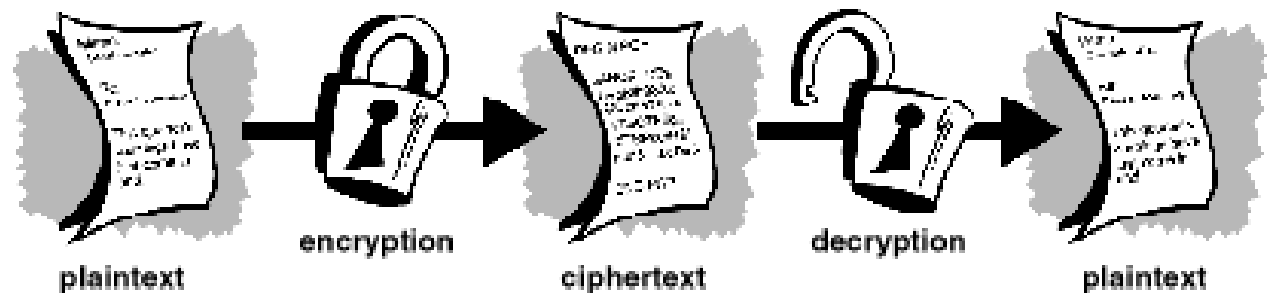


# Arquitetura e Organização de Sistemas Computadorizados - Criptologia

**Osmar de Oliveira Braz Junior**

**Márcia Cargnin Martins Giraldi**





# Objetivos

- Apresentar a criptologia e conceitos para criptografar e desincryptografar.

# Enigma



# Máquina de Rotor

- Este algoritmo de criptografia foi utilizado durante a Segunda Guerra Mundial pelos alemães (**Enigma**) e pelos japoneses (**Purple**). O fato dos aliados terem conseguido quebrar estes códigos foi um dos fatores decisivos para o resultado final da disputa.
- A Máquina de Rotor consiste de um conjunto de cilindros independentes. Estes cilindros possuem 26 entradas e 26 saídas, sendo que as conexões internas interligam cada conector de entrada a um único conector de saída. Assim, cada cilindro define uma substituição mono-alfabética.
- Após a entrada de uma letra, o rotor mais externo gira de uma posição, modificando a substituição a ser utilizada na próxima entrada. Quando o rotor mais externo completar uma volta, o rotor seguinte gira de uma posição. Assim, todos os cilindros da máquina giram em frequências diferentes. Veja o funcionamento da Máquina de Rotor no simulador.
- Uma máquina com três rotores apresenta **17.576** ( $26 \times 26 \times 26$ ) diferentes substituições, antes de haver qualquer repetição!

# Criptografia - Objetivo

- O objetivo principal da **criptografia** é prover **confidencialidade**. Contudo, também é possível obter autenticação, integridade, e não-repudição.
- **Dois** tipos de informação podem ser protegidas pela criptografia: **informações armazenadas** no sistema e **informações que estejam em trânsito** de um sistema para outro.

# Criptologia

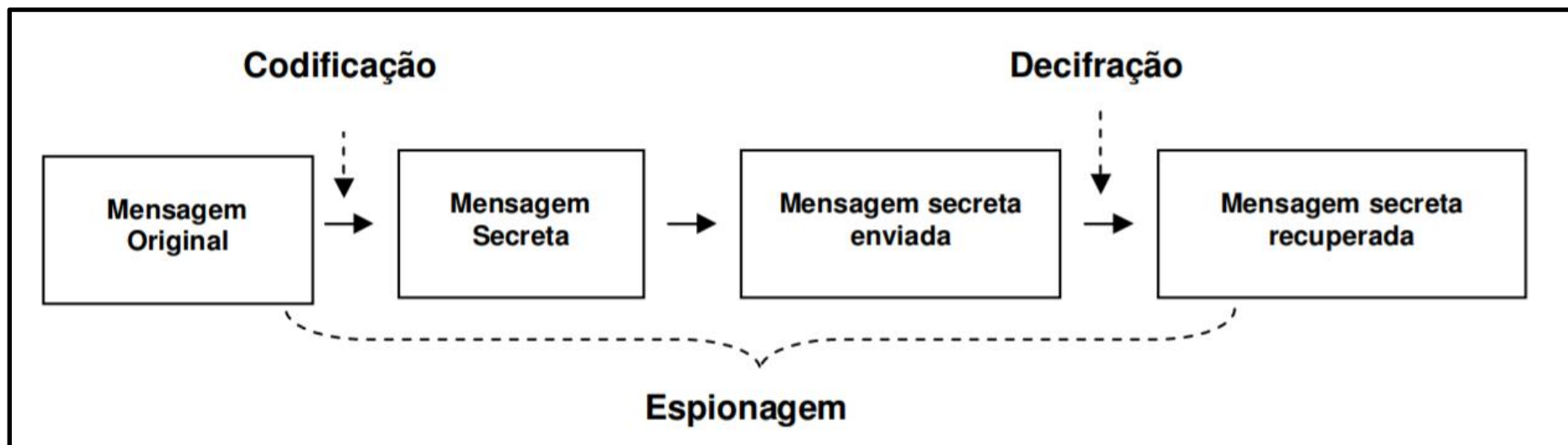
- É a arte ou a ciência de escrever em cifra ou em código; em outras palavras, ela abarca o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e a compreenda.



