

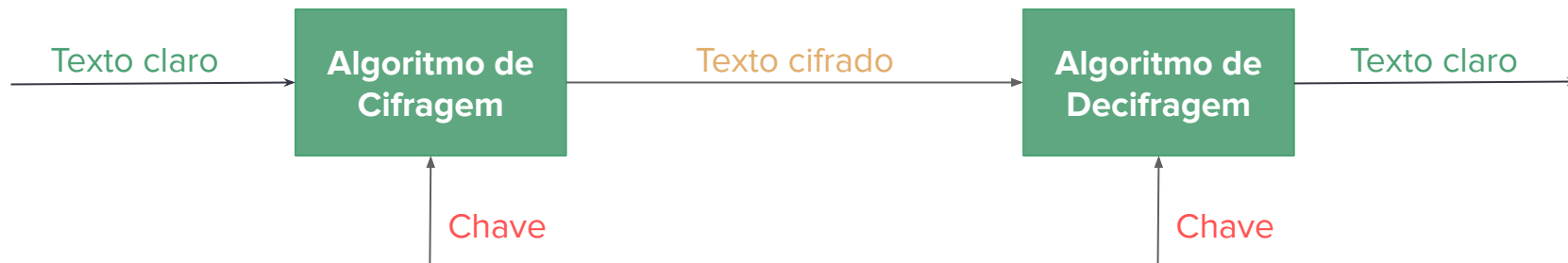
Criptografia Aplicada

Introdução à criptografia

Introdução à criptografia

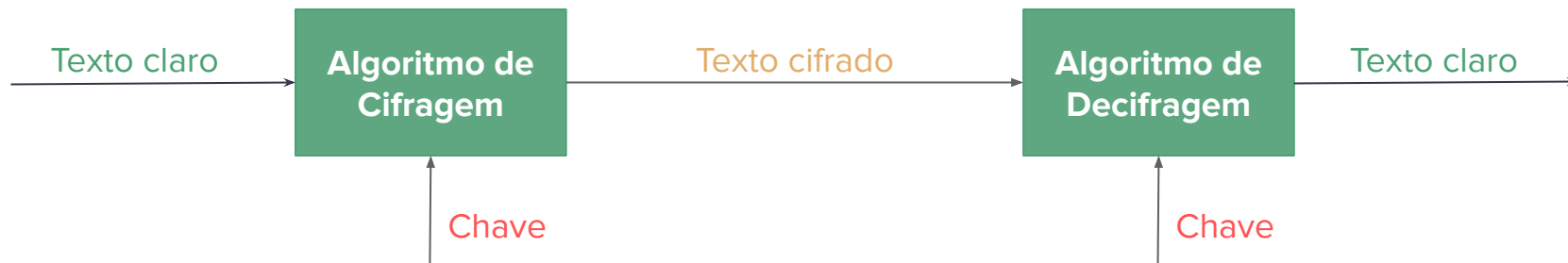
- Definições básicas
 - Cifragem x decifragem
 - Criptoanálise
 - Criptografia Simétrica
 - Criptografia Assimétrica
 - Requisitos de segurança
- Criptografia Clássica

Definições básicas



Criptossistema: especificação completa de chaves e como elas são usadas para cifragem e decifragem

Definições básicas



O princípio de Kerckhoffs: um sistema de criptografia deve ser seguro ainda que o adversário conheça todos os detalhes do sistema, com exceção da chave secreta

