Técnicas Clássicas de Criptografia

Criptografia e Segurança de Redes, Cap. 2
Willian Stallings
4 Ed. Pearson, 2008

Conceitos

- A palavra “Criptografia”
- Conceito de Código
- Conceito de Cifra
- Criptoanálise
- Força Bruta
- Técnicas de Substituição
- One-Time Pad (chave de uso único)
- Técnicas de Transposição
- Esteganografia

Conceito de Código

- Substitui uma **palavra por outra palavra** ou uma **palavra por um símbolo**.

- **Códigos, no sentido da criptografia, não são mais utilizados**, embora tenham tido uma história …
  - O código na linguagem navajo dos índios americanos, utilizado pelos mesmos contra os japoneses na Segunda Guerra Mundial.

Conceito de Código

- A linguagem navajo era caracterizada apenas por sons.
- Um código é uma transformação que envolve somente duas partes.
- O que é gerado chama-se uma codificação.

Conceito de Código

- A transformação leva em conta a **estrutura linguística da mensagem** sendo transformada.

- Lembre da transformação em um compilador.

Conceito de Cifra

- É uma **transformação de caractere por caractere** ou **bit pot bit**, **sem levar em conta a estrutura linguística da mensagem**.

- Substituindo um por outro.
- Transpondo a ordem dos símbolos.

Esteganografia

- **Esteganografia** (do grego "escrita escondida") é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma de segurança por obscurantismo.

Esteganografia

- Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido.

Esteganografia

- É importante frisar a diferença entre criptografia e esteganografia. Enquanto a primeira oculta o significado da mensagem, a segunda oculta a existência da mensagem.

- http://pt.wikipedia.org/wiki/Esteganografia

Significado da palavra “Criptografia”

- A palavra **criptografia** vem das palavras gregas que significam “**escrita secreta**”.

- *Kriptos* (em grego) = Secreto + Grafia (de escrever)
- *Criptografia* = Escrita secreta.
- **Criar mensagens cifradas**.

- História de milhares de anos.

Jargões da Criptografia

- Encripta (codifica, criptografa, cifra)
- Decripta (decodifica, decriptografa, decifra)

Criptografia

- Possui emprego nas mais diferentes áreas de atuação, mas em todas, tem o mesmo significado:
  - **proteger informações consideradas ‘especiais’ ou de qualidade sensível**.

Criptografia

- Atualmente a CRIPTOGRAFIA é definida como a **ciência que oculta e/ou protege informações – escrita, eletrônica ou de comunicação**.

Criptografia

- É o ato de alterar uma mensagem para esconder o significado desta.

- Mas, como esconder ?
  - Criando um **código** ?
  - Criando **cifra** ?

Criptoanálise

- Tenta deduzir um texto claro específico ou quebrar a chave utilizada.

- Natureza do algoritmo
- Talvez algumas características do texto claro
- Pares de amostra de texto claro e texto cifrado