# Criptologia - Aplicações

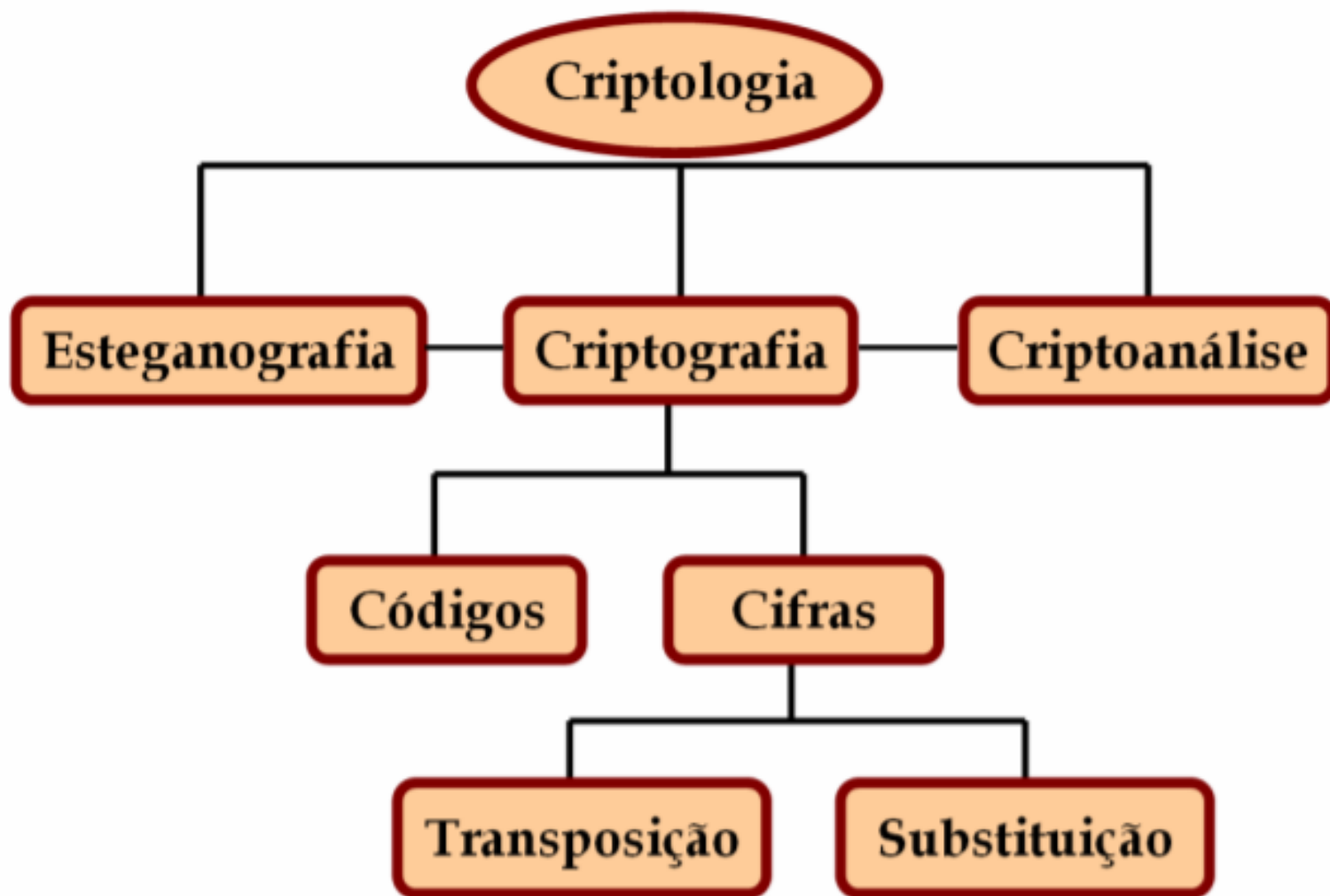
- sigilo em banco de dados;
- censos;
- investigações governamentais;
- dossiês de pessoas sob investigação;
- dados hospitalares;
- informações de crédito pessoal;
- decisões estratégicas empresariais;
- sigilo em comunicação de dados;
- comandos militares;
- mensagens diplomáticas;
- operações bancárias;
- comércio eletrônico;
- transações por troca de documentos eletrônicos (EDI);
- estudo de idiomas desconhecidos;
- recuperação de documentos arqueológicos, hieróglifos;
- e até tentativas de comunicações extraterrestres!

# Criptologia - Perigo





# Criptologia - Áreas



# Esteganografia

- A esteganografia estuda meios e métodos para se esconder a existência da mensagem.



A marca d'água (na figura, a bandeira nacional) é um recurso esteganográfico presente nas notas de dinheiro que ajuda a combater a falsificação.

# Esteganografia

- Estas cabeças formam uma série, podendo ordenar-se da primeira à sexta, segundo uma ordem lógica.



# Criptologia

- Para **codificarmos** ou **decodificarmos** uma mensagem necessitamos de informações confidenciais denominadas **CHAVE**.
- A **criptoanálise** estuda formas de decodificar uma mensagem sem se conhecer, de antemão, a chave.
- Na ciência da **criptografia** estudam-se os códigos e as cifras.