Criptanálise

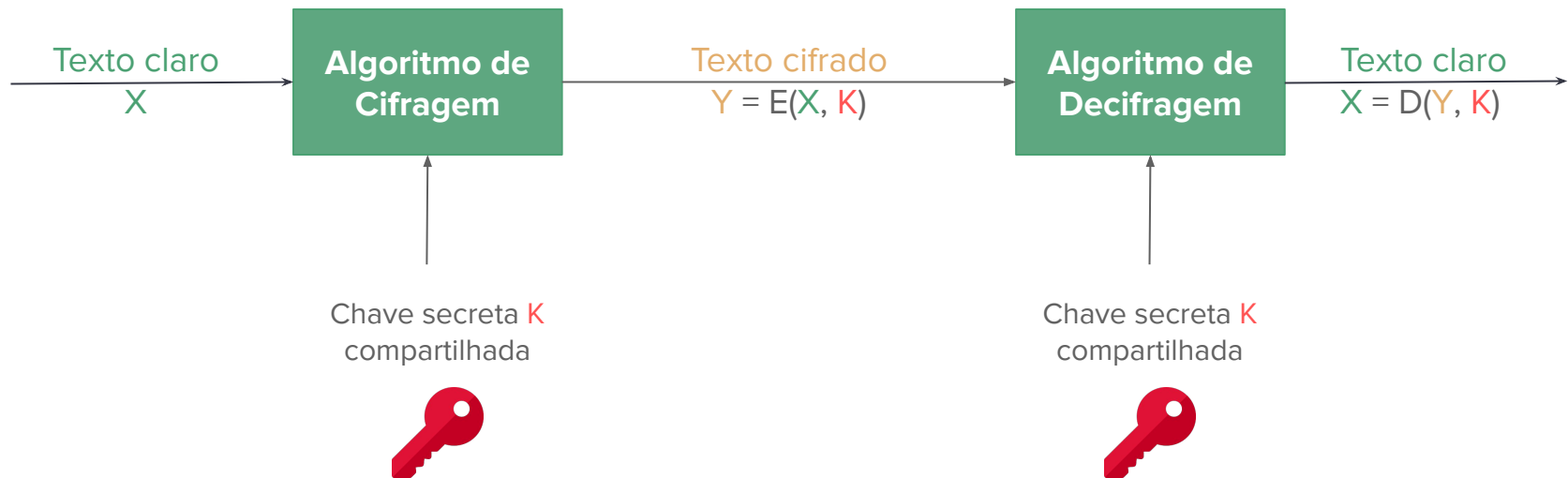
Criptografia: área que estuda os esquemas utilizados para cifragem e decifragem.

- Tipos de operações utilizadas para transformar texto claro em texto cifrado
- Número de chaves utilizado
- A forma como o texto claro é processado

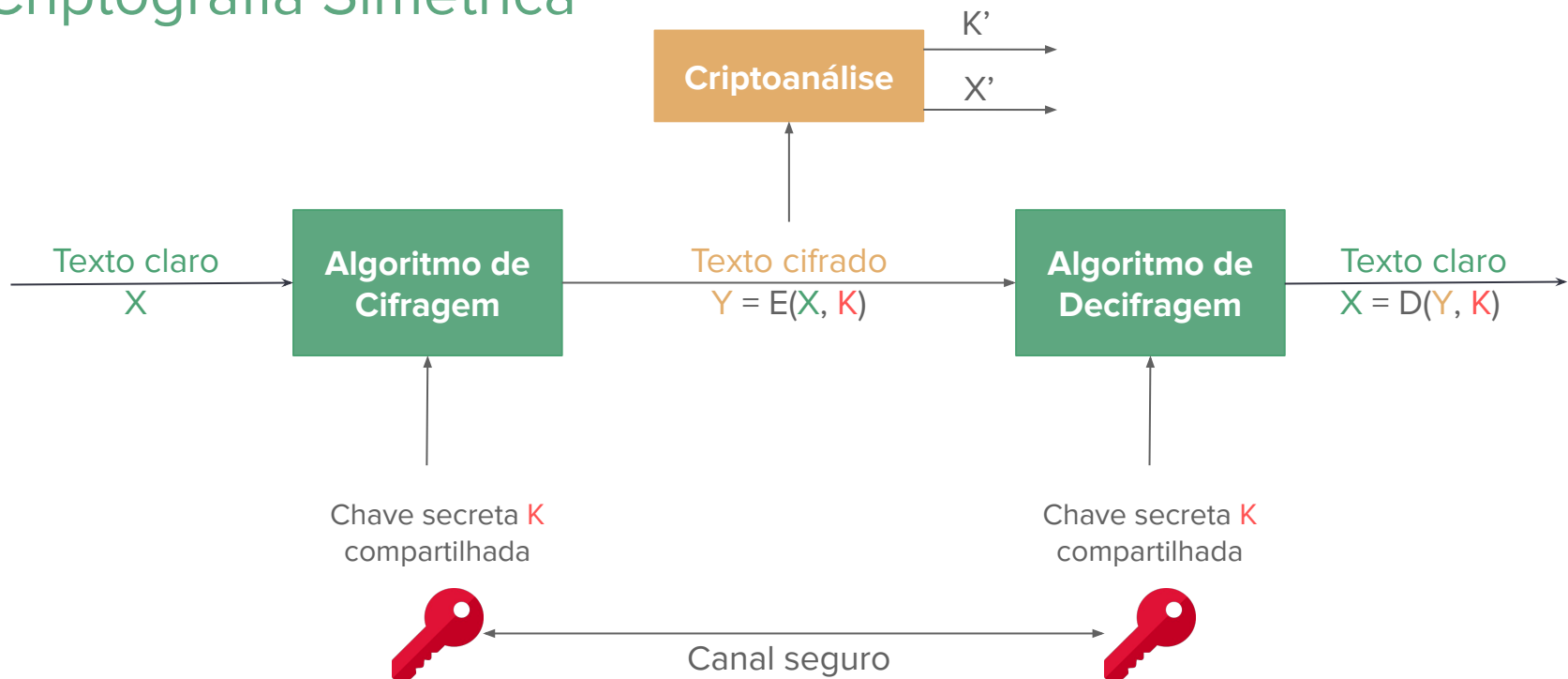
Criptanálise: área que estuda técnicas de decifragem sem conhecimento da chave.

