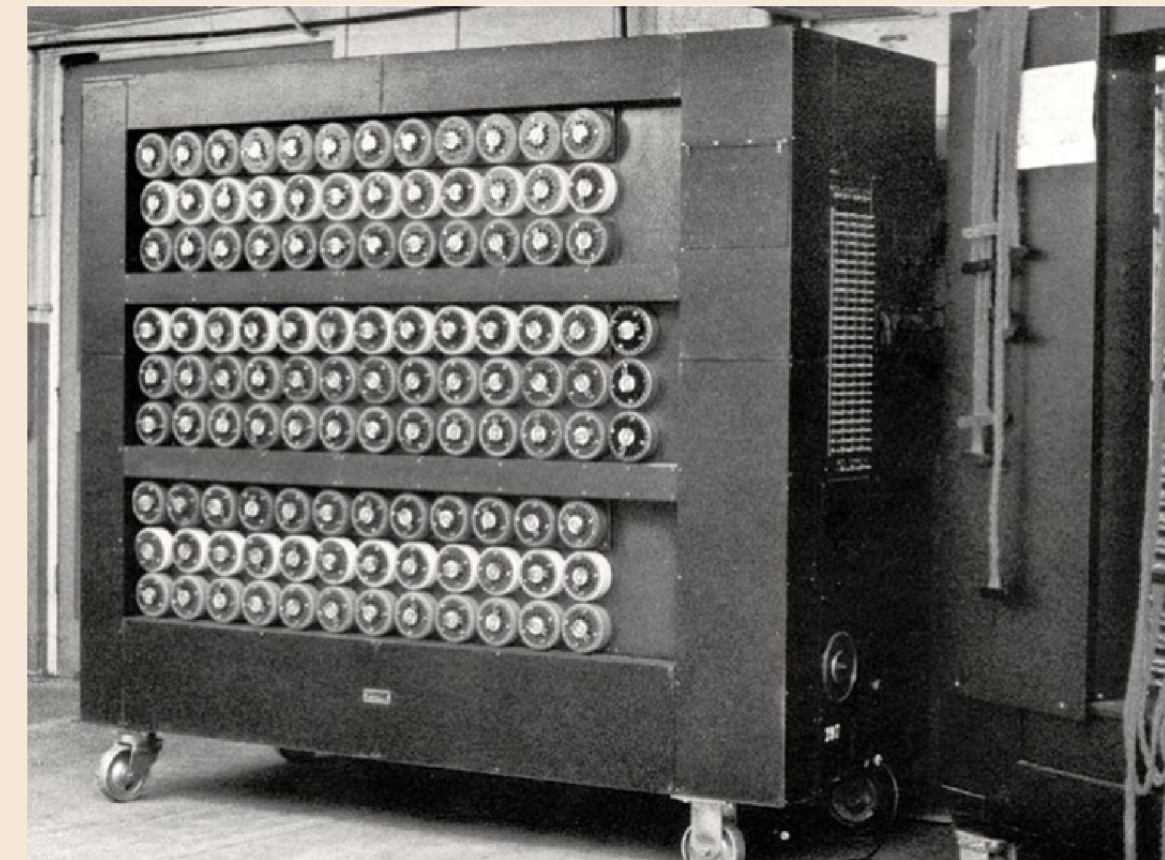
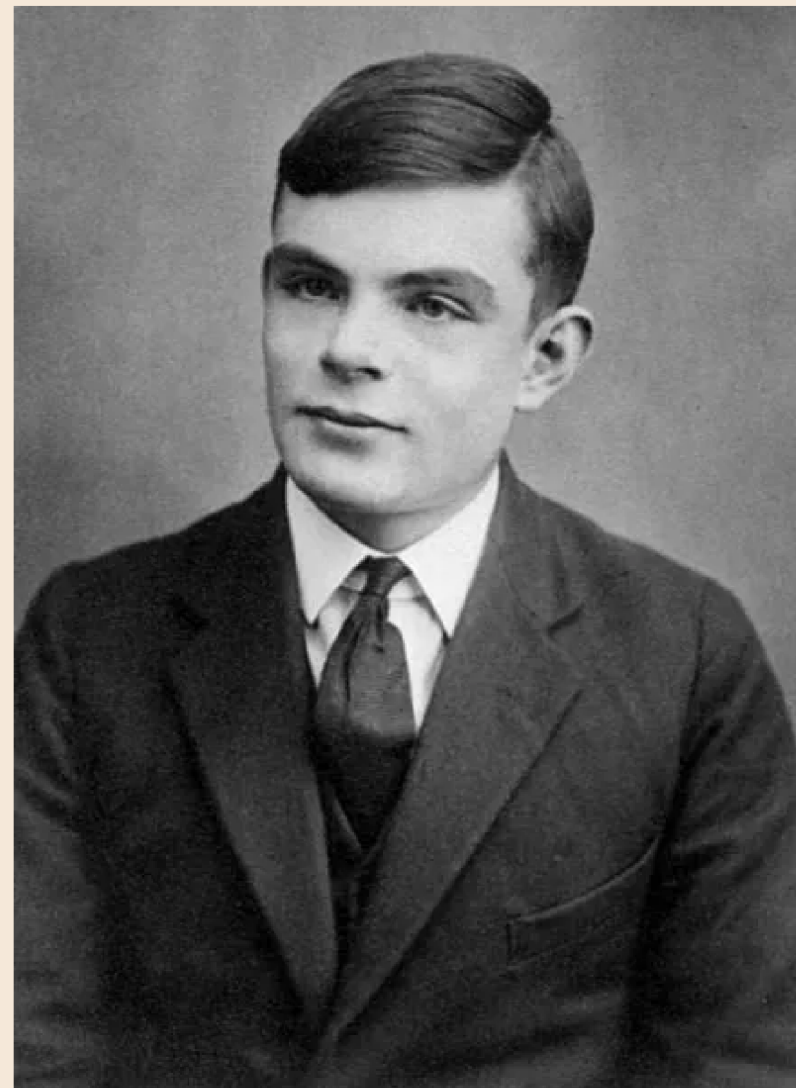
158,962,555,217,826
,360,000

UM POUCO DA HISTÓRIA DA CRIPTOGRAFIA

(e um pouco de história geral)

A Bombe, projetada por Alan Turing fez com que os Aliados conseguissem fazer avanços significativos na quebra da Enigma.

A Bombe tinha circuitos elétricos especializados, e conseguia testar milhares de combinações possíveis em busca das configurações corretas dos rotores e do plugboard da Enigma.



CRIPTOGRAFIA ANTIGA



Uso de símbolos e simbologias religiosas.



Apenas os escribas podiam ler e decifrar.



Segurança do sistema depende do fato de que os detalhes internos do protocolo ou algoritmo não são conhecidos por potenciais atacantes.

CRIPTOGRAFIA MODERNA

Uso de conceitos de teoria dos números e teoria da probabilidade.


Não é mais usada apenas para mensagens secretas, mas como forma de armazenar informações e transmiti-las de forma segura e exclusiva

O mundo online implica em comunicação e compartilhamento de dados pessoais, elevando a importância da proteção de dados pessoais.

A demonstração da segurança de um protocolo é baseada em provas matemáticas de independem do fato de o protocolo ser conhecido ou não

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)

ALGUNS PRINCÍPIOS TEÓRICOS

KERCKHOFF

O princípio de Kerckhoff afirma que a segurança de um sistema criptográfico não deve depender do sigilo do algoritmo, mas sim da chave secreta. Isso implica que a transparência do algoritmo é essencial para garantir a segurança.

SHANNON

A segurança perfeita afirma que uma cifra é inquebrável se a chave for aleatória, secreta e tão longa quanto a mensagem, garantindo assim uma segurança teoricamente impenetrável.