# Criptografia

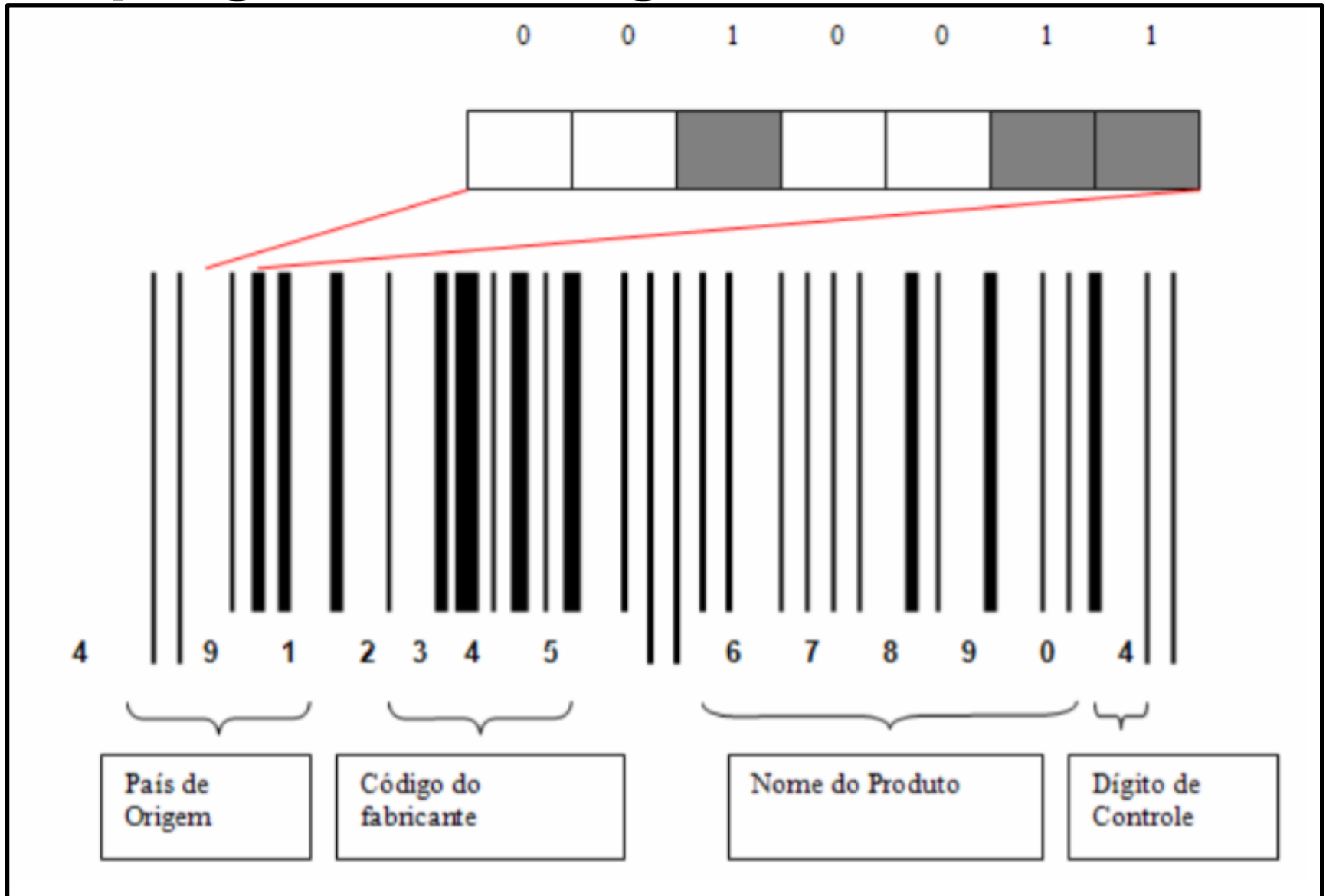
**Criptograma:** Mensagem cujo conteúdo foi obtido a partir de uma técnica de criptografia.

**Ciframento:** Técnica de criptografia para obter um criptograma a partir da mensagem.

**Deciframento:** Técnica de criptografia para obter a mensagem original a partir de um criptograma.



# Criptografia - Código de Barras



# Criptografia - Número de controle

- A Identidade de um Livro – **ISBN** (*International Standard Book Number*): é um número que consiste 10 dígitos, indicados pelo editor.



- **CPF** (Cadastro de Pessoa Física): é um número único de identificação de um cidadão brasileiro.



# Criptografia - Cifras

- Há uma unidade básica de substituição formada por letras ou símbolos, isolados ou agrupados,
- Os métodos de cifragem são divididos segundo sua natureza:
  - métodos de substituição (quando uma letra é trocada por outra, em geral diferente dela),
  - cifragem de transposição (em que as letras da mensagem são apenas permutadas, mas não substituídas)
  - cifragem mista.



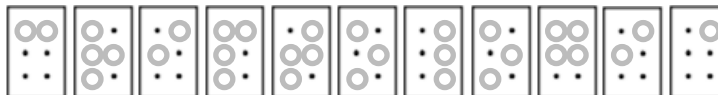
# Criptografia - Cifras (substituição)



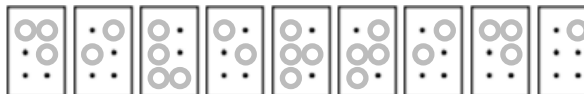
# Criptografia - Cifras (substituição)

**Considerando a cifra de Braille, decifre a mensagem à direita**

a	b	c	d	e	f	g	h	i	j
k	l	m	n	o	p	q	r	s	t
u	v	x	y	z	ç	é	á	è	ú
â	ê	ì	ô	ù	à	í	û	õ	w
í	ó	ã	señal numérico	-	,	—	...	grifo	maiúscula
,	;	:	\$	?	!	( )	"	*	"
1	2	3	4	5	6	7	8	9	0
<div> <div> <div></div><div></div><div></div> </div> <div> <div></div><div></div><div></div> </div> </div> cebra braille completa			<div> <div>1 4</div><div>2 5</div><div>3 6</div> </div> numeração convencional dos pontos						



