

Criptografia simétrica

Segurança Computacional

Prof. Carlos Maziero

DInf UFPR, Curitiba PR

2019 - 2025

Conteúdo

- 1 Conceitos básicos
- 2 Cifragem e decifragem
- 3 Algoritmos simétricos

Conceitos básicos

Criptografia

Origem da palavra:

- **Cryptos**: escondido, oculto
- **Graphos**: escrita

Técnicas para garantir a confidencialidade de dados

Também podem prover integridade e autenticidade

Não confundir com **esteganografia**!

Criptografia

Áreas de estudo:

- **Criptografia:** técnicas para codificar informações
- **Criptanálise:** técnicas para “quebrar” codificações
- **Criptologia:** área geral (criptografia + criptanálise)
- **Criptossistema:** conjunto de algoritmos para um tipo específico de criptografia

Criptografia

Elementos básicos:

- **Texto aberto:** informação a codificar (x)
- **Texto cifrado:** informação codificada (x')
- **Chave:** informação complementar secreta (k)
- **Cifrar:** transformar o texto aberto em cifrado ($x \xrightarrow{k} x'$)
- **Decifrar:** transformar o texto cifrado em aberto ($x' \xrightarrow{k} x$)
- **Cifrador:** mecanismo para cifrar/decifrar a informação

Notação matemática

Cifrar um texto aberto x usando uma chave k :

$$x' = \{x\}_k$$

Decifrar um texto cifrado x' usando uma chave k :

$$x = \{x'\}_k^{-1}$$

Cifragem e decifragem

O cifrador de César

Usado por Júlio César para se comunicar com seus generais

Cifrador de César com chave k

Cada caractere do texto aberto é substituído pelo k -ésimo caractere sucessivo no alfabeto

Exemplo:

Msg aberta m : Reunir todos os generais para o ataque
 m' com $k = 1$: Sfvojs upept pt hfofsbjt qbsb p bubrvf
 m' com $k = 2$: Tgwpkt vqfqu qu igpgtcku rctc q cvcswg
 m' com $k = 3$: Uhxqlu wrgrv rv jhqhudlv sdud r dwdtxh

O cifrador de César

Para decifrar uma mensagem é necessário:

- A mensagem cifrada m'
- O valor de k usado para cifrar m (*chave criptográfica*)

ou:

- Testar todos os valores possíveis para k
- Análise exaustiva (*brute force analysis*)

Espaço de chaves

Keyspace: número de chaves possíveis em um cifrador

O espaço de chaves do cifrador de César é 26 (alfabeto)

A análise de força bruta é trivial!

Princípio de Kerckhoffs (1883)

O segredo de uma técnica criptográfica não deve residir no algoritmo em si, mas no **espaço de chaves** que ele provê

Espaço de chaves

A criptografia moderna:

- se baseia em algoritmos públicos bem avaliados
- usa espaços de chaves MUITO grandes
- torna inviável a análise exaustiva

Exemplo: AES com chaves de 128 bits: 2^{128} chaves possíveis

340.282.366.920.938.463.463.374.607.431.768.211.456 chaves!

Testando um bilhão (10^9) de chaves por segundo, precisaremos de **10 sextilhões de anos** para testar todas as chaves!

O cifrador de Vernam-Mauborgne

Inventado por Gilbert Vernam e Joseph Mauborgne em 1917

Também conhecido como “One-Time Pad”

Princípio:

- operação XOR ($\oplus$) entre o texto aberto e uma chave
- o texto e a chave devem ter o mesmo tamanho t
- espaço de chaves: 2^t

O cifrador de Vernam-Mauborgne

Seja uma mensagem x e uma chave k , ambas com t bytes:

Operação de **cifragem**:

$$x' = x \oplus k, \text{ ou seja, } \forall i \in [1...t], x'_i = x_i \oplus k_i$$

Operação de **decifragem**:

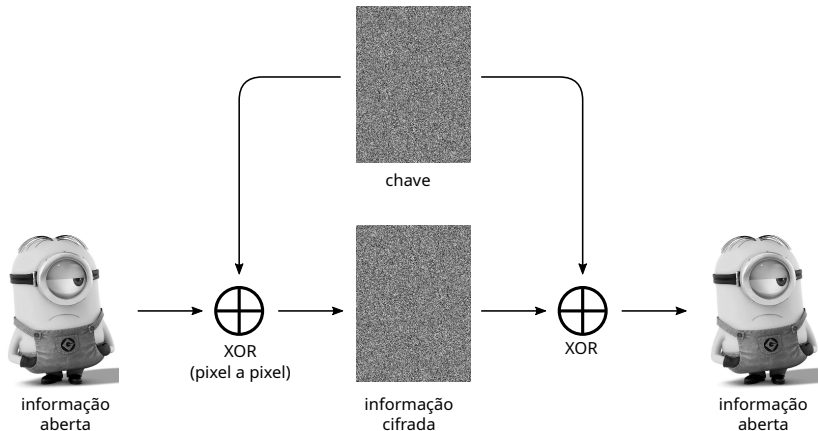
$$x = x' \oplus k, \text{ ou seja, } \forall i \in [1...t], x_i = x'_i \oplus k_i$$

