CIFRAS SIMÉTRICAS

Gerência e Segurança de Redes

Objetivos de Aprendizagem

Introduzir o conceito de cifra simétrica

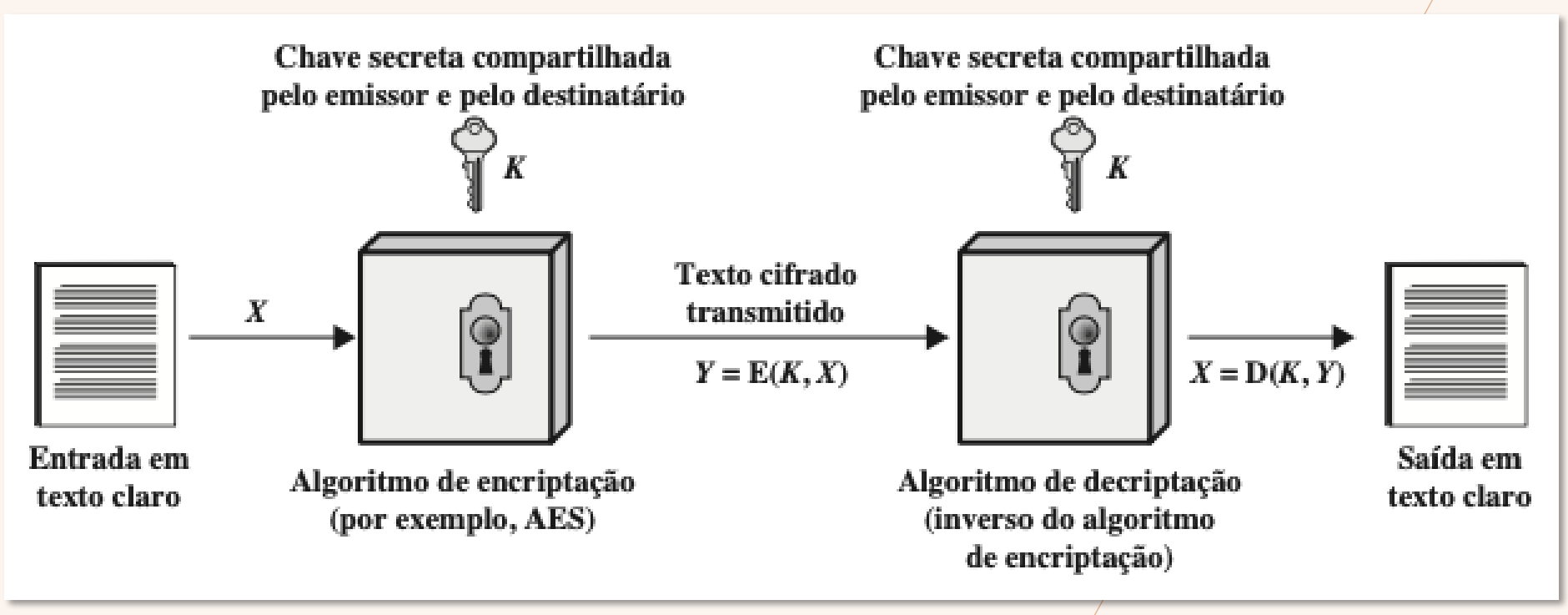
Apresentar as técnicas clássicas

Agenda

1. Modelo
2. Técnicas de substituição
3. Técnicas de transposição
4. Máquinas de rotor

Modelo de Cifra Simétrica

Modelo de Cifra Simétrica



Elementos

- Texto claro

  Mensagem ou dados originais

- Algoritmo de encriptação/decriptação

  Realiza substituições e transformações para tornar a mensagem ilegível

- Chave secreta

  Entrada para o algoritmo que modifica a mensagem original

- Texto cifrado

  Mensagem embaralhada produzida pelo algoritmo

REQUISITOS PARA O USO SEGURO

PRIMEIRO

“Um oponente deverá ser incapaz de decifrar o texto cifrado ou descobrir a chave, mesmo que possua diversos textos cifrados com seus respectivos textos claros”