# Criptologia pode ser divertida



# Criptografia - Cifras (substituição)

3M UM D14 D3 VER40, 3S7AVA N4 PR4I4, O853RV4NDO DU4S  
CR14NÇ4S 8B1NC4ND0 N4 4REI4. EL45 TR4B4LH4V4M MUI7O  
C0N57R1ND0 UM C4ATEL0 D3 AR3I4, C0M 70RR35, P4554R3L4S  
3 P4554G3N5 1N7ERN4S. QU4ND0 ES74V4M QU4S3  
T3RM1N4ND0, V310 UM4 0ND4 3 3S7RU1U 7UDO, R3DU21NDO 0  
C4S7EL0 4 UM MON73 D3 4REI4 3 3SPUM4. 4CH31 QU3 D3P01S  
D3 74N70 35FORÇ0 3 CU1D4D0, 45 CR1ANC4S C4IR4M N0  
CH0R0, CORR3R4M P3L4 PR41A, FUG1ND0 DA 4GU4, R1NDO D3  
M405 D4D4S 3 C0M3C4R4M 4 C0NS7RU1R 0UTR0 C4573LO.  
C0NPR33ND1 QU3 H4V14 4PR3ND1D0 UM4 GR4ND3 L1Ç40;  
G4ST4M0S MU170 7EMP0 D4 NO554 V1D4 C0NS7RU1NDO  
4LGUM4 C01S4 3 M41S 74RD3, UM4 0ND4 P0D3R4 V1R 3  
DES7RU1R 7UD0 0 QU3 L3V4M0S 7ANTO 73MP0 P4R4  
C0NS7RU1R.

# Criptografia - Cifras (substituição)

3M UM D14 D3 VER40, 3S7AVA N4 PR4I4, O853RV4NDO DU4S  
CR14NÇ4S 8B1NC4ND0 N4 4REI4. EL45 TR4B4LH4V4M MUI7O  
C0N57R1ND0 UM C4AT 70RR35, P4554R3L4S  
3 P4554G3N5 1N7ERN4 M QU4S3  
T3RM1N4ND0, V310 UM 7UDO, R3DU21NDO 0  
C4S7EL0 4 UM MON73 4CH31 QU3 D3P01S  
D3 74N70 35FORÇ0 3 C C4S C4IR4M N0  
CH0R0, CORR3R4M P3 DA 4GU4, R1NDO D3  
M405 D4D4S 3 C0M3C4 OUTR0 C4573LO.  
C0NPR33ND1 QU3 H4V GR4ND3 L1Ç40;  
G4ST4M0S MU170 7EM C0NS7RU1NDO  
4LGUM4 C01S4 3 M41S P0D3R4 V1R 3  
DES7RU1R 7UD0 0 QU3 L3V4M0S 7ANTO 73MP0 P4R4  
C0NS7RU1R.

0 = O

1 = I

2 = Z

3 = E

4 = A

5 = S

7 = T

8 = B

# Criptografia - Cifras (substituição)

Considerando o código Morse, passe a mensagem: “SOS”

A	.-	M	--	Y	-.--	6	-....
B	-...	N	-.	Z	--..	7	--...
C	-.-.	O	---	Ä	.-.-	8	---..
D	-..	P	.--.	Ö	---.	9	----.
E	.	Q	--.-	Ü	..--	.	.-.-.-
F	...-	R	.-.	Ch	----	,	--..--
G	--.	S	...	0	-----	?	..--..
H	....	T	-	1	.-----	!	.._..
I	..	U	..-	2	..----	:	---...
J	.----	V	...-	3	...--	“	.-...-
K	-. -	W	.--	4	....-	’	.----.
L	.-..	X	-.-	5	.....	=	-...-

CARACTER	TEMPO
ponto	UT
traço	3 UT
intervalo entre letras	3 UT
intervalo entre palavras	7 UT

# Criptografia - Cifras (substituição)



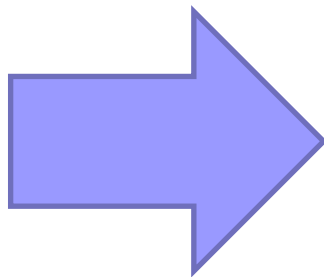
... ..  
S O S



# Criptografia - Cifras (substituição)

- Neste método os conteúdos das mensagens original e criptografada são os mesmos, porém com as letras trocadas

**CARRO**

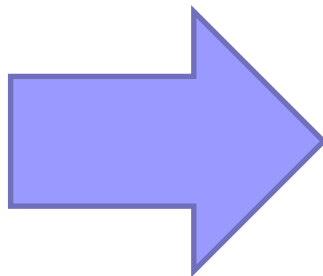


**ORARC**

# Criptografia - Cifras (substituição)

- Cifra linear, ou de troca, neste método cada letra do texto é trocada por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes.