Exemplo com m="TOMATE" e k="ABCDEF"

x (texto)	T	O	M	A	T	E
k (chave)	A	B	C	D	E	F
x (ASCII)	84	79	77	65	84	69
k (ASCII)	65	66	67	68	69	70
x (bin)	01010100	01001111	01001101	01000001	01010100	01000101
k (bin)	01000001	01000010	01000011	01000100	01000101	01000110
$x' = x \oplus k$	00010101	00001101	00001110	00000101	00010001	00000011
x' (ASCII)	21	13	14	5	17	3

x'	00010101	00001101	00001110	00000101	00010001	00000011
k (chave)	01000001	01000010	01000011	01000100	01000101	01000110
$x' \oplus k$	01010100	01001111	01001101	01000001	01010100	01000101
(ASCII)	84	79	77	65	84	69
(texto)	T	O	M	A	T	E

O cifrador de Vernam-Mauborgne



O cifrador de Vernam-Mauborgne

É o único cifrador realmente “inquebrável”!

Requisitos da chave:

- ser realmente aleatória
- ser mantida secreta
- **ter o mesmo tamanho da informação a cifrar**
- **nunca ser reutilizada**

Pouco usado, devido a essas restrições

Algoritmos simétricos

Algoritmos simétricos

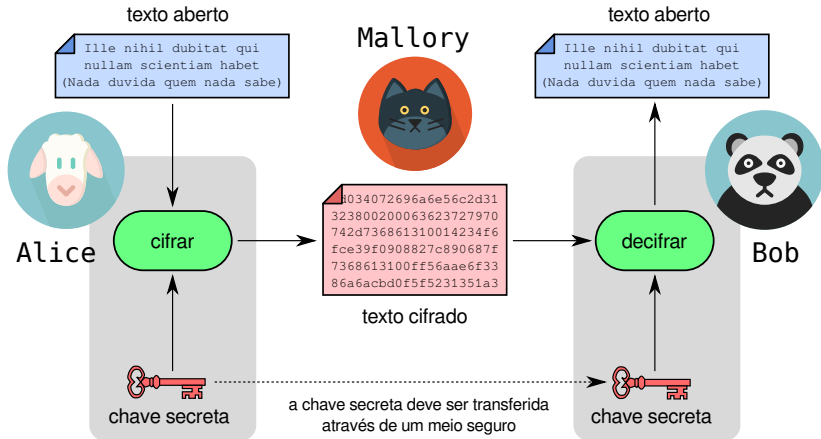
A mesma chave k é usada para cifrar e decifrar a informação:

$$\{ \{ x \}_k \}_{k'}^{-1} = x \iff k' = k$$

ou

$$x \xrightarrow{k} x' \xrightarrow{k} x$$

Algoritmos simétricos



Exemplos de algoritmos simétricos

- Cifradores de César e de Vernam-Mauborgne
- DES (*Data Encryption Standard*)
 - criado pela IBM nos anos 1970
 - usa chaves de 56 bits
- 3-DES: variante do DES com chaves de 168 bits
- AES (*Advanced Encryption Standard*):
 - padrão de segurança do governo americano (2002)
 - usa chaves de 128, 192 ou 256 bits
 - Muito usado na Internet e em cifragem de disco
- A5/1, A5/2, A5/3:
 - usados em telefonia celular GSM (cifragem de áudio)

Tipos de algoritmos simétricos

Quanto à estratégia de cifragem:

- Cifradores de **substituição**
 - Monoalfabéticos ou Polialfabéticos
 - Monográficos ou Poligráficos
- Cifradores de **transposição**

Quanto ao agrupamento dos dados:

- Cifradores de **fluxo**
- Cifradores de **bloco**

Cifradores de substituição

- Bytes da mensagem são substituídos usando regras
- Visam aumentar a *confusão* dos dados (Shannon)
- Podem ser mono- ou polialfabéticos
- Exemplos: Cesar cipher, Vigenère, Alien language (Futurama)

Cifradores polialfabéticos

Usam mais de uma tabela de substituição (“alfabeto”)

Exemplo clássico: cifrador de Vigenère

- Proposto por Giovan Battista Bellaso em 1553
- Refinado por Blaise de Vigenère no século XIX
- Combina vários cifradores de César em sequência
- Usa uma tabela chamada *tabula rasa*

O cifrador de Vigenère

		mensagem																									
		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
palavra-chave	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

O cifrador de Vigenère

Passos:

- 1 Escolher uma palavra-chave qualquer (BICICLETA)
- 2 Repetir a chave até ter o mesmo comprimento da msg
- 3 Para cada caractere da mensagem:
 - 1 escolher linha da tabela indicada pela letra da chave
 - 2 Codificar o caractere da mensagem usando aquela linha