Entropia da Informação
+
One-time-pad

DIFFIE-HELLMAN

Método de troca de chaves que permite que duas partes estabeleçam uma chave sobre um canal de comunicação inseguro, sem precisar compartilhar previamente uma chave secreta.

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Alice

Bento

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Vamos escolher os parâmetros públicos:

- primo muito grande p , onde vamos trabalhar com Z_p
- inteiro gerador g , $g \in Z_p$

Esses parâmetros são compartilhados publicamente

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

g

Alice

g

Bento

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Cada parte gera a sua chave privada aleatória

- Alice gera a
- Bento gera b

Essas chaves são mantidas em segredo

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

g, a Alice

g, b Bento

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Cada parte agora calcula a sua chave pública correspondente

- Alice calcula $A = g^a \pmod p$
- Bento calcula $B = g^b \pmod p$

Essas chaves são mantidas em segredo.

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

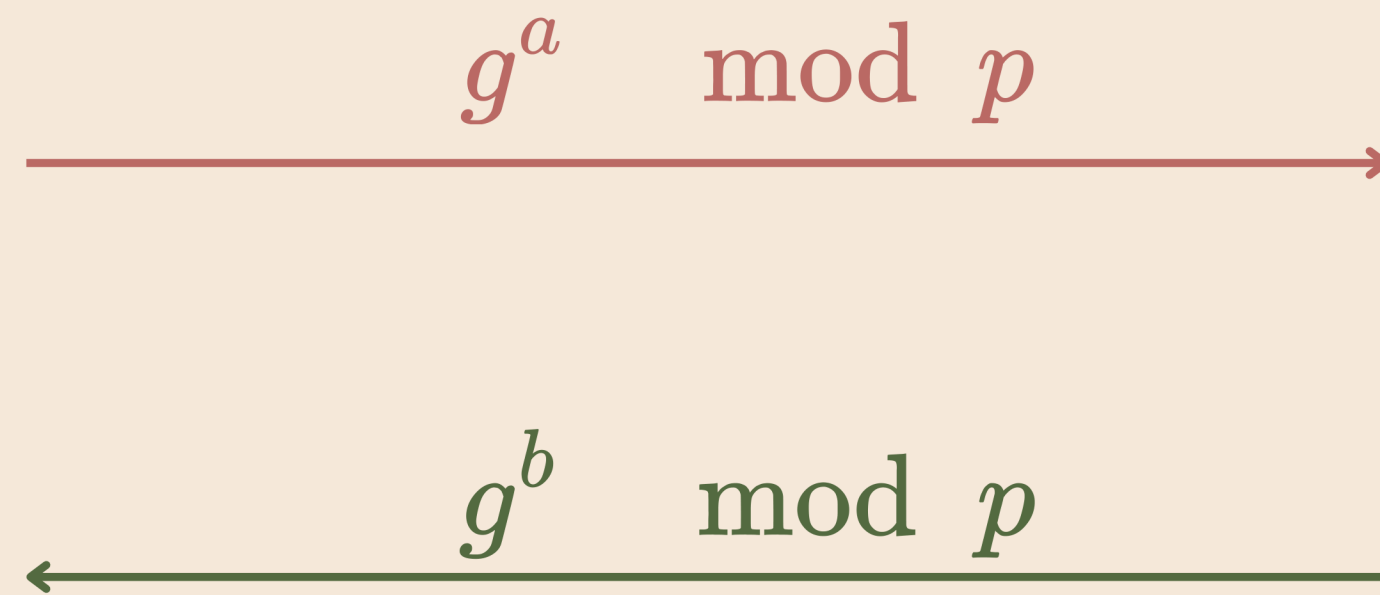
PROTOCOLO DIFFIE-HELLMAN

Alice e *Bento* , quando forem se comunicar, trocam suas chaves públicas pelo canal de comunicação inseguro.

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Alice
 g, a



Bento
 g, b

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

Cada parte utiliza a chave pública recebida de outra parte e sua própria chave privada para calcular a chave compartilhada

- Alice calcula $S = B^a \pmod p$
- Bento calcula $S = A^b \pmod p$

Agora, Alice e Bento possuem a mesma chave S compartilhada que pode ser usada para cifrar e decifrar mensagens

COMO ESTABELECEER UM SEGREDO COMPARTILHADO?

PROTOCOLO DIFFIE-HELLMAN

A segurança desse protocolo está na dificuldade matemática de se calcular o logaritmo discreto:

Dado um primo p e um gerador g , $h \in [1, p - 1]$

queremos encontrar um inteiro x (se é que ele existe),

$$\text{tal que } g^x \equiv h \pmod{p}$$

ALGUNS OUTROS PROBLEMAS MATEMATICAMENTE DIFICEIS

FATORAÇÃO DE INTEIROS

Dado um inteiro $N = pq$
encontrar os fatores primos p e q .

LOGARITMO DISCRETO EM CURVAS ELIPTICAS

Dada uma curva elíptica definida sobre E/F_q
e $P, Q \in E(F_{q^k})$
encontrar o valor de x (caso exista)
tal que $xP = Q$

ALGUMAS PRIMITIVAS

operações fundamentais usadas nos sistemas criptográficos

CIFRAR/DECIFRAR

Geralmente utiliza criptografia de chave secreta.

CRIAÇÃO DE CHAVE COMPARTILHADA

Uso do protocolo Diffie Hellman

ASSINATURA E VERIFICAÇÃO DE DOCUMENTOS

Geralmente usa a criptografia de chave pública.

TIPOS DE CRIPTOGRAFIA

CRIPTOGRAFIA DE
CHAVE SECRETA (OU
CRIPTOGRAFIA
SIMÉTRICA)

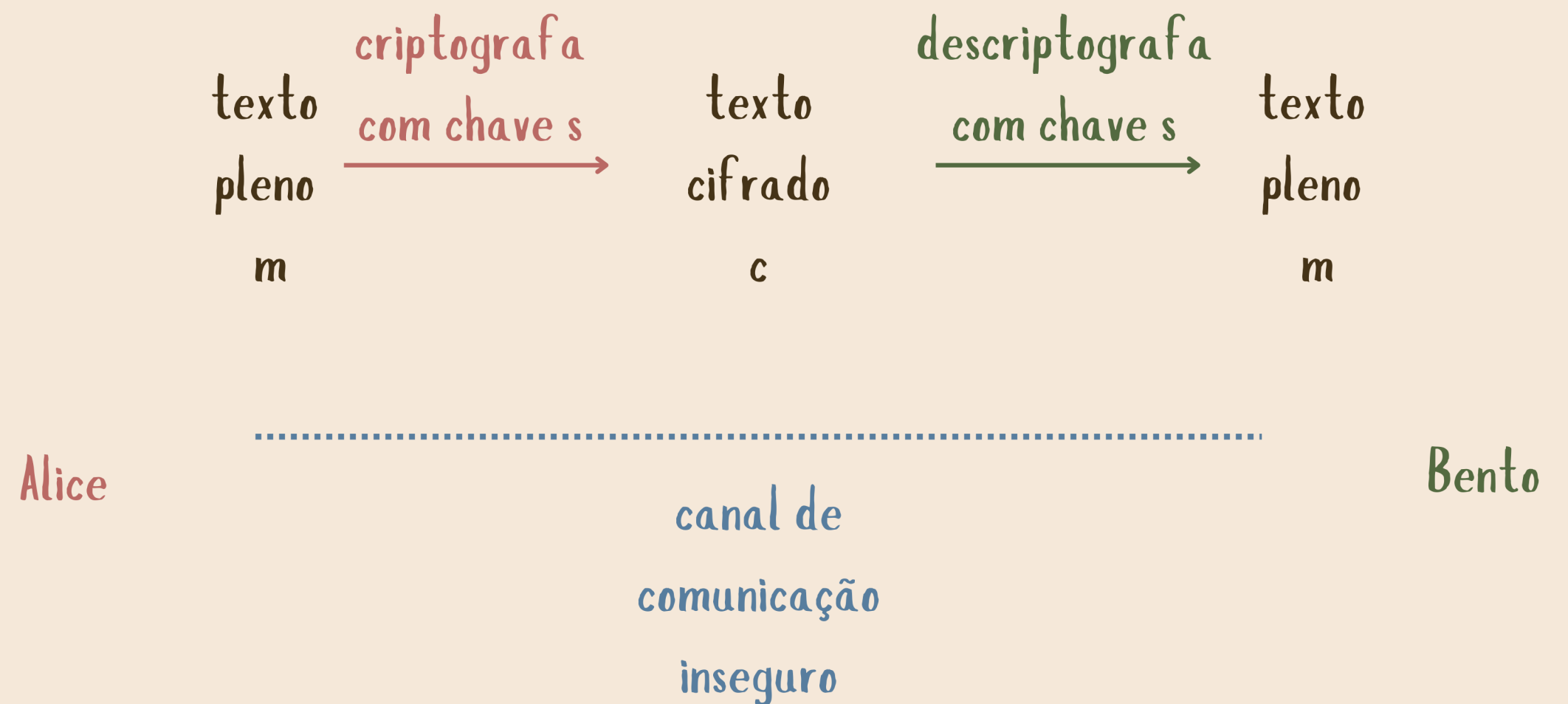
CRIPTOGRAFIA DE
CHAVE PÚBLICA
(OU CRIPTOGRAFIA
ASSIMÉTRICA)