Modelo de Cripto-Sistema Convencional

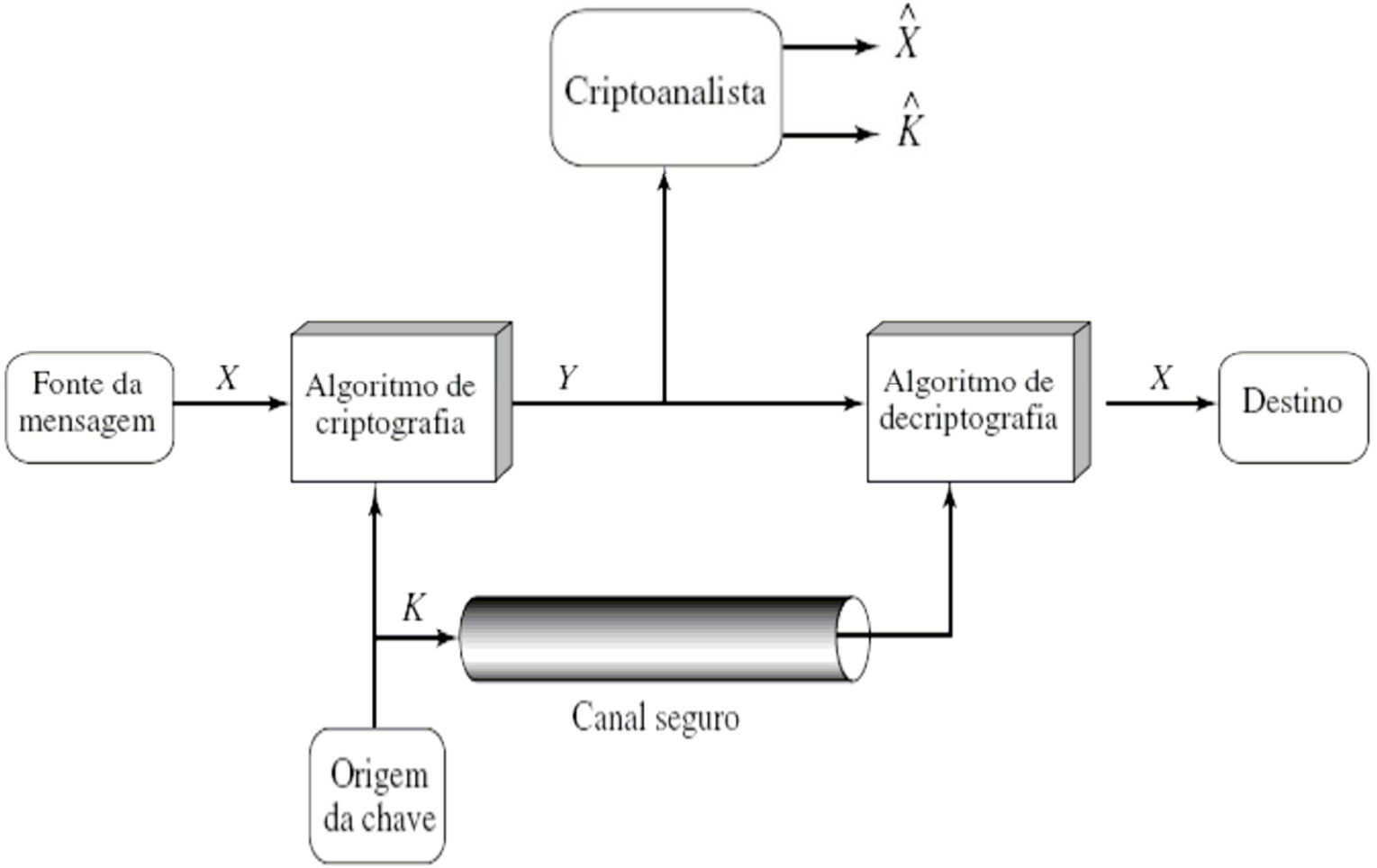


Figura 2.2 Modelo de criptossistema convencional

Tabela 2.1 Tipos de ataques a mensagens criptografadas

Tipo de ataque	Conhecido ao criptoanalista
Apenas texto cifrado	• Algoritmo de criptografia • Texto cifrado
Texto claro conhecido	• Algoritmo de criptografia • Texto cifrado • Um ou mais pares de texto claro/texto cifrado formados com a chave secreta
Texto claro escolhido	• Algoritmo de criptografia • Texto cifrado • Mensagem de texto claro escolhida pelo criptoanalista, juntamente com seu texto cifrado correspondente, gerado com a chave secreta
Texto cifrado escolhido	• Algoritmo de criptografia • Texto cifrado • Texto cifrado pretendido, escolhido pelo criptoanalista, juntamente com seu texto claro decriptografado correspondente, gerado com a chave secreta
Texto escolhido	• Algoritmo de criptografia • Texto cifrado • Mensagem de texto claro escolhida pelo criptoanalista, juntamente com seu texto cifrado correspondente, gerado com a chave secreta • Texto cifrado pretendido, escolhido pelo criptoanalista, juntamente com seu texto claro decriptografado correspondente, gerado com a chave secreta

Definições dignas de nota

- Incondicionalmente Seguro

  Um esquema de criptografia é incondicionalmente seguro se o texto cifrado gerado não tiver informações suficientes para determinar exclusivamente o texto claro correspondente.