- Força bruta
- Ataque na natureza do algoritmo (falhas ou vazamento de informação)
- Características do texto (claro e cifrado)

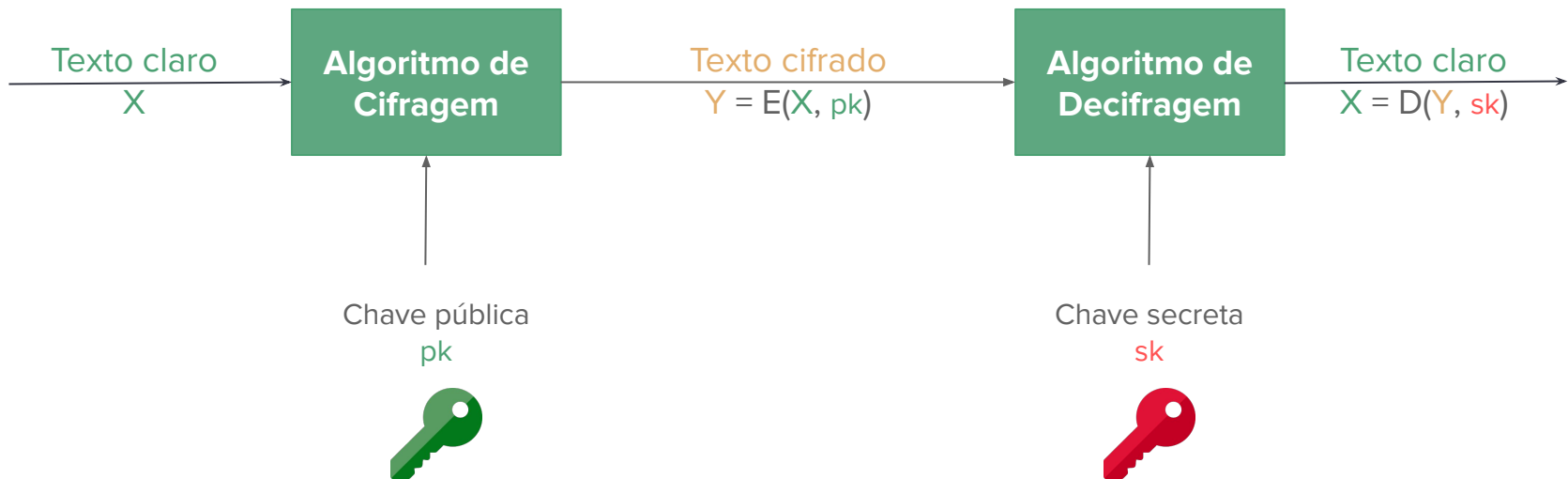
Criptografia Simétrica



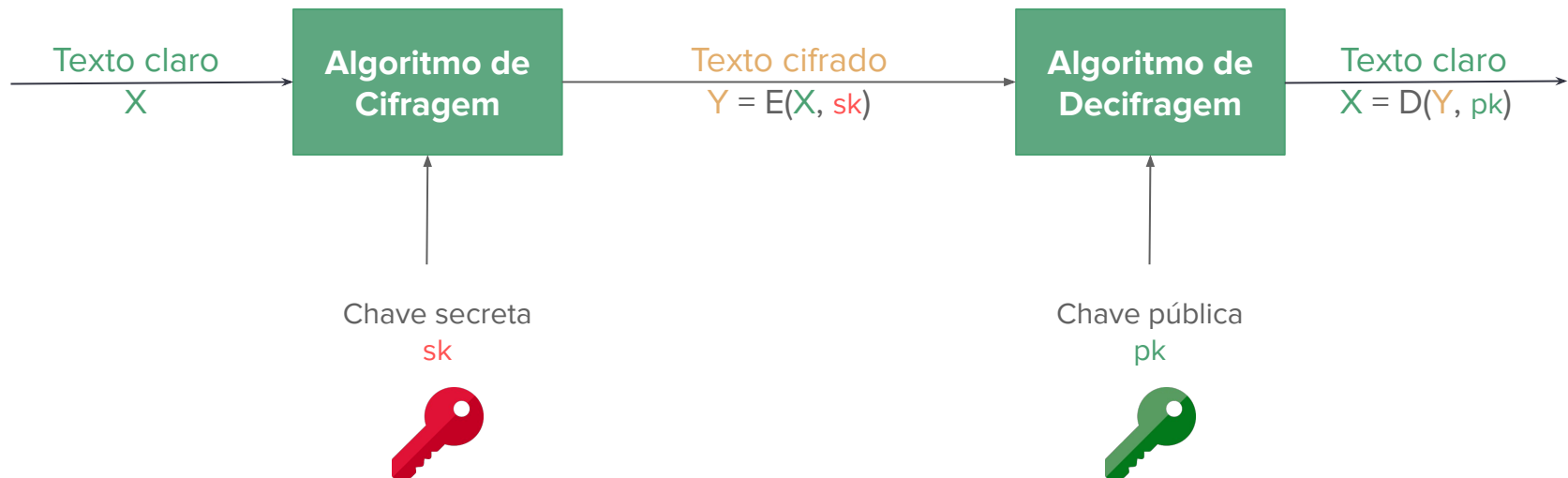
Criptografia Simétrica



Criptografia Assimétrica

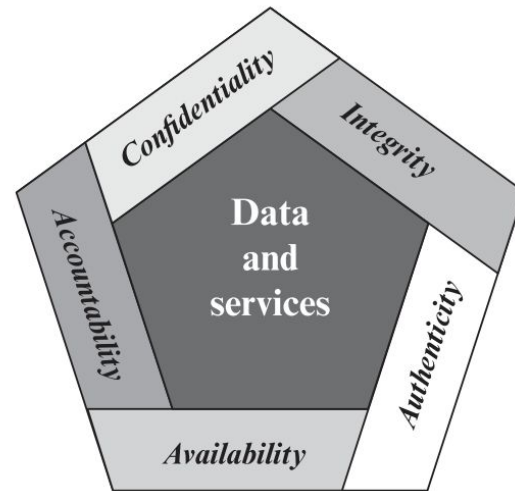


Criptografia Assimétrica



Requisitos de segurança

- Confidencialidade
- Integridade
- Disponibilidade (availability)
- Autenticidade
- Responsabilização (accountability)



Fonte: W. Stallings. Cryptography and network security. Cap 1.1

Conceitos básicos de criptografia

- Definições básicas
 - Cifragem x decifragem
 - Criptoanálise
 - Criptografia Simétrica
 - Criptografia Assimétrica
 - Requisitos de segurança
- **Criptografia Clássica**
 - História da criptografia
 - Cifradores mono-alfabéticos
 - Cifradores poli-alfabéticos
 - Máquinas de rotores

História da Criptografia

- A história da criptografia é marcada por diversos períodos.
- Com o passar do tempo, a criptografia evoluiu junto com a civilização

antiquity	1500 BC – 100 AD
Arab civilization	800 – 1400
European Middle Ages	1000 – 1500
Renaissance	1450 – 1600
Baroque, salon cryptography	1600 – 1850
mechanical devices	1580 – 1950
electromechanical devices	1920 – 1950
computers	1943 – present
public key systems	1976 – present

Table A.4: Cryptographic time periods.