FUNÇÕES HASH

TIPOS DE CRIPTOGRAFIA

CRIPTOGRAFIA DE CHAVE SECRETA

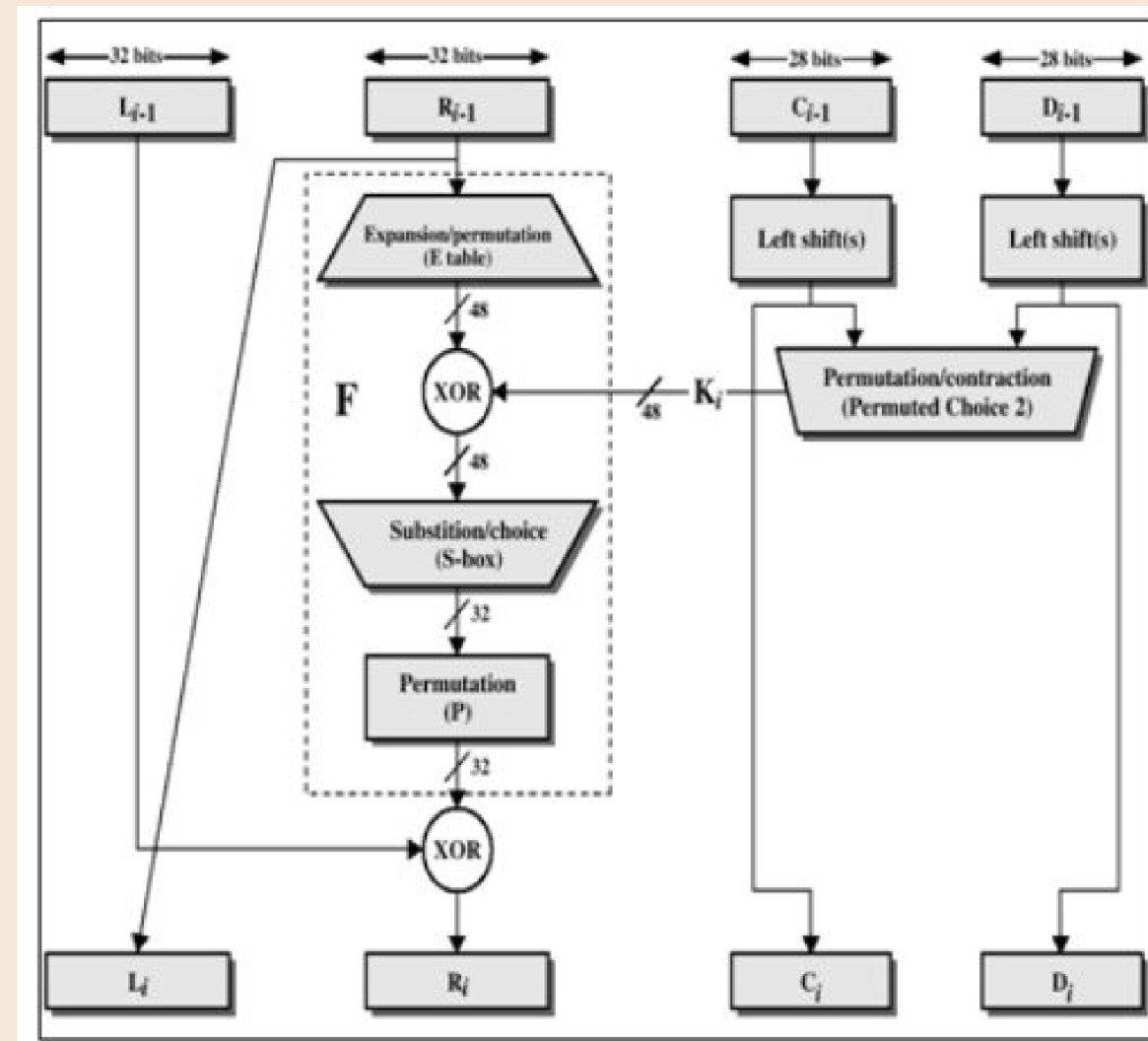
Todos os participante (quem envia e quem recebe a mensagem) tem a mesma chave. A chave é o pedaço de informação ou o parâmetro que determina a cifra.