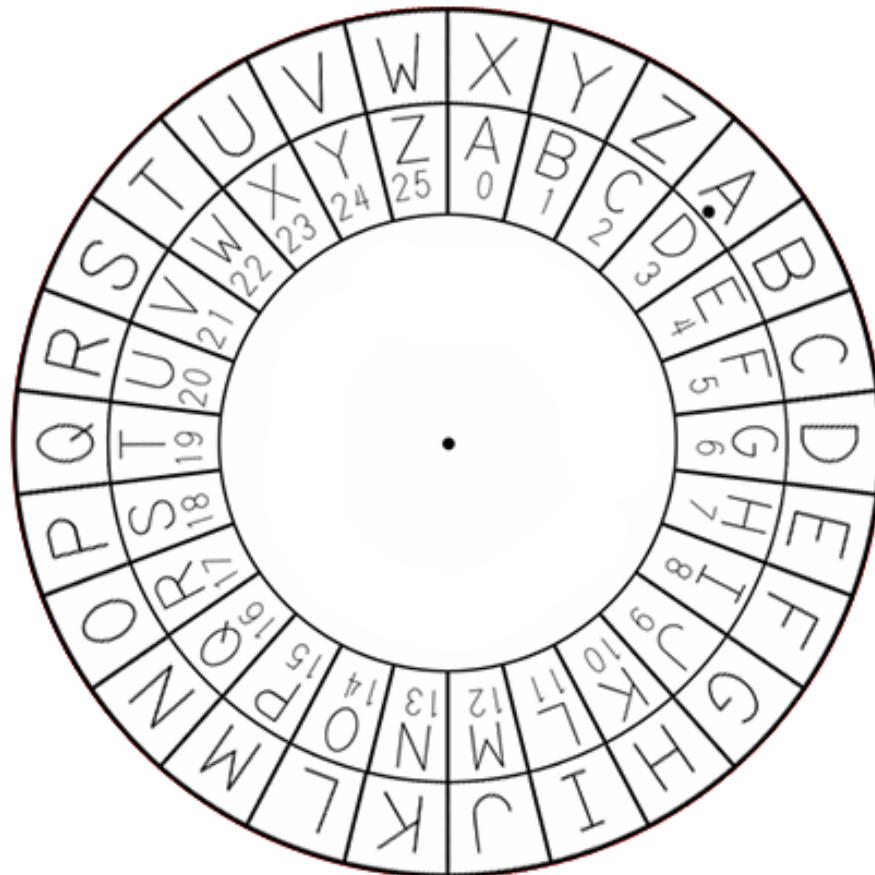
**CASA**



**FDVD**



# Criptografia - Cifras (troca)



Click wheel to rotate.

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
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

# Criptografia - Cifras (transposição)

- Uma cifra é classificada de transposição quando o criptograma possui as mesmas letras, que são trocadas entre si.

# Criptografia - Cifras (transposição)

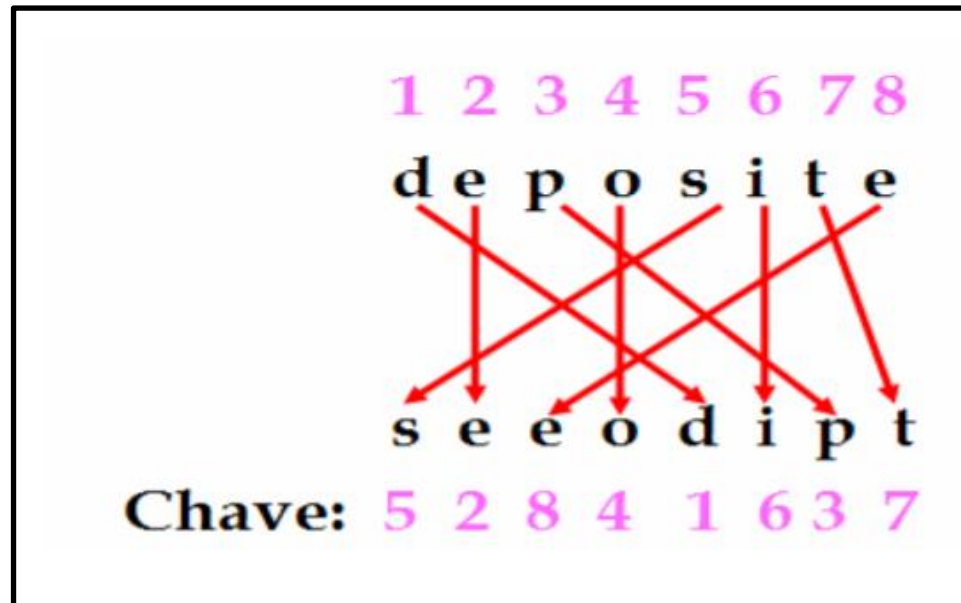
- Cifra reflexa, é o método mais simples de transposição e foi usada por Leonardo da Vinci.
- Método de cifra e decifra: escrever linhas do fim para o início!
- Exemplo:
  - Texto plano: ATACAR AMANHA
  - Criptograma: AHNAMA

# Criptografia - Cifras (transposição)

- Método da permutação de colunas(coluna singular): Dada a mensagem original,  
deposite\_um\_milhão\_de\_dólares\_em\_minha  
\_conta\_na\_suiça.\_número\_dois\_um\_sete\_seis.
- Codifique a mensagem, utilizando o ciframento por transposição e a chave: **5 2 8 4 1 6 3 7**.
- Nota histórica: Substituição de palavras, seguida por transposição de coluna usada pelo exército da união na guerra civil norte-americana.

# Criptografia - Cifras (transposição)

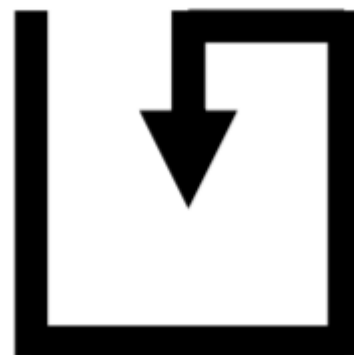
d	e	p	o	s	i	t	e
_	u	m	_	m	i	l	h
ã	o	_	d	e	_	d	ó
l	a	r	e	s	_	e	m
_	m	i	n	h	a	_	c
o	n	t	a	_	n	a	_
s	u	i	ç	a	.	_	n
ú	m	e	r	o	_	d	o
i	s	_	u	m	_	s	e
t	e	_	s	e	i	s	.



# Criptografia - Cifras (transposição)

- Qual é o conteúdo da mensagem AASBMEROSATE?