REQUISITOS PARA O USO SEGURO

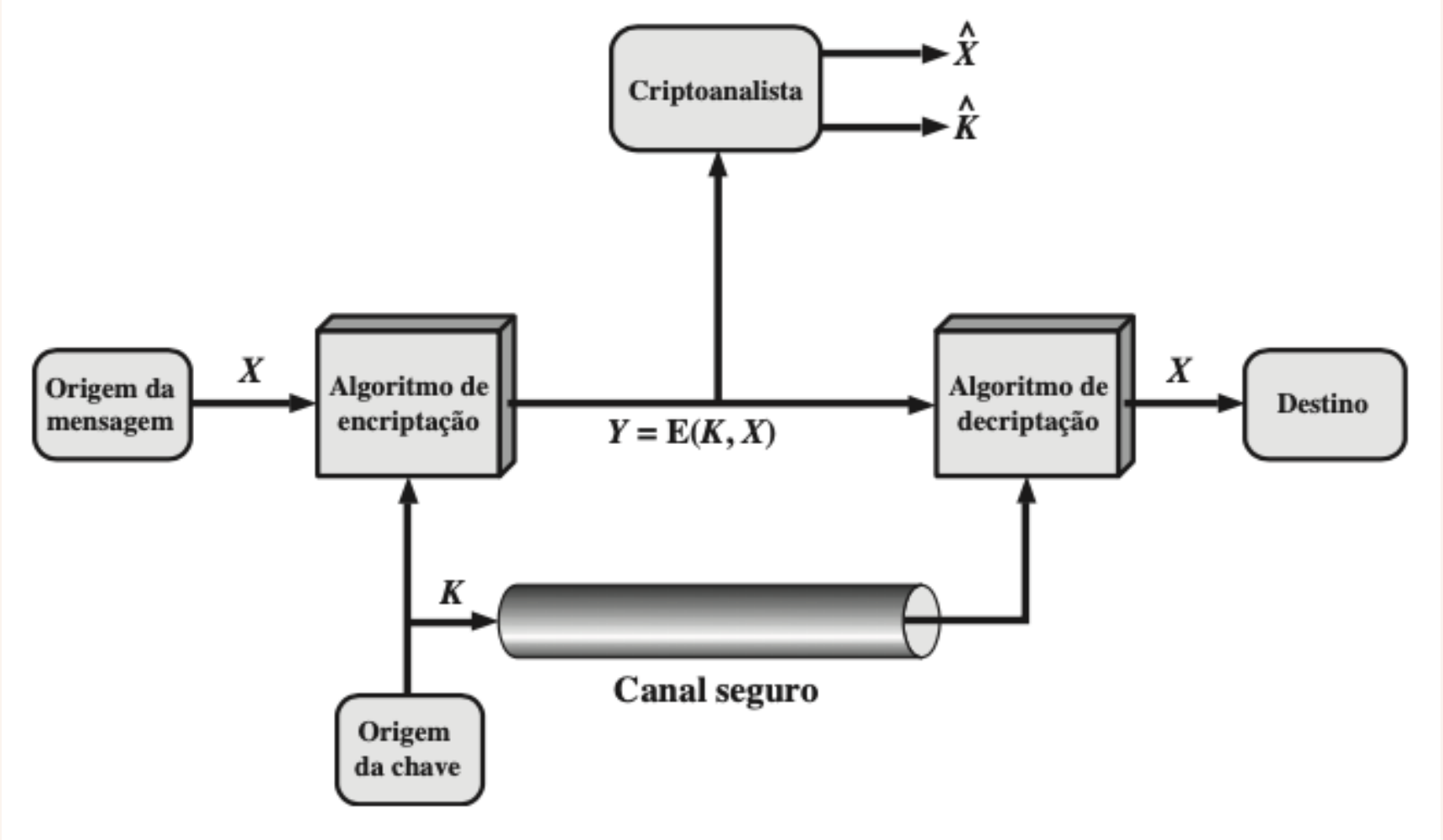
SEGUNDO

“Emissor e Receptor precisam ter obtido a chave secreta de forma segura. Se um oponente descobrir a chave e o algoritmo a comunicação está comprometida”