Fonte: Joachim von zur Gathen, *CryptoSchool*, Capítulo A.

História da Criptografia

- Antigamente, o conhecimento da escrita era tão exclusivo que, de maneira geral, não havia necessidade de proteger textos escritos;
- entretanto, alguns textos eram considerados extremamente secretos, e portanto apenas o mais alto nível de realeza poderia acessar;
- foi então que surgiu a necessidade de garantir confidencialidade.

História da Criptografia

- Egito (1332 - 1322 AC):
 - Hieróglifos modificados da tumba do faraó Tutankhamon;
 - comunicação de informações religiosas secretas ao faraó;
 - indecifrável por qualquer pessoa fora do círculo real.



Figure A.6: Two goddesses around a pole representing Re.

Fonte: Joachim von zur Gathen,
CryptoSchool, Capítulo A.

História da Criptografia

- Roma (464 - 167 AC):
 - Utilizada na primeira guerra da Macedônia;
 - cinco tochas de cada lado, as da direita indicam a linha e as da esquerda a coluna;
 - sistema parecido foi usado pelos EUA durante a guerra civil, com bandeiras no lugar de tochas.

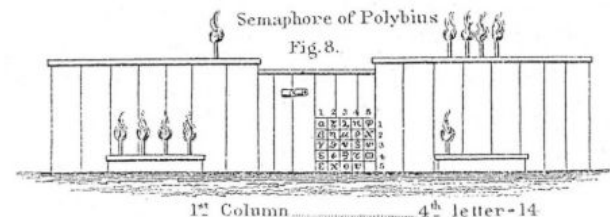



Figure A.9: Polybius' signalling system as interpreted by Myer (1879).

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

Figure A.10: The Polybius Square.

Fonte: Joachim von zur Gathen
CryptoSchool, Capítulo A. 

Cifras de substituição

- Consistem na substituição de letras do texto claro por outras letras ou símbolos.
- Exemplos de cifras de substituição:
 - Cifra de César
 - Cifradores mono-alfabéticos
 - Playfair
 - Cifradores poli-alfabéticos
 - Vigenère
 - Vernam
 - One-time pad

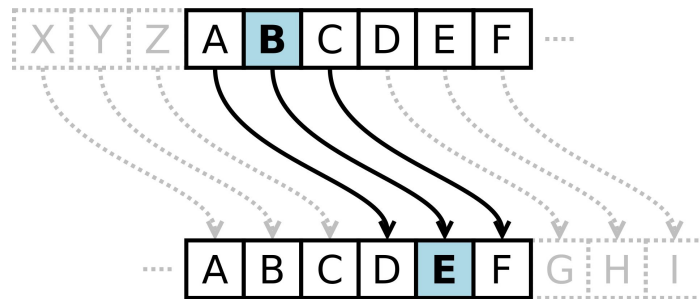
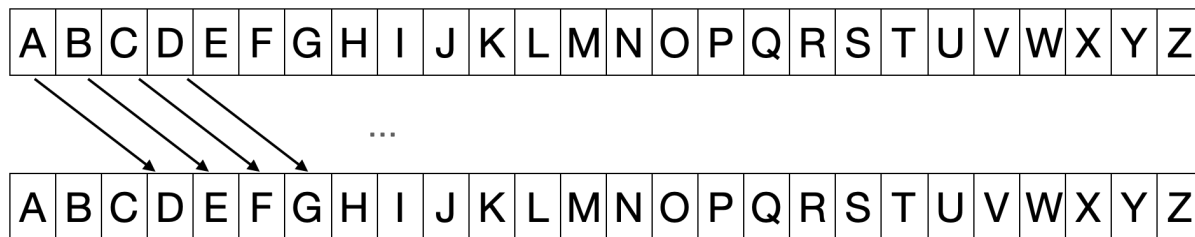


Imagem: <https://tinyurl.com/cifra-cesar>

Cifra de César (100 - 44 AC)

- Substituímos cada letra da mensagem pela letra 3 casas a frente
 - Texto Claro: me encontre depois da aula
 - Texto Cifrado: PH HQFRQWUH GHSRLV GD DXOD
- Matematicamente:
 - $c = E(m, 3) = (m + 3) \bmod 26$
 - Ou mais genérico: $c = E(m, i) = (m + i) \bmod 26$