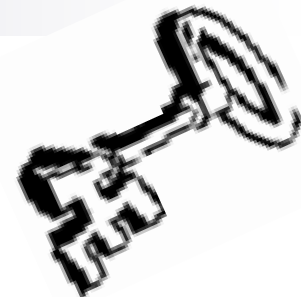
A	A	S
B	M	E
R	O	S
A	T	E



# Criptografia - Cifras (transposição)

DE AORCDO COM UMA PQSIEUSA DE UMA  
UINRVESRIDDAE IGNLSEA, NÃO IPOMTRA EM  
QAUŁ ODREM AS LRTEAS DE UMA PLRAVAA  
ETÃSO, A ÚNCIA CSIOA IPROTMATNE É QUE A  
PIREMRIA E ÚTMLIA LRTEAS ETEJASM NO  
LGAUR CRTEO. O RSETO PDOE SER UMA TTAOL  
BÇGUANA QUE VCOÊ PDOE ANIDA LER SEM  
POBRLMEA. ITSO É POQRUE NÓS NÃO LMEOS  
CDAA LRTEA ISLADOA, MAS A PLRAVAA CMOO  
UM TDOO.

# Criptografia - Chave



- Uma chave é um valor que trabalha com um algoritmo de criptografia para produzir dados encriptados específicos. Chaves são basicamente números realmente grandes.
- O tamanho da chave é medido em bits; Em criptografia com chave pública, quanto maior a chave, mais seguro ficam os dados encriptados.
- Quanto maior a chave, mais seguro é, mas os algoritmos usados para cada tipo de criptografia são muito diferentes e assim comparação entre as duas é igual a se comparar maçãs com laranjas.



# Criptografia - Chave/Funcionamento

- Um algoritmo de **criptografia** é uma função matemática usada no processo de **encriptação** e de **desencriptação**.

```
textoCifrado = funcaoCripto("Mensagem secreta")
```

- Um algoritmo de criptografia trabalha em conjunto com uma chave—uma palavra, numero, ou frase—para encriptar os dados.

# Criptografia - Chave/Funcionamento

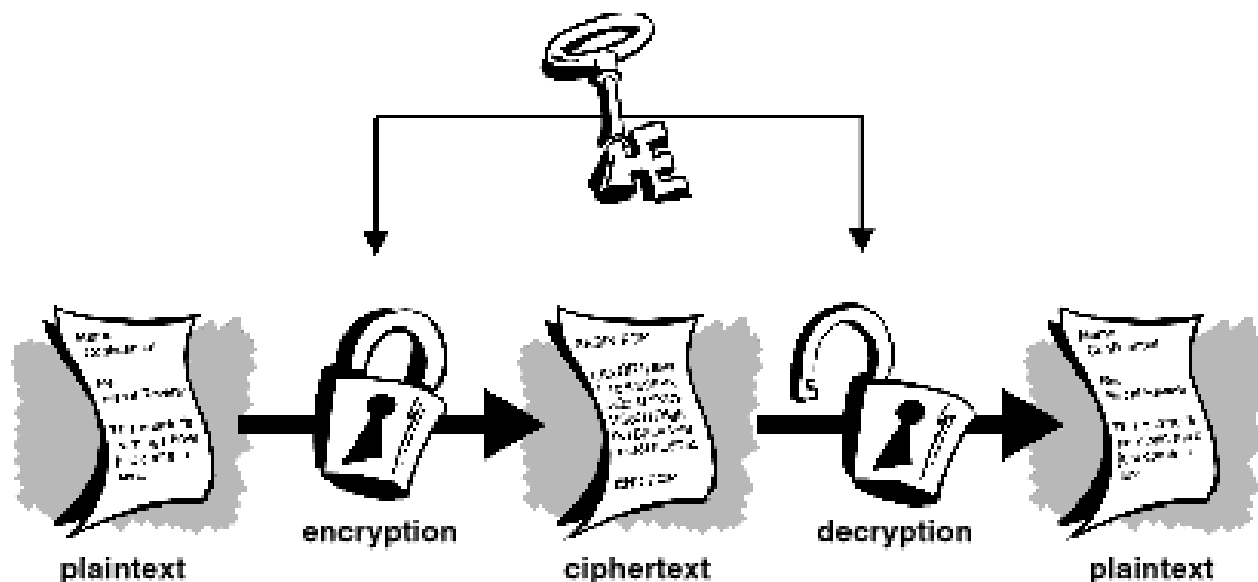
- Um algoritmo de criptografia trabalha em conjunto com uma chave—uma palavra, numero, ou frase—para encriptar os dados.
- Os mesmos dados podem gerar diferentes dados encriptados usando chaves diferentes, ou seja, se mudarmos a chave, para um mesmo conjunto de dados geramos dados encriptados **diferentes**.

```
textoCifrado = funcaoCripto("Mensagem secreta", "Chave")
```

- A segurança de dados encriptados é completamente dependente em duas coisas: a **força do algoritmo** de criptografia e o **segredo da chave**

# Criptografia – Chave Privada

- Na criptografia com **chave privada** ou **simétrica**, também chamado de *secret-key* ou *symmetric-key encryption*, uma chave é usada tanto para **criptação** quanto para **descriptação**.
  - Ex.: O *Data Encryption Standard* (DES) é um exemplo de um sistema de criptografia com chave privada.