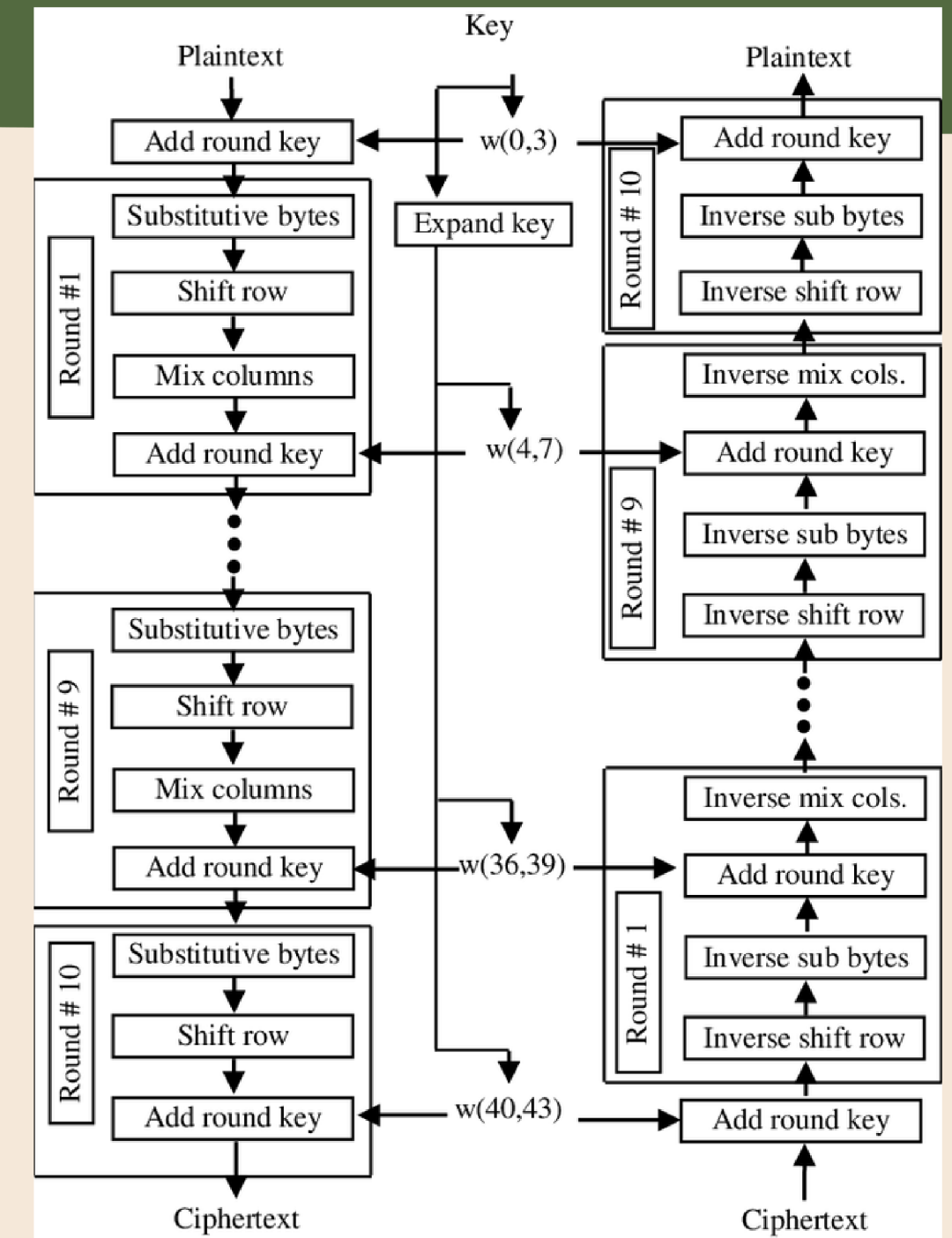
TIPOS DE CRIPTOGRAFIA

CRIPTOGRAFIA DE CHAVE SECRETA

Todos os participante (quem envia e quem recebe a mensagem) tem a mesma chave. A chave é o pedaço de informação ou o parâmetro que determina a cifra.



DES (DATA ENCRYPTION STANDARD)

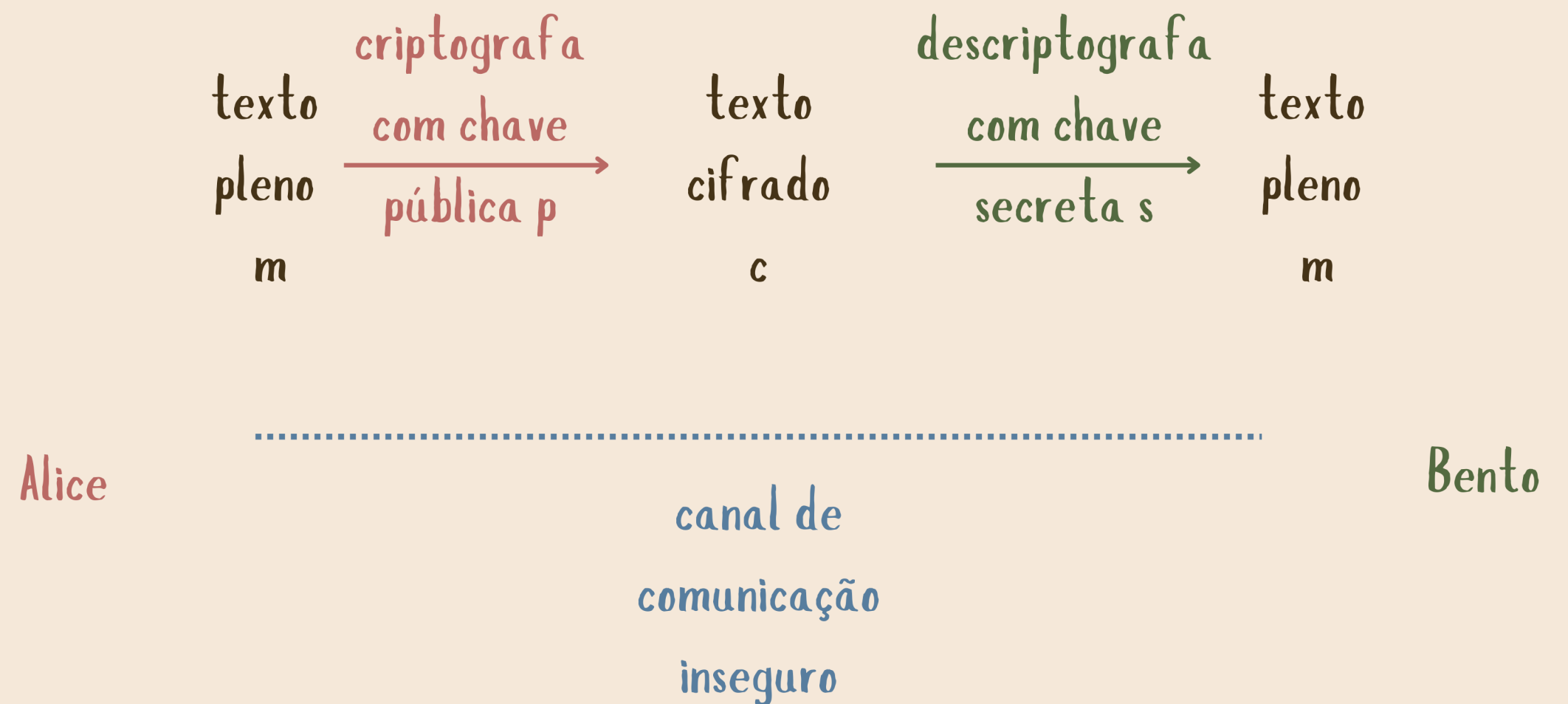


AES (ADVANCED ENCRYPTION STANDARD)

TIPOS DE CRIPTOGRAFIA

CRIPTOGRAFIA DE CHAVE PÚBLICA

As chaves dos participantes não são as mesmas. Cada participante possui uma chave pública e uma chave privada. A chave pública é usada para criptografar a mensagem e a chave privada é usada para descriptografar.



TIPOS DE CRIPTOGRAFIA

CRIPTOGRAFIA DE CHAVE PÚBLICA

As chaves dos participantes não são as mesmas. Cada participante possui uma chave pública e uma chave privada. A chave pública é usada para criptografar a mensagem e a chave privada é usada para descriptografar.