Exemplo:

Palavra-chave	BICICLET	AB	IC	IC	LE	TAB	BIC	IC	LE	TAB	IC	IC	L
Texto aberto	A	T	A	C	A	R	E	M	O	S	A	O	A
Texto cifrado	B	B	C	K	C	C	I	F	O	T	I	Q	I

Cifradores de transposição

- Partes da mensagem são trocados entre si usando regras
- Visam aumentar a *difusão* dos dados (Shannon)

Exemplo: Cifragem “Rail Fence”

Texto aberto: WEAREDISCOVEREDFLEEATONCE

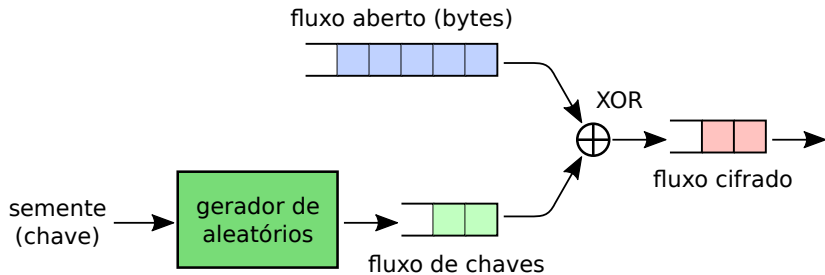
W	.	.	.	E	.	.	.	C	.	.	.	R	.	.	.	L	.	.	.	T	.	.	.	E
.	E	.	R	.	D	.	S	.	O	.	E	.	E	.	F	.	E	.	A	.	O	.	C	.
.	.	A	.	.	.	I	.	.	.	V	.	.	.	D	.	.	.	E	.	.	.	N	.	.

Texto cifrado ($k = 3$): WECRLTEERDSOEFEAOCAIVDEN

Cifradores de fluxo

- Cifram os dados byte a byte, em sequência
- Importantes para multimídia, VoIP, etc
- Inspirados do cifrador “one-time pad”
- Chave produzida por gerador pseudo-aleatório
- Exemplos: RC4, A5/1

Cifradores de fluxo

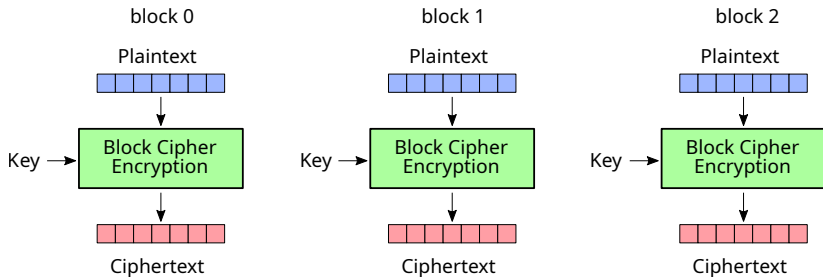


Cifradores de bloco

- Cifram os dados em blocos de mesmo tamanho
- Blocos usuais entre 64 e 128 bits
- Adequados para protocolos de rede, arquivos em disco
- Vários modos de operação: ECB, CBC, CFB, OFB, ...
- Exemplos: DES, 3DES, AES

Cifradores de bloco

Modo ECB - *Electronic Codebook*



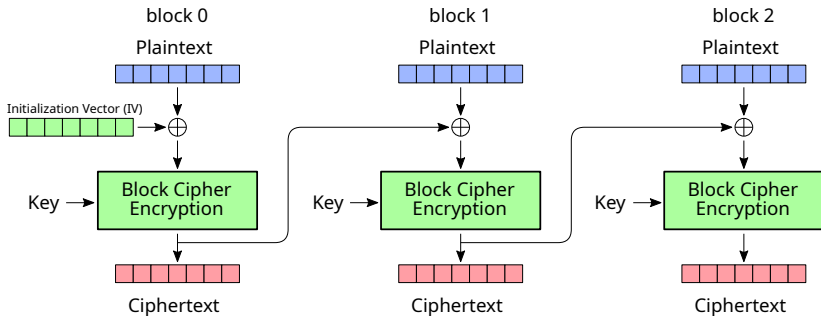
Algoritmos simétricos

Modo ECB - *Electronic Codebook*



Algoritmos simétricos

Modo CBC - *Cipher Block Chaining*



Algoritmos simétricos

Modo CBC - *Cipher Block Chaining*



Algoritmos simétricos

Características:

- São geralmente muito rápidos
- Usam chaves pequenas (80-256 bits)
- Muito usados na cifragem de dados
 - arquivos em um disco
 - pacotes de rede
 - fluxos multimídia

Exemplos: AES, 3-DES, Serpent, Blowfish, ...

Problema: Como enviar a chave através da rede?