Cifra de César (100 - 44 AC)

- Decifragem:
 - $m = D(c, i) = (c - i) \bmod 26$
- Criptoanálise:
 - **Chave**: valor de i
 - Força Bruta: tentar todas as 25 possibilidades de chaves

	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
KEY						
1	oggv	og	chvgt	vjg	vqic	rtva
2	nfpu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrp	rfe	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	moxqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	objv	kvmot
9	gyyn	gy	uznvl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlg
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puigt	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkk	znk	zumg	vgxze
24	rjyy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

Fonte: W. Stallings. *Cryptography and network security*. Cap 3.2

Cifradores mono-alfabéticos

- Mapeia de um alfabeto para outro alfabeto
- Troca de uma letra por outra letra qualquer
 - Variação da cifra de César.
 - **Chave**: 26 letras que representam o mapeamento do alfabeto original para o de cifragem
- Espaço de Chaves:
 - $26! = 4 \times 10^{26}$
 - Maior que DES
- Criptoanálise:
 - Análise de frequência
 - Análise de duplas, triplas

Frequência Relativa das Letras

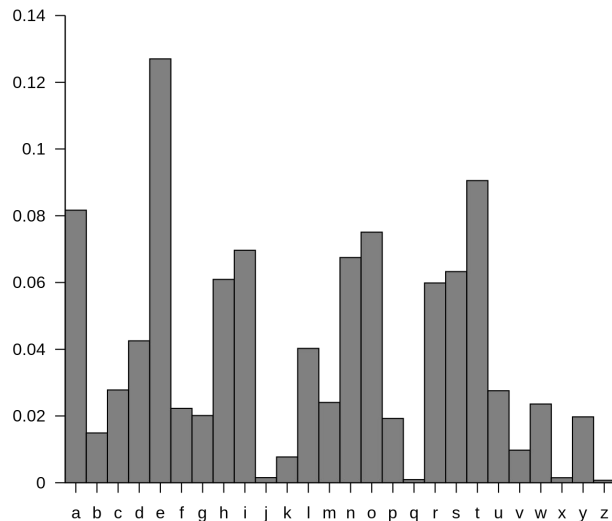


Imagem: <https://tinyurl.com/frequencia-en>

Frequência (inglês)

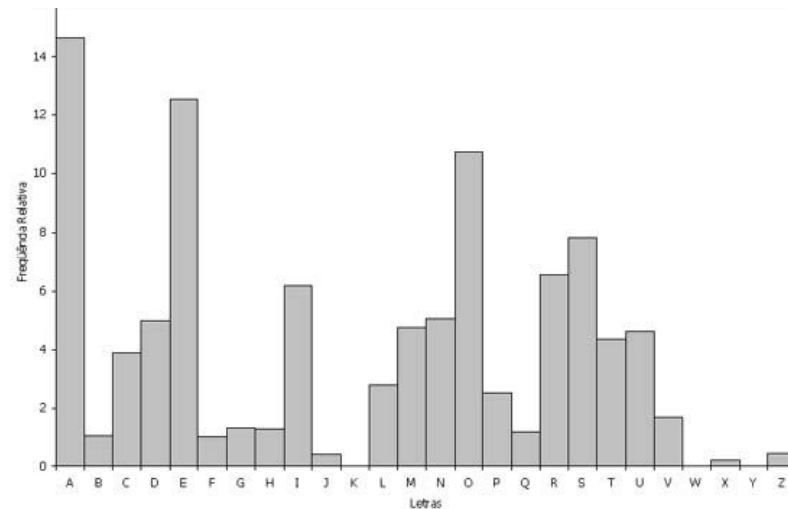


Imagem: <https://tinyurl.com/frequencia-pt>

Frequência (português)

Cifradores poli-alfabéticos

- Usam um conjunto de substituições mono-alfabéticas
- Uma chave determina qual substituição será utilizada em cada letra
- Objetivo: tornar a criptoanálise mais difícil
- Cifras poli-alfabéticas:
 - Vigenère
 - Vernam
 - One-time pad

One-Time Pad (1917)

- Transformação do texto em bits
- Transformação da chave em bits
- Ou-Exclusivo bit a bit
- **Cifragem:** $c_i = m_i \oplus k_i$
- **Decifragem:** $m_i = c_i \oplus k_i$