REQUISITOS PARA O USO SEGURO

OBSERVAÇÃO

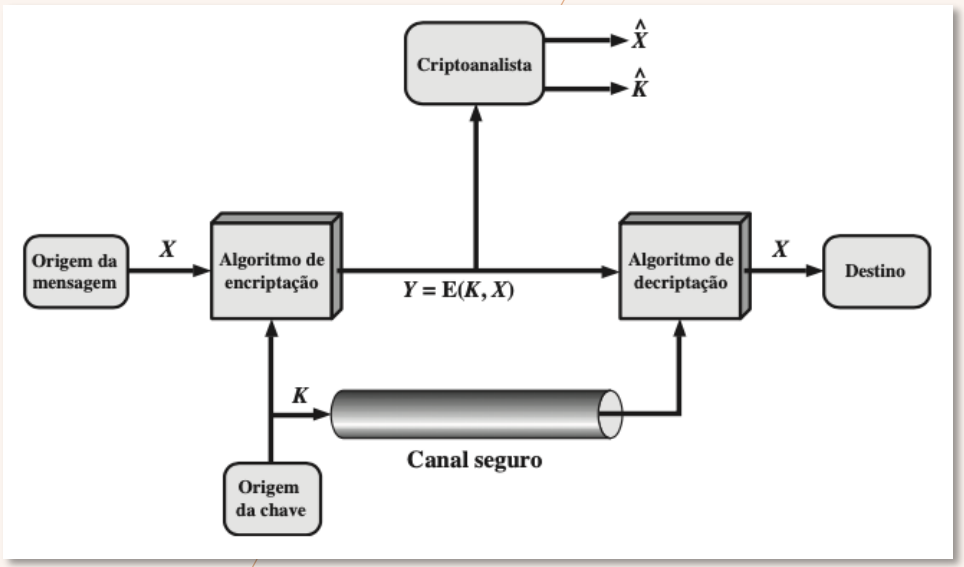
“O sigilo do algoritmo de encriptação/decriptação não é determinante para a segurança”


Criptoanalista
$\hat{X}$
$\hat{K}$
Origem da mensagem
X
Algoritmo de encriptação
Y = E(K, X)
Algoritmo de decriptação
X
Destino
K
Canal seguro
Origem da chave

TIPO DE ATAQUE	CONHECIDO AO CRIPTOANALISTA
Apenas texto cifrado	■ Algoritmo de encriptação ■ Texto cifrado
Texto claro conhecido	■ Algoritmo de encriptação ■ Texto cifrado ■ Um ou mais pares de texto claro-texto cifrado produzidos pela chave secreta
Texto claro escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Mensagem de texto claro escolhida pelo criptoanalista, com seu respectivo texto cifrado gerado com a chave secreta
Texto cifrado escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Texto cifrado escolhido pelo criptoanalista, com seu respectivo texto claro decriptado produzido pela chave secreta
Texto escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Mensagem de texto claro escolhida pelo criptoanalista, com seu respectivo texto cifrado produzido pela chave secreta ■ Texto cifrado escolhido pelo criptoanalista, com seu respectivo texto claro decriptado produzido pela chave secreta