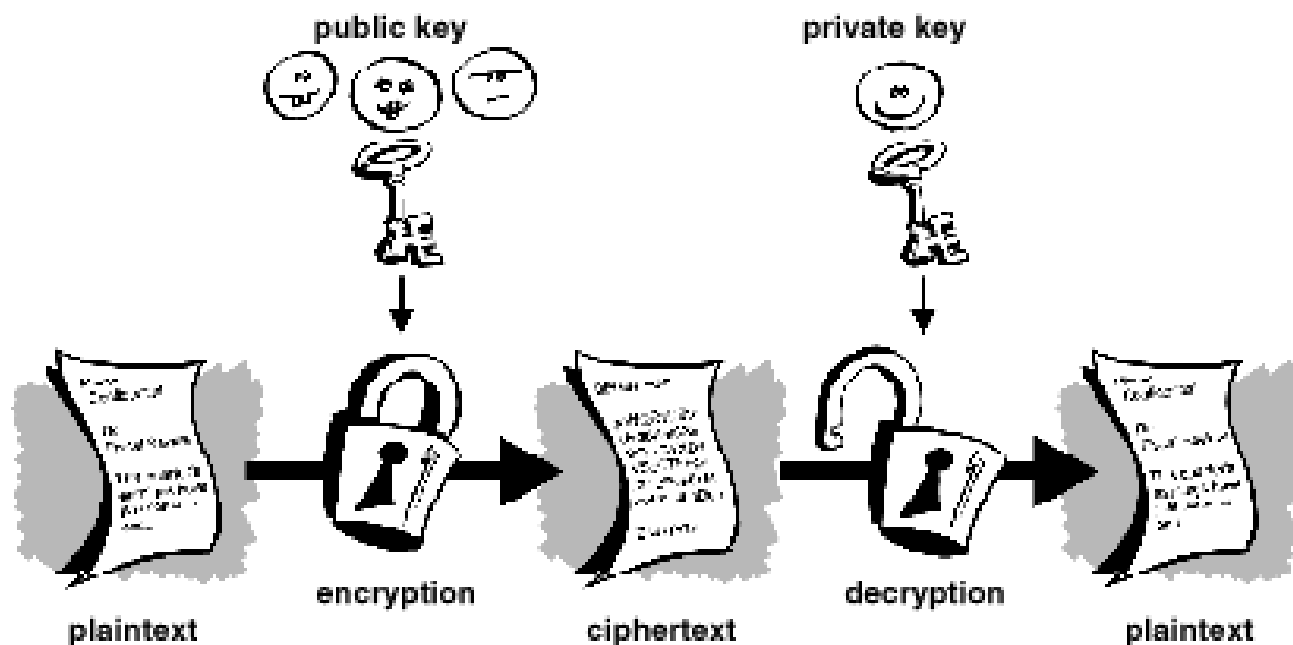


# Criptografia – Chave Pública

- Os problemas da **distribuição** chave são resolvidos através da criptografia com **chave pública**, conceito este que foi introduzido por Whitfield Diffie e Martin Hellman em 1975.
- Há evidência agora que o **Serviço Secreto britânico** inventou isto alguns anos antes de Diffie e Hellman, mas manteve isto em segredo—e não fez nada com isto.

# Criptografia – Chave Pública

- Criptografia com **chave pública** é um **esquema assimétrico** que usa um **par de chaves** para encriptação: uma **chave pública**, que encripta dados, e uma **chave privada** correspondente (as duas chaves são relacionadas entre si), secreta para desencriptação.

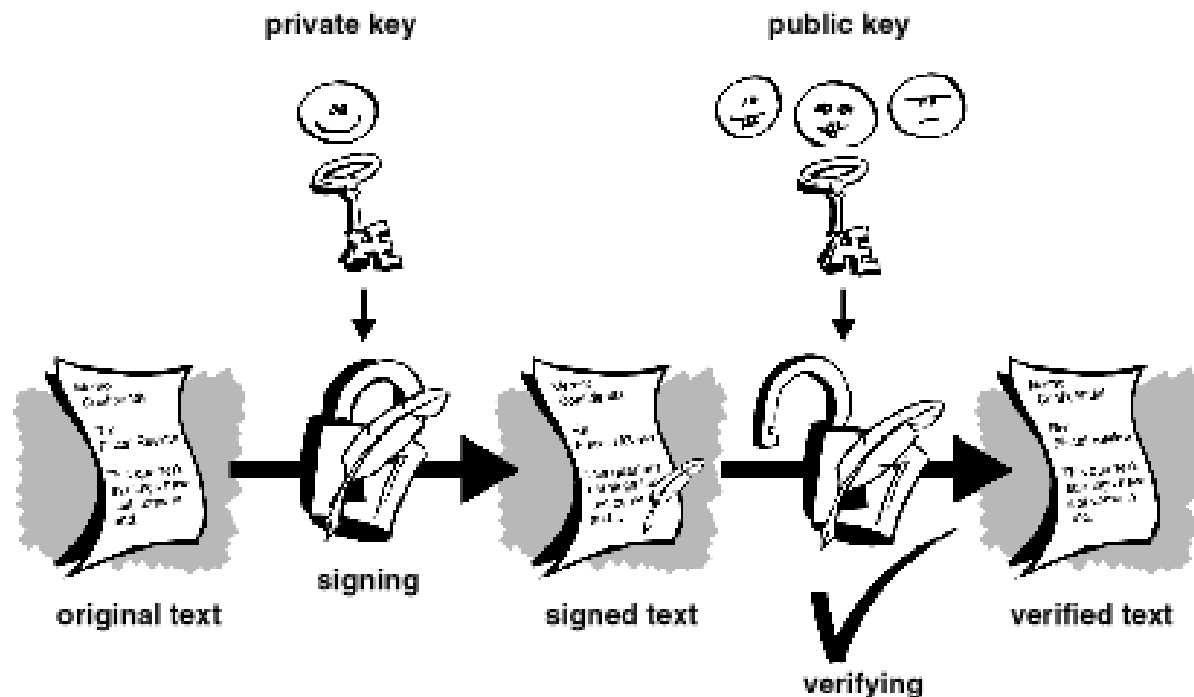


# Criptografia – Assinatura Digital

- Um outro benefício de criptografia **com chave pública** é que provê um método para empregar **assinaturas digitais**.
- **Assinaturas digitais** habilitam o receptor da informação verificar a autenticidade da origem da informação, e também verifica se a informação está intacta.
- Assim, **assinaturas digitais** com **chave pública** provêm autenticação e integridade de dados.
- Uma assinatura digital também provê não repúdio, o que significa que previne o emissor de reivindicar que ele ou ela não enviaram de fato a informação.
- Estas características são tão fundamentais para criptografia como privacidade.