Mensagem	H 01001000	E 01000101	L 01001100	L 01001100	O 01001111
Chave	P 01010000	L 01001100	U 01010101	T 01010100	O 01001111
Texto cifrado	00011000	00001001	00011001	00011000	00000000

One-Time Pad (1917)

- Chave aleatória tão grande quanto a mensagem e de uso único.
- Essa modificação torna o sistema **inquebrável** (*perfect secrecy*)
 - segurança baseada na aleatoriedade da chave
 - texto cifrado não tem nenhuma relação estatística com o texto claro
 - força bruta geraria diversos textos claros plausíveis

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: pxlmvmsydofoyrvzwc tnlebnecvgdupahfzzlmnyih

plaintext: mr mustard with the candlestick in the hall

key: pftgpmiydgaxgoufhklllmhsqdgogtewbqfgyovuhwt

plaintext: miss scarlet with the knife in the library

One-Time Pad (1917)

Limitações:

- Para que seja inquebrável, a chave precisa ser aleatória e nunca reutilizada
- Geração de grandes quantidades de chaves aleatórias é muito difícil
- Distribuição dessas chaves entre emissor e receptor é muito difícil
- Uso do one-time pad é limitado a aplicações que requerem um nível de segurança muito grande

Máquinas de rotores

- Usar múltiplas etapas de cifragem faz com que o algoritmo fique mais resistente à criptoanálise
 - Tanto em cifras de substituição quanto nas de transposição.
 - A aplicação mais importante desse princípio (antes do DES/AES) foi nas máquinas de rotores.
- Usada nas comunicações da segunda guerra mundial
 - Pela Alemanha com a máquina Enigma
 - Pelo Japão com a máquina Purple
- Sistema eletro-mecânico complexo.

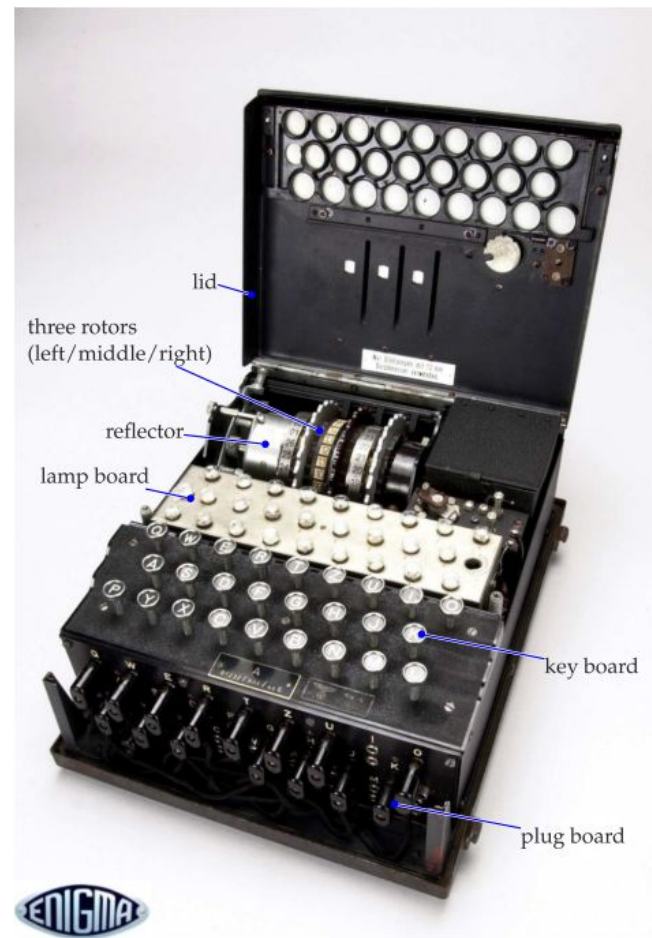
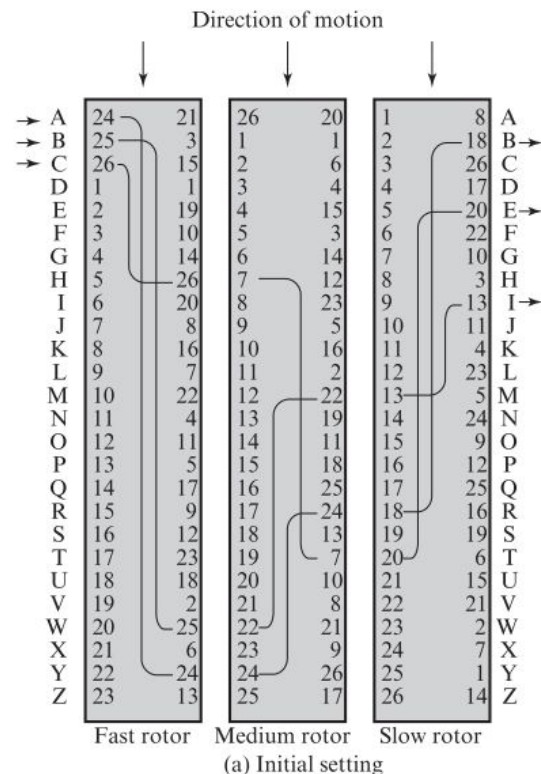