Ataque Texto Cifrado Conhecido

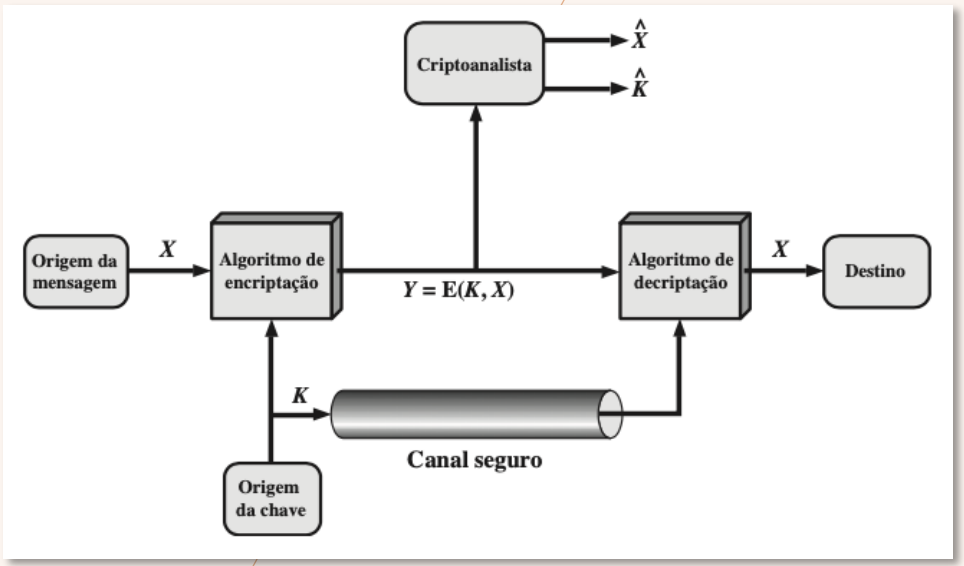
- Ataque usando a técnica de Força Bruta
- Utiliza testes estatísticos
- Necessário conhecer um padrão mínimo do texto claro
- Mais fácil de ser defendido
- Apenas algoritmos fracos não suportam esse tipo de ataque



Ataque Texto Claro Conhecido

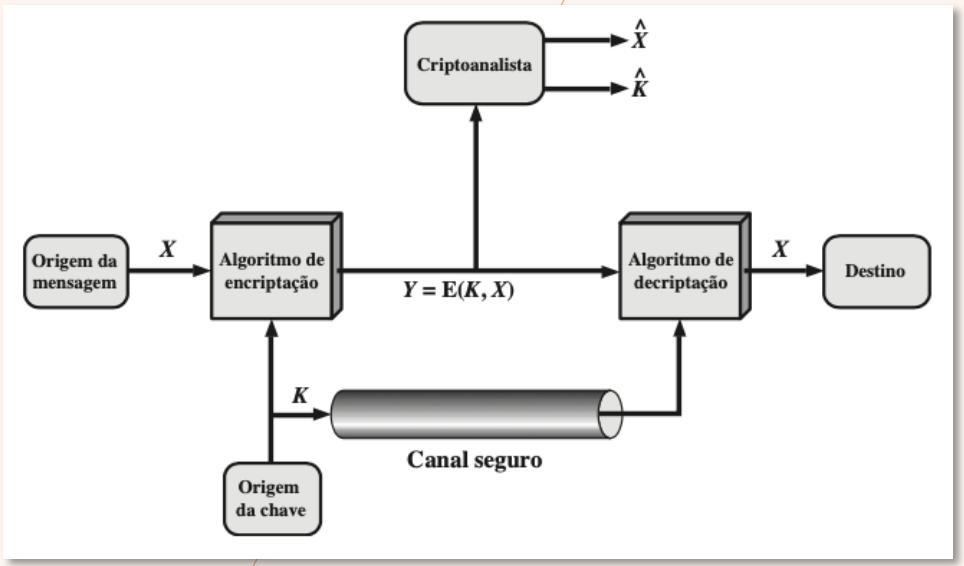
- Texto claro capturado
- Padrão de texto claro observado pelo oponente

  Banner padronizado, mensagem de copyright, padrões de arquivo
- Dedução da chave



Ataque Texto Claro Escolhido

- Injeta-se texto claro na origem para observar o texto cifrado e deduzir a chave



Encriptação Computacionalmente Segura

- Custo para quebrar a cifra ultrapassa o valor da informação encriptada
- Tempo exigido para quebrar a cifra supera o tempo de vida útil da informação

Classificação

- **Tipo de operação**
  Substituição ou Transposição
- **Quantidade de chaves**
  Simétrica ou assimétrica
- **Modo de processamento**
  Bloco ou Fluxo