RSA Algorithm

Key Generation

Select p, q	p and q , both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod n$

RSA (RIVEST-SHAMIR-ADLEMAN)

EL GAMMAL

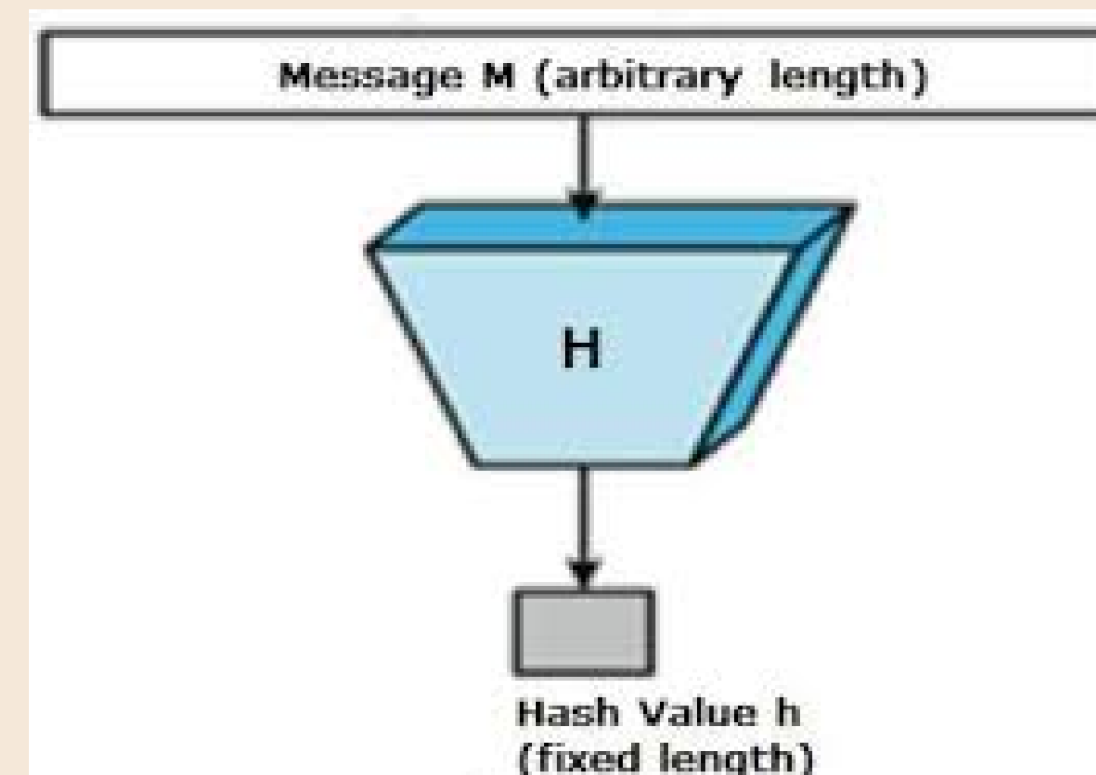
DSA (DIGITAL SIGNATURE ALGORITHM),

TIPOS DE CRIPTOGRAFIA

FUNÇÃO HASH

É uma função que usa um bloco arbitrário de dado e retorna uma bit string de tamanho fixo (hash criptografico) tal que mudar os dados de entrada, mudam o valor do hash.

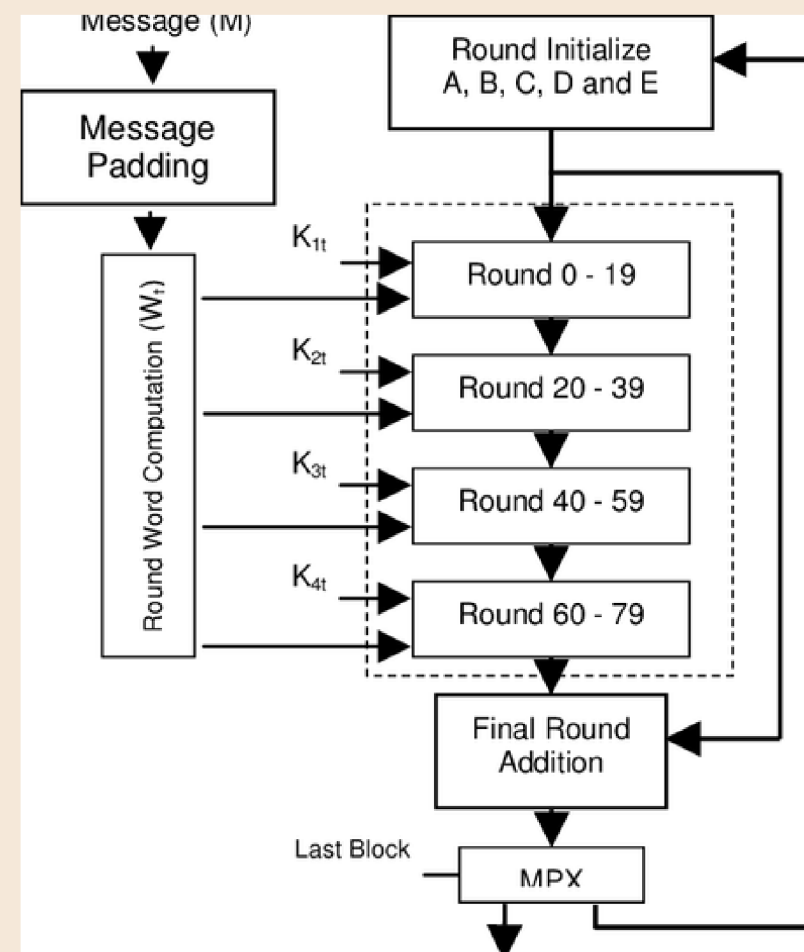
- Para qualquer mensagem, é fácil de calcular seu hash
- Dado o hash de uma função é impossível calcular a mensagem original
- É impossível modificar a mensagem sem modificar o hash também
- É impossível ter duas mensagens com o mesmo valor de hash



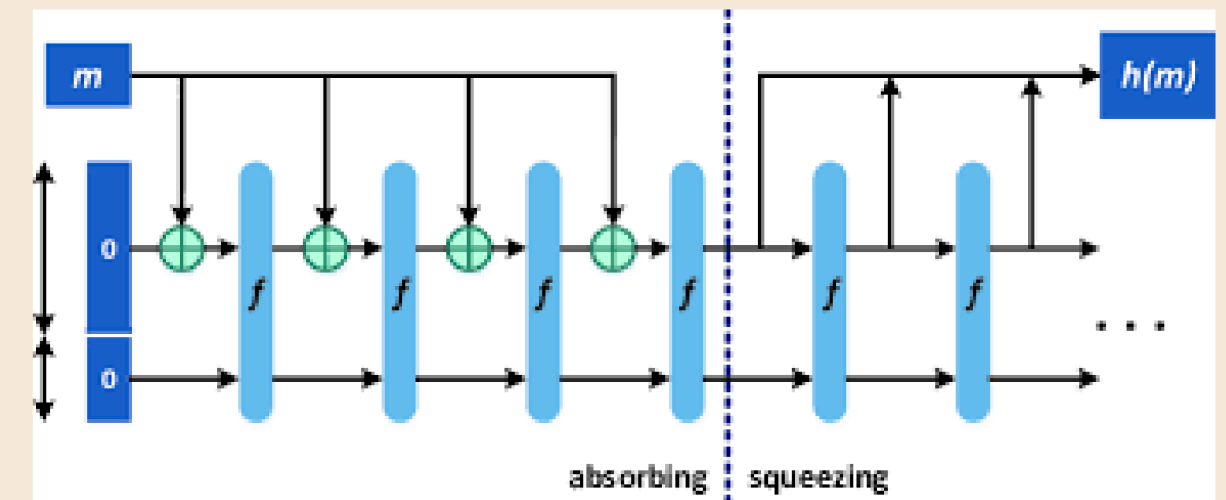
TIPOS DE CRIPTOGRAFIA

FUNÇÃO HASH

É uma função que usa um bloco arbitrário de dado e retorna uma bit string de tamanho fixo (hash criptografico) tal que mudar os dados de entrada, mudam o valor do hash.



SHA (SECURE HASH ALGORITHMS)



SHA-3 (SECURE HASH ALGORITHM 3) - KECCAK

IMPORTANTE!

1

Todos os esquemas existentes podem ser quebrados, basta que se tenha muuuuito tempo e poder computacional

2


Cada problema possui uma dificuldade matemática associada, assim como cada um é mais ou menos apropriado para determinada aplicação

3

A maioria dos ataques acontecem de dentro, ou seja, de alguém que tem acesso ao canal de comunicação de forma "invisível".