# Criptografia – Assinatura Digital

- Em vez de encriptar informação usando a chave pública de outra pessoa, você encripta ela com sua **chave privada**. Se a informação pode ser descriptada com sua **chave pública**, então ela pode ser verificada se foi originado de você.



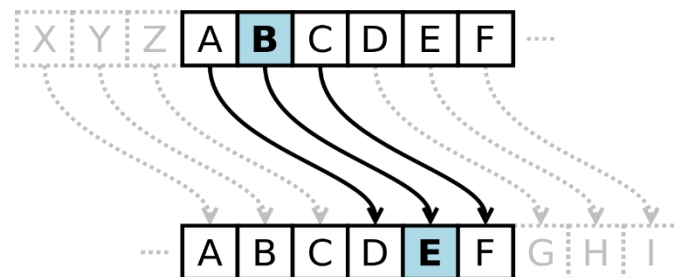
# Criptografia – passphrase

- A maioria das pessoas está familiarizado com a restrição de acesso para sistemas de computador por uma conta-senha que é uma única string de carácter que um usuário digita como um código de identificação.
- Um **passphrase** é uma versão mais longa de uma **contra-senha**, e teoricamente, mais seguro.
- Tipicamente composto de palavras múltiplas, um **passphrase** é mais protegido contra ataques de dicionário, em que o atacante tenta todas as palavras no dicionário em uma tentativa para determinar sua contra-senha.
- Os melhores **passphrases** são relativamente longos e complexos e contém uma combinação de letras superiores, carácter de pontuação e numéricos



# Exercício 1

- A cifra de César consiste no deslocamento do alfabeto em  $n$ . Veja o exemplo a seguir, sendo que o deslocamento é 4



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						

*Tendo esse conceito em mente, transcreva a mensagem “Criptologia pode ser divertida!”, sendo que o deslocamento é de 23.*

# Exercício 2

- No próximo slide apresenta-se o quadrado de Vigenère.
- A cifra de Vigenère é um método de criptografia que utiliza uma série de diferentes "cifras de César" com base nas letras de uma palavra-chave.
- Em uma cifra de César, cada letra da passagem é movida de posição um certo número de letras, para ser substituída pela letra correspondente.
- A cifra de Vigenère baseia-se neste método, utilizando várias cifras de César em diferentes pontos da mensagem.
- Se for escrever a mensagem "THIAGO", utilizando a palavra-chave FOGO; para poder codificar a mensagem é necessário repetir a palavra-chave, conforme a quantidade de letras que serão utilizadas na mensagem: FOGOFO. Agora, para codificar é necessário procurar a LINHA conforme a palavra-chave, e procurar a coluna referente a letra da mensagem. A primeira letra da mensagem é T e a primeira letra da palavra-chave é F, então a codificação ficaria Y. A mensagem final ficaria YVOOLC. Agora codifique a mensagem "Criptologia pode ser divertida!"

- Se for escrever a mensagem “THIAGO”, utilizando a palavra-chave FOGO; para poder codificar a mensagem é necessário repetir a palavra-chave, conforme a quantidade de letras que serão utilizadas na mensagem: FOGOFO. Agora, para codificar é necessário procurar a LINHA conforme a palavra-chave, e procurar a coluna referente a letra da mensagem. A primeira letra da mensagem é T e a primeira letra da palavra-chave é F, então a codificação ficaria Y. A mensagem final ficaria YVOOLC.
- Agora codifique a mensagem “Criptologia pode ser divertida!”

	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

# Exercício 3

- Pesquise algoritmos de criptografia e responda:
- Qual o tipo de criptografia(S/A)?
- Quem é o autor?
- Quando foi criado?
- Como funciona?
- Onde é utilizado?
- Ex.:
  - Algoritmo RSA (Rivest, Shamir, Adleman)
  - Algoritmo ATBASH
  - Algoritmo Diffie-Hellman
  - Algoritmo de Elgamal
  - Algoritmo de Assinatura Digital (inventada por David Kravitz).

# Conclusão

- Conhecemos um pouco sobre criptografia.
- Existem outros métodos de criptografia, portanto o estudo não termina aqui.

# Referências

- WEBER, Raul Fernando. Fundamentos de arquitetura de computadores. 4. ed. Porto Alegre: Bookman, 2012. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788540701434>
- STALLINGS, William. Arquitetura e organização de computadores. 8.ed. São Paulo: Pearson, 2010. E-book. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/459/epub/0>
- HOGLUND, Greg. Como quebrar códigos: a arte de explorar (e proteger) software. São Paulo: Pearson, 2006. E-book. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/179934/epub/0>

# Vídeos

- Criptografia | Nerdologia Tech
  - [https://www.youtube.com/watch?v=\\_Eeg1LxVWa8](https://www.youtube.com/watch?v=_Eeg1LxVWa8)
- Criptografia (Guia Básico para Entender Como Funciona) // Dicionário do Programador
  - <https://www.youtube.com/watch?v=qHFbuXpz7e4>
- Como funciona a criptografia?
  - <https://www.youtube.com/watch?v=glGrlf5mWcY>
- Entendendo Conceitos Básicos de CRIPTOGRAFIA | Parte 1 e 2 (Fábio Akita)
  - [https://www.youtube.com/watch?v=CcU5Kc\\_FN\\_4](https://www.youtube.com/watch?v=CcU5Kc_FN_4)
  - <https://www.youtube.com/watch?v=HCHqtpipwu4>



# Fim