Ataque de Força Bruta

- Metade das chaves precisa ser experimentada
- Texto claro em idioma conhecido facilita a quebra da chave
- Arquivos numéricos e/ou compactados dificultam a quebra da chave

Técnica de Substituição

Cifra de César

```
claro: meet me after the toga party
cifra: PHHW PH DIWHU WKH WRJD SDUWB
```

```
claro: 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
cifra: 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
```

Criptoanálise e Cifra de César

CHAVE	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg 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 glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

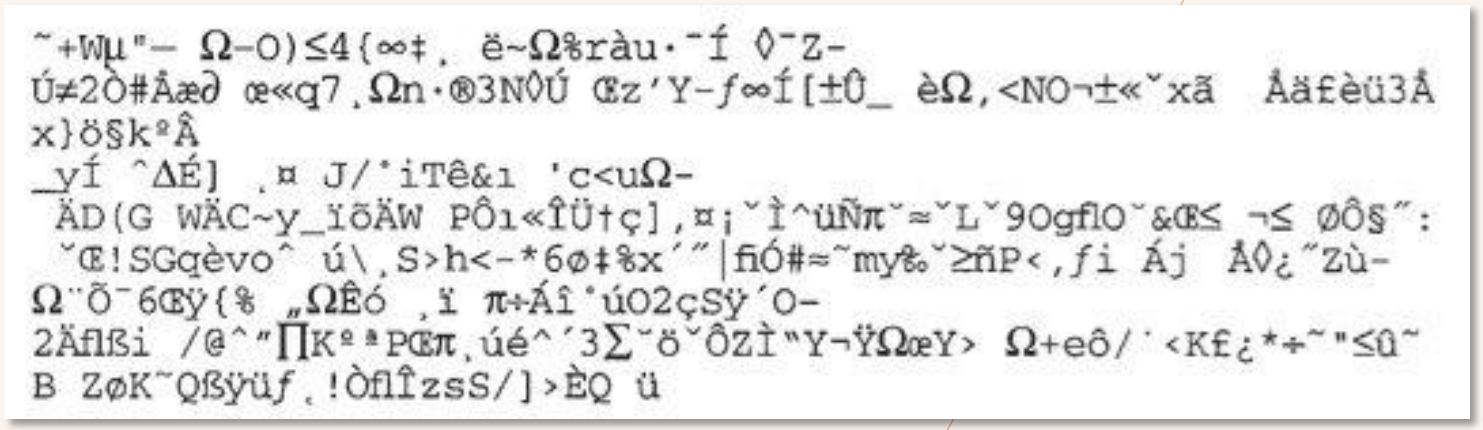
Criptoanálise e Cifra de César

- Algoritmos conhecidos
- Chave fraca
- Mensagem em texto claro identificável

CHAVE	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg 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 glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Criptoanálise de Texto Compactado

- Chave de 168 bits
- ZIP de um arquivo texto plano



Cifras Monoalfabéticas

- A cifra de César respeita a sequência do alfabeto cifrado criando 25 possibilidades de chave
- As cifras monoalfabéticas trazem um aprimoramento substituindo cada letra por QUALQUER outra letra em uma ordem específica

  a->Q

  b->W

  c->E

  d->R

Cifras Monoalfabéticas

- Chaves de cifras de substituição monoalfabéticas possuem **26!** Possibilidades
- Aparenta segurança comparada a cifra de César
- Mesmo com pequena quantidade de texto a cifra pode ser quebrada com estratégias de **propriedades estatísticas de idiomas**

Exemplo de Texto Cifrado

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Frequência Relativa

- Considerando que o texto é em Inglês
- Extrair a frequência relativa do texto cifrado
- Comparar com a frequência do idioma