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)

TEMAS LEGAIS NA CRIPTOGRAFIA

(segundo a minha opinião)

PRIVATE INFORMATION RETRIEVAL

Recuperação segura de informações de uma base de dados sem revelar quaisquer detalhes sobre as consultas feitas.

MULTI-PARTY COMPUTATION

Envolve múltiplas partes interessadas que desejam realizar cálculos colaborativos sem revelar suas entradas originais.

ZERO- KNOWLEDGE PROOFS

Permitem que uma parte prove a validade de uma declaração sem revelar qualquer informação adicional além da própria validade.

TEMAS LEGAIS NA CRIPTOGRAFIA

(segundo a minha opinião)

CRIPTOGRAFIA HOMOMÓRFICA

Permite realizar operações matemáticas em dados criptografados sem descriptografá-los.

CURVAS ELÍPTICAS

Utiliza propriedades matemáticas de curvas elípticas para fornecer segurança em sistemas criptográficos, oferecendo eficiência em termos de uso de recursos computacionais e tamanho das chaves.

SECURE MESSAGING

Envolve o uso de protocolos criptográficos para garantir a confidencialidade, integridade e autenticidade das mensagens transmitidas em comunicações eletrônicas, como e-mails, mensagens instantâneas e chamadas de voz.


TEMAS LEGAIS NA CRIPTOGRAFIA

(segundo a minha opinião)

MUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUITOS OUTROS TEMAS

AGENDA

- # O que é criptografia?
- # Glossário
- # Histórico da Criptografia
- # Tipos de Criptografia
- # Temas legais dentro da criptografia
- # O futuro da criptografia e problemas modernos



Fiquem à vontade para interromper e tirar dúvidas ou perguntar o que quiserem :)



TA, MAS E
AGORA?



well



E O FUTURO...

COMPUTADORES QUÂNTICOS

Com o avanço na tecnologia de computação quântica, os algoritmos criptográficos atuais podem se tornar vulneráveis a ataques de computadores quânticos. A criptografia pós-quântica se torna essencial para garantir a segurança de longo prazo das comunicações digitais.

RSA

SSI/TLS(VPN)

Assinaturas digitais

Mais usada em proteção de arquivos

DSA

Certificados digitais

Mais usada em governos e setor financeiro

CURVAS ELIPTICAS

TLS/TTLS/SSL

Pagamento por aproximação

Redes sem fio

E O FUTURO...

PRIVACIDADE

Há o aumento das preocupações com a privacidade dos dados pessoais e regulamentações mais rígidas.

Existe o GDPR na Europa, a LGPD no Brasil, mas há uma crescente demanda por técnicas mais seguras

COMUNICAÇÕES

SEGURAS

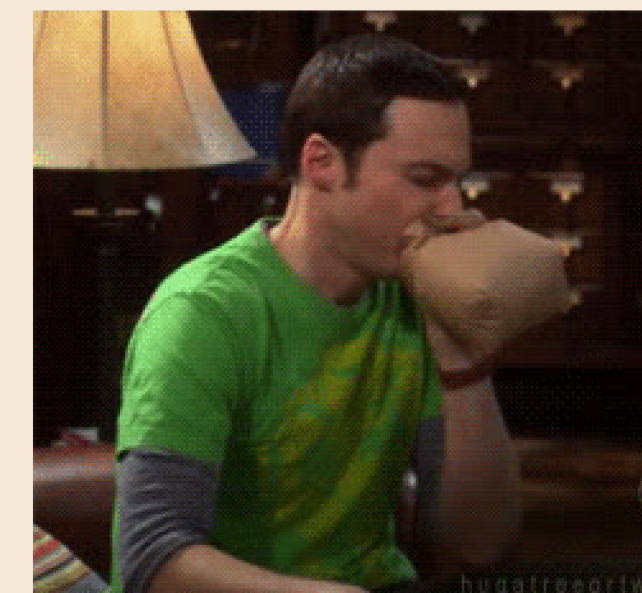
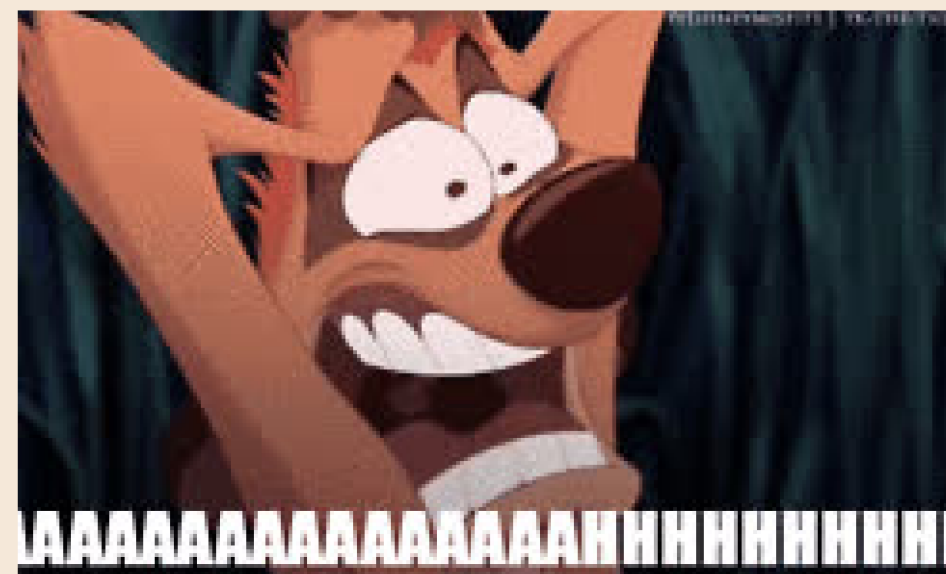
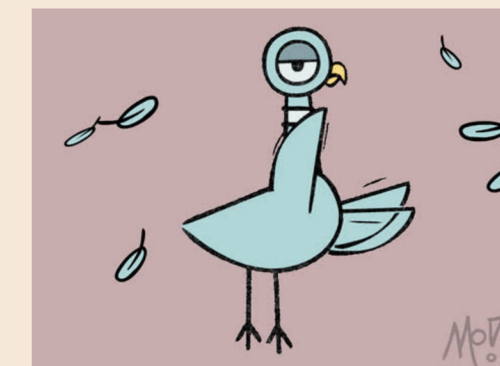
Monitoramento!

VIGILÂNCIA
URBANA

E O FUTURO...