Figure J.1: An ENIGMA machine with open lid.

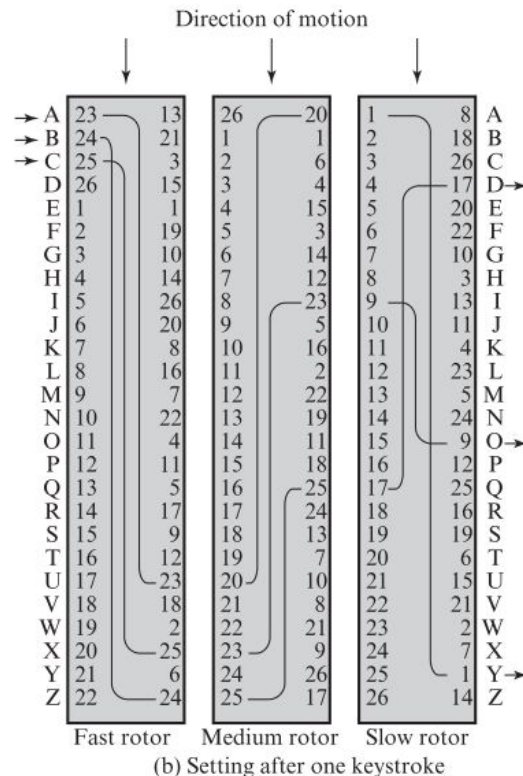
Máquinas de rotores

- Conjunto de cilindros (rotores) independentes.
- Cada cilindro é um cifrador mono-alfabético com 26 entradas e 26 saídas.
- Conexões internas ligam cada entrada à uma única saída.
- Cada saída de um cilindro é ligada à entrada de outro
 - Na figura, a letra A é substituída pela letra B.
- Depois de cifrar uma letra, há um shift nos cilindros e uma nova substituição mono-alfabética é definida.



Máquinas de rotores

- Depois de cifrar uma letra, há um shift nos cilindros e uma nova substituição mono-alfabética é definida.
 - Houve um shift no primeiro rotor, então a letra A é substituída pela letra Y.
 - Com 3 rotores, existem $26 \times 26 \times 26 = 17576$ alfabetos de substituição diferentes antes que o sistema repita o mapeamento
- **Chave:**
 - Segurança baseada apenas no segredo da chave
 - Escolha e sequência dos rotores, configuração dos rotores, conexões do plugboard.
 - Combinação de 2^{67} possíveis chaves
- **Criptanálise:**
 - Extremamente complexa, contou com o auxílio de espiões e de modos de operação inseguros
 - Trabalho de Turing



E hoje?

- Com o surgimento dos computadores, a criptografia precisou evoluir
- Criptografia clássica tinha por objetivo apenas a confidencialidade
- *A criptografia moderna* busca também outras garantias de segurança

Para a próxima aula

Instalar e testar o *openssl*

Referências

- W. Stallings. *Cryptography and network security*. 7a edição.
 - Capítulos 1.1, 3.2, 3.3, 3.4, 9.1
- D. Stinson e M. Paterson. *Cryptography: Theory and Practice*. 4a edição.
 - Capítulos 1.1, 2.1, 2.2, 3.3
- Joachim von zur Gathen. *CryptoSchool*. 1a edição.
 - Capítulo A.1, A.2, F.2, J.1, 9.4
- Imagens: Flaticon.com