P 13,33	H 5,83	F 3,33	B 1,67	C 0,00
Z 11,67	D 5,00	W 3,33	G 1,67	K 0,00
S 8,33	E 5,00	Q 2,50	Y 1,67	L 0,00
U 8,33	V 4,17	T 2,50	I 0,83	N 0,00
O 7,50	X 4,17	A 1,67	J 0,83	R 0,00
M 6,67				

Frequência Relativa

- É provável que P e Z correspondam a 'e' e 't'
- É provável S, U, O, M e H correspondam ao conjunto {a, h, i, n, o, r, s}
- A, B, G, Y, I, J devem pertencer ao conjunto {b, j, k , q, v, x, z}

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Frequência Relativa

- Busca pelo digrama mais frequente em inglês: th

  Corresponde ao ZW

- Busca pelo trigrama mais frequente: the

  Corresponde ao ZWP

- A sequência ZWSZ na primeira linha

  Corresponde a th?t

  Fazendo uma tentativa de atribuição a that, teríamos S=a

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Resultado Parcial

- A partir de 4 letras

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a         e   e te   a that e e a         a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t    ta t ha e ee   a e   th     t   a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e   e e tat   e    the    t
```

Resultado Final

- Continuando a análise da frequência e o conhecimento do idioma

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Cifras de Substituição

- A frequência do alfabeto original se reflete no alfabeto da cifra, facilitando sua quebra
- Uma melhoria da CS consiste em utilizar vários alfabetos de cifra

  Cifras polialfabéticas
- Outra possível melhoria seria o uso de homófonos

  Atribuir várias símbolos diferentes em rodízio para mesma letra

  Cifra Playfair

  Cifra de Hill

Cifras Polialfabéticas

- Utilizam um conjunto de regras monoalfabéticas simultaneamente
- Uma chave determina a regra específica
- Cifra de Vigenère

  Utiliza as 26 cifras de César
- Exemplo

Exemplo