NOVAS IMPLEMENTAÇÕES

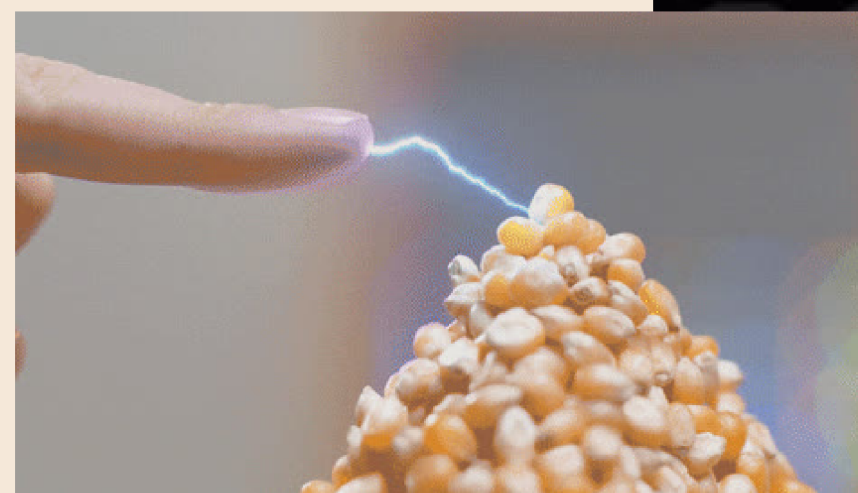
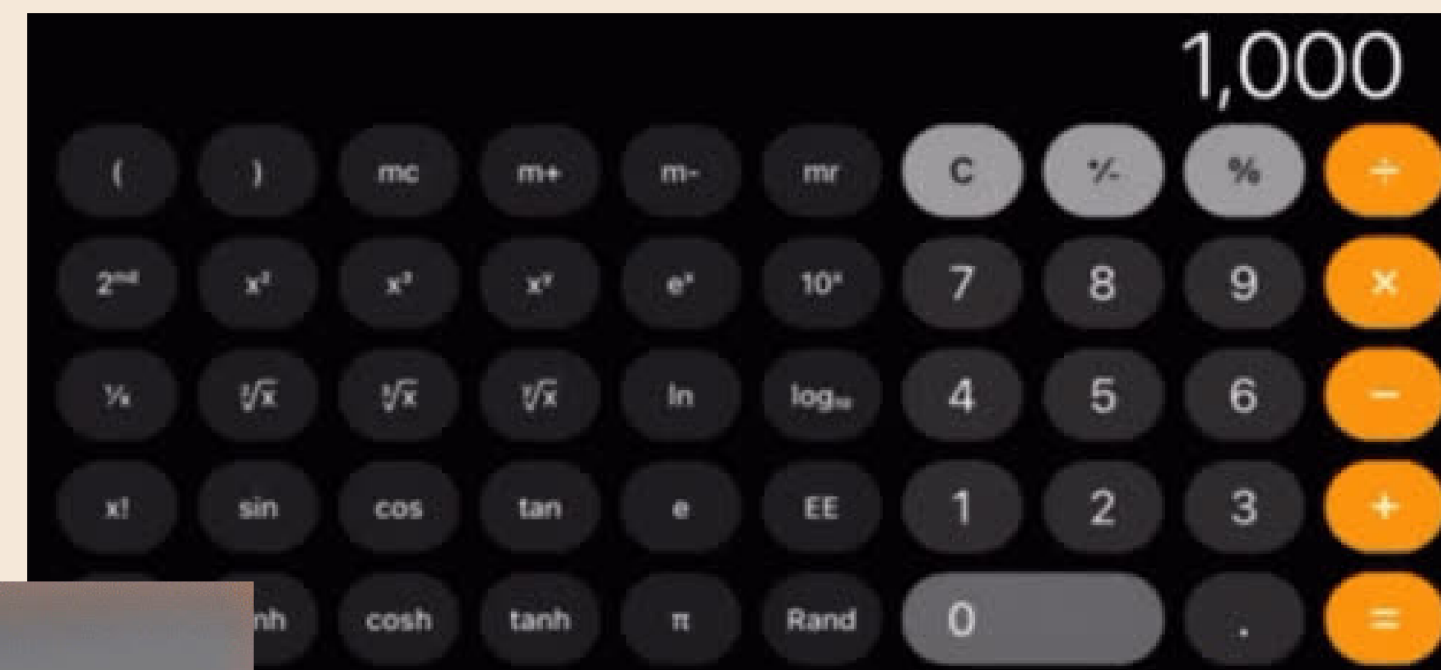
Com o avanço da tecnologia e o aumento da demanda por comunicações seguras e eficientes, há uma necessidade contínua de desenvolver implementações criptográficas mais rápidas, eficientes



E O FUTURO...

MAIS E MAIS DADOS

Com o rápido crescimento da quantidade de dados gerados e transmitidos digitalmente, a criptografia precisa lidar com desafios de escalabilidade e eficiência para garantir que os sistemas criptográficos possam lidar com grandes volumes de dados de maneira eficaz.



E O FUTURO...

ENGENHARIA SOCIAL

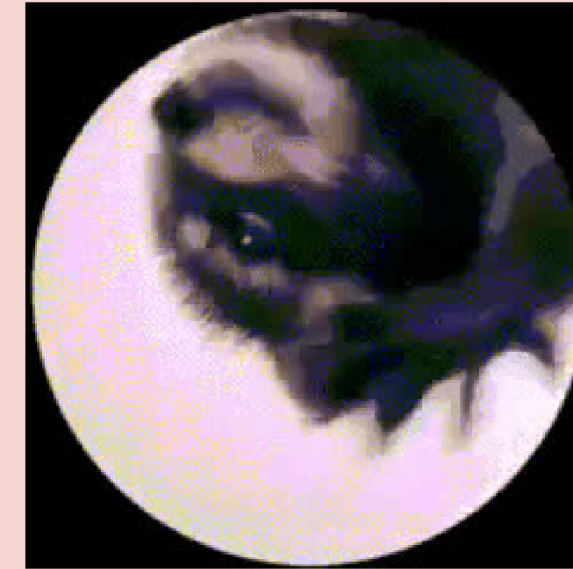
Os ataques de engenharia social continuam sendo uma ameaça significativa à segurança cibernética. Desenvolver técnicas criptográficas que ajudem a mitigar esses tipos de ataques e proteger os usuários contra manipulação e fraude é crucial.



Um pouco
sobre mim!



<https://luizabrs.github.io/>



GRADUAÇÃO

*ime-
USP*

Bacharelado em Ciência da
Computação
Maratona de Programação,
IC e RD(CG e MAC)

MESTRADO

*Ensimag
- UGA*

MSc. Cybersecurity
Início em set. 2024

ALGUNS LIVROS LEGAIS



- # Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography (2nd ed.). CRC Press.
- # Terada, R. Segurança de dados: criptografia em redes de computador. São Paulo: Edgard Blucher, 2000. (O RT é professor aqui no IME)
- # Stinson, D.R., & Paterson, M. (2017). Cryptography: Theory and Practice (4th ed.). Chapman and Hall/CRC.
<https://doi.org/10.1201/9781315282497>
- # Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.