```
chave:              deceptivedeceptivedeceptive
texto claro:        wearediscoveredsaveyourself
texto cifrado:      ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Exemplo

```
chave:              deceptivewearediscoveredsav
texto claro:        wearediscoveredsaveyourself
texto cifrado:      ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Fragilidades CV

- Estudo de criptoanálise pode determinar que foi utilizada uma cifra mono ou polialfabética

  Estatísticas de Frequência

- É possível determinar o tamanho da palavra chave buscando padrões de repetição no texto cifrado

One Time Pad

- Chave do mesmo tamanho da mensagem
- Chave descartada após o uso
- Sistema inquebrável
- Exemplo

texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
texto claro:*	mr mustard with the candlestick in the hall
texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt*
texto claro:**	miss scarlet with the knife in the library

Fragilidades OTP

- Sistema inquebrável, porém pouco prático
- A largura de banda exigida para as chaves é similar aos dados
- Problema de distribuição de chaves

texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
texto claro:*	mr mustard with the candlestick in the hall
texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	*mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt*
texto claro:**	miss scarlet with the knife in the library

Técnicas de Transposição

Transposição

- Técnicas que envolvem a permutação das letras do texto claro
- Rail Fence
- Exemplo

  Meet after the toga party

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

Rail Fence

Chave:	4 3 1 2 5 6 7
Texto claro:	a t t a c k p
	o s t p o n e
	d u n t i l t
	w o a m x y z
Texto cifrado:	TTNAAPTMTSUOAODWCOIXKNLYPETZ

Cifras de Transposição

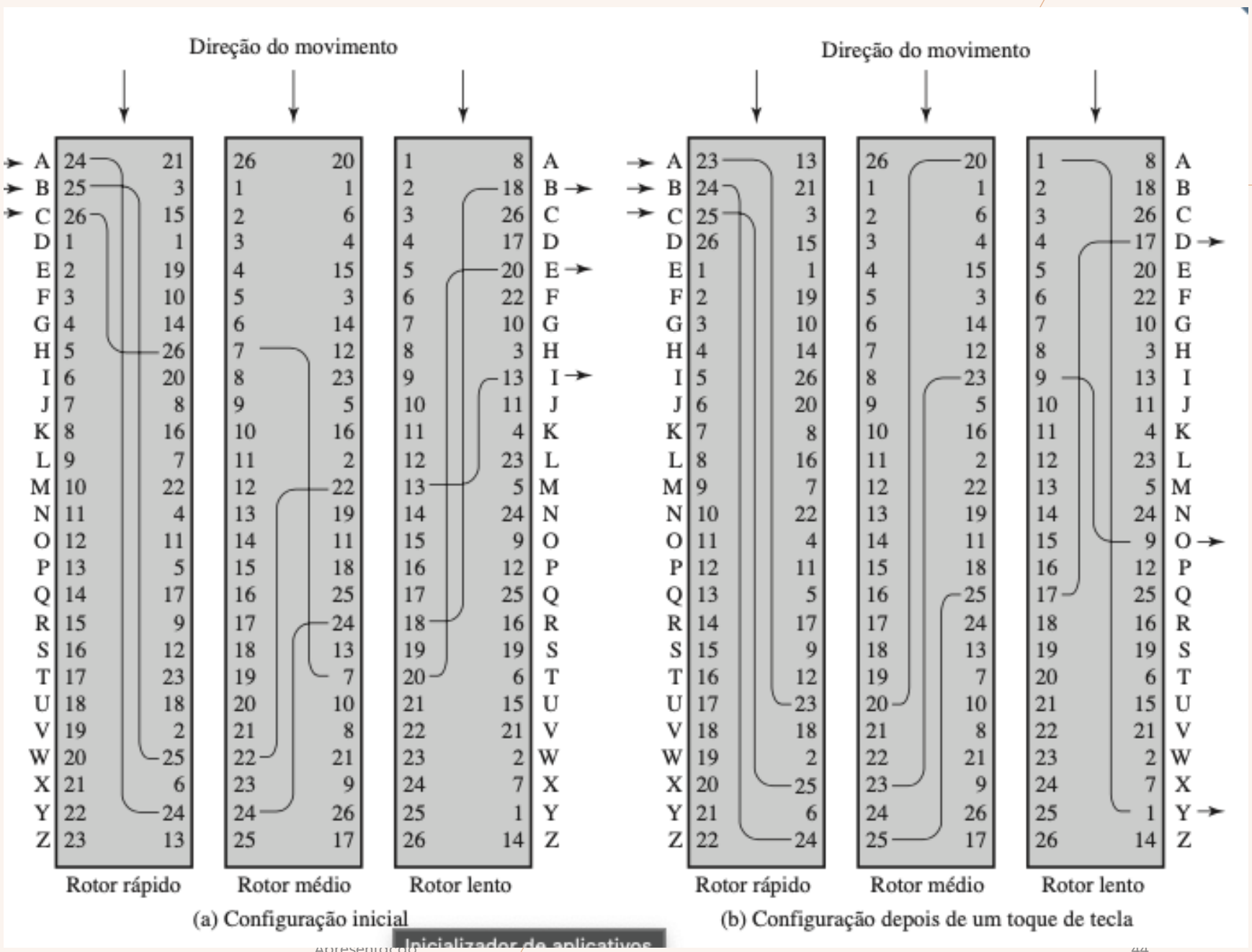
- Criptoanálise explora as CT através das estatísticas de frequência aplicadas as cifras alfabéticas
- Melhorias são obtidas aplicando múltiplos estágios de transposição

Máquinas de Rotor

Máquinas de Rotor

- Aplica várias etapas de encriptação
- Precursor da encriptação DES
- Conjunto de cilindros independentes
- 26 pinos de entrada + 26 pinos de saída

Máquinas de Rotor



Exemplos

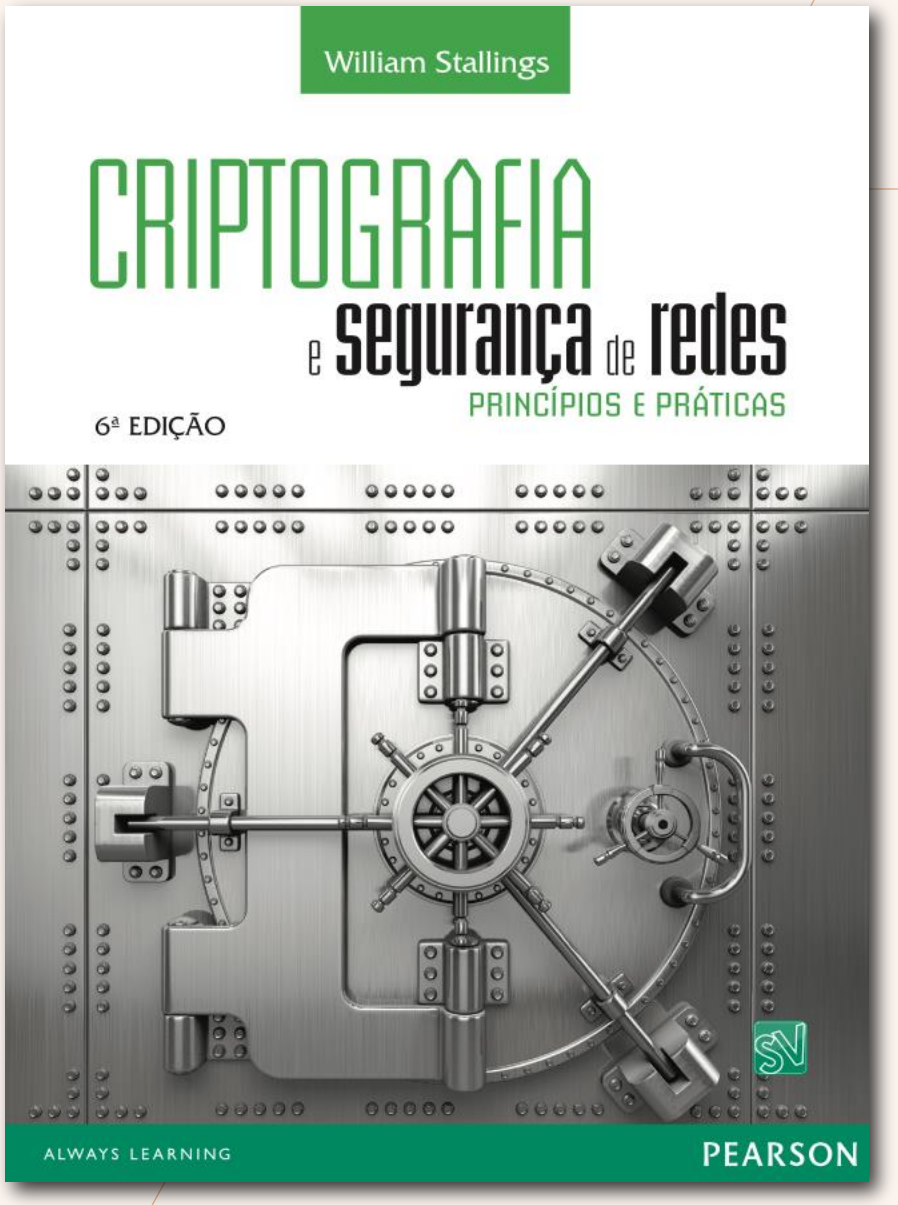
- Aplicando 3 rotores com 26 letras cada tem-se 17.576 alfabetos possíveis
- Com 4 rotores 456.976 alfabetos
- Uma máquina com 5 rotores é equivalente a uma Cifra de Vigenère com chave de tamanho maior que 11 milhões de letras
- Enigma e Purple foram máquinas usadas na segunda guerra.

Referências

- https://www.youtube.com/watch?v=5w3zDa7bgLU
- https://www.youtube.com/watch?v=E0YX8BC4RLo

Referências

- **Capítulo 2**. Criptografia e Segurança de Redes. *William Stallings*. 6ª. Edição. Editora Pearson.



FIM

Prof. José Roberto Bezerra

jbroberto@ifce.edu.br

IFCE – *Campus* Fortaleza