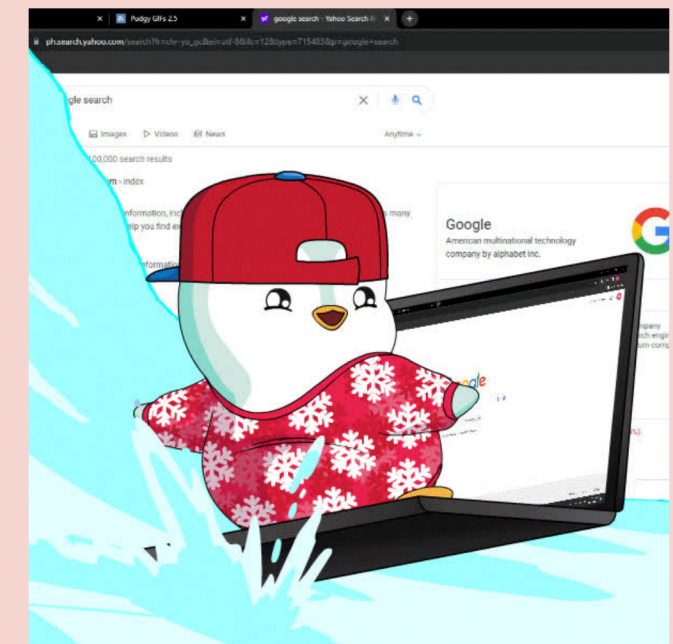
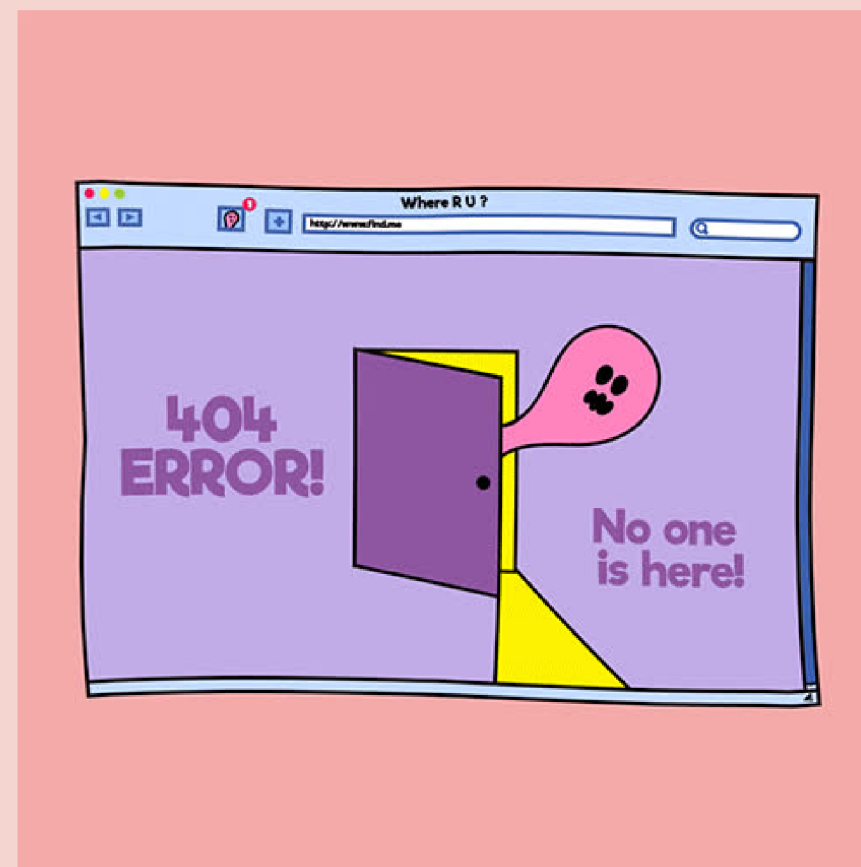
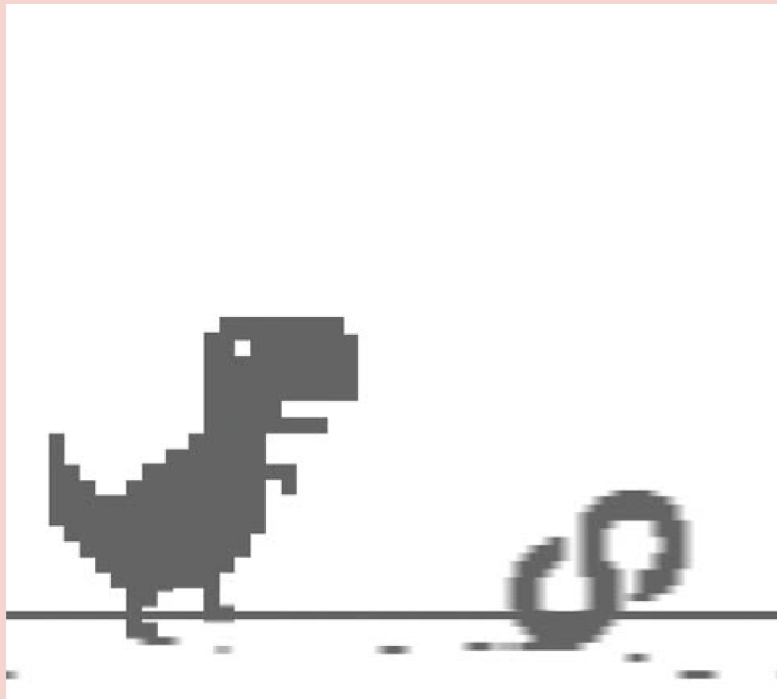


ALGUNS SITES LEGAIS

<https://www.dcode.fr/en>

<https://www.geeksforgeeks.org/cryptography-introduction/>

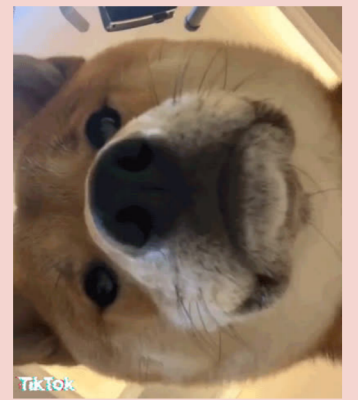
<https://www.youtube.com/@Computerphile>





alguns eventos

muito legais!



RE-IMAGINING CRYPTOGRAPHY & PRIVACY



★ WORKSHOP ★

WHAT: a SPACE to EXPLORE the ways in which DIGITAL PRIVACY TECHNOLOGIES INTERSECT with HUMAN EXPERIENCES, STRATEGIZE toward DISMANTLING SYSTEMS of TECH-FACILITATED MARGINALIZATION, & DREAM of ways we can LEVERAGE TECH to SUSTAIN LIVES & LIVELIHOODS.

WHEN: MAY 2-3 from 9AM-5PM

WHERE: TUFTS UNIVERSITY & ZOOM

WHO : OPEN to ALL who REGISTER → recapworkshop.online



BIBLIOTECA MARIO DE ANDRADE

10 E 11 DE MAIO



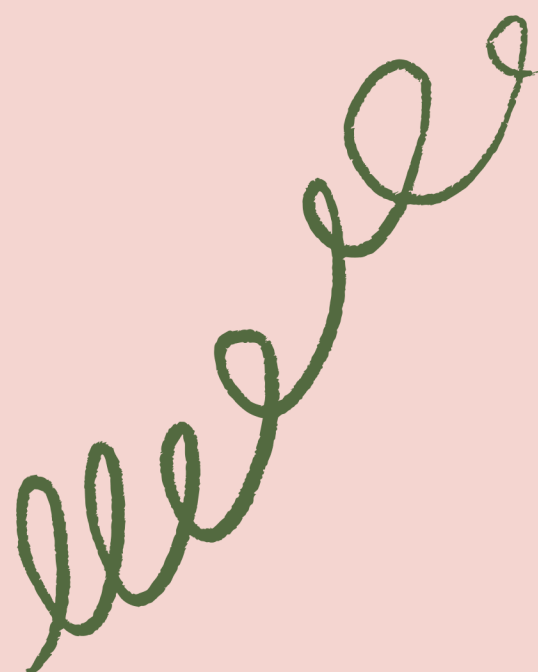
NÃO PERCAM!



Como usar o ChatGPT para
proteger a minha rede de
computadores?

Prof. Daniel Batista

4ªf. 15:15 - 16:15



Como Newton se protegeria
de um espião quântico

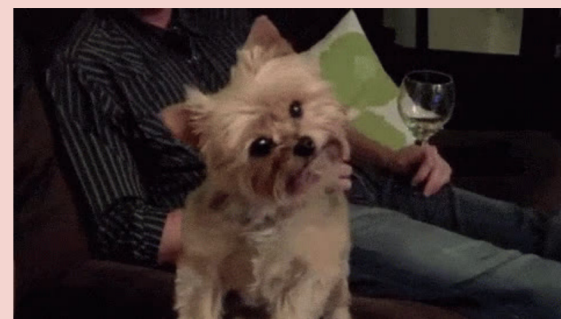
Hilder Vitor Lima Pereira

6ªf. 14:00 - 15:00



Obrigada :)

Perguntas?



lllll