  Não existe algoritmo incondicionalmente seguro.

Definições dignas de nota

- Computacionalmente seguro

  Se um dos critérios for atendido:

  - Custo para quebrar a cifra é superior ao valor da informação cifrada.

  - Tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

Ataque por Força Bruta

- Envolve a tentativa de usar cada chave possível até que uma, proporcione uma tradução inteligível do texto cifrado para o texto claro.

- Na média, metade de todas as chaves possíveis precisa ser experimentada para se conseguir sucesso.

Tabela 2.2 Tempo médio exigido para busca completa da chave

Tamanho da chave (bits)	Número de chaves alternativas	Tempo necessário para 1 decriptografia/μs	Tempo necessário para 10^6 decriptografias/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milissegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1142 anos	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ anos	$5{,}4 \times 10^{18}$ anos
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ anos	$5{,}9 \times 10^{30}$ anos
26 caracteres (permutação)	$26! = 4 \times 10^{26}$	2×10^{26} μs = $6{,}4 \times 10^{12}$ anos	$6{,}4 \times 10^6$ anos

Criptografia Tradicional

- Historicamente, os **métodos tradicionais de criptografia** são divididos em duas categorias:
  - Cifras de **Substituição**
  - Cifras de **Transposição**

Cifras de Substituição

- Cada **letra** ou **grupo de letras** é substituído por **outra letra** ou **grupo de letras**, de modo a criar um “disfarce”.

- Exemplo: A Cifra de César (Caeser Cipher).

  Considerando as 26 letras do alfabeto inglês (a,b,c,d,e,f,g,h,I,j,k,m,n,o,p,q,r,s,t,u,v,x,w,y,z),

  Neste método, a se torna **D**, b se torna E, c se torna F, … …, z se torna **C**.

Cifra de César

- Para cada letra “p” do texto claro, substitui pela letra “C” no texto cifrado:

- Atribui-se um equivalente numérico para cada letra (a=1, b=2, …)

- $C = E(p) = (p+3) \bmod 26$

Cifras de Substituição

- Cifra de César:
  - cada letra é deslocada 3 vezes.
- A chave tem o mesmo tamanho que o texto claro.

- Para um texto claro como:

```
meet me after the toga party
```

- O texto cifrado será:

```
PHHW PH DIWHU WKH WRJD SDUWB
```

- Teremos 25 chaves possíveis.

Generalização da Cifra de César

- Cada letra se desloca *k* vezes, em vez de três. Neste caso, k passa a ser uma chave para o método genérico dos alfabetos deslocados de forma circular.

- C = E(p)= (p+k) mod 26
- Um deslocamento pode ser qualquer k=1..25
- p = D(C) = (C-k) mod 26

KEY						
	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

Figura 2.3 Criptoanálise pela força bruta da cifra de César.

Cifras de Substituição Monoalfabética

- Próximo aprimoramento:
  - Cada letra do texto simples, do alfabeto de 26 letras, seja mapeada para alguma outra letra.

- a -> Q, b -> W, c -> E, d -> R, e ->T, ...

- Esse sistema geral é chamado **cifra de substituição monoalfabética.**

Cifras de Substituição Monoalfabética

- Sendo a **chave** uma *string* de 26 letras correspondente ao alfabeto completo.
- Quebra da chave: 26! chaves possíveis.

Cifras de Substituição

- As **cifras de substituição** **preservam a ordem dos símbolos** no texto claro, **mas disfarçam esses símbolos**.

Cifras de Substituição Monoalfabética

- Entretanto, apesar de parecer seguro, com um volume de texto cifrado surpreendentemente pequeno, a cifra pode ser descoberta.

- Estratégia: a propriedades estatísticas dos idiomas.

Cifras de Substituição Monoalfabética

- Inglês: e é a letra mais comum, seguida de *t, o, a, n, i, ...*
- Digramas mais comuns: *th, in, er, re, na, ...*
- Trigramas mais comuns: *the, ing, and, ion.*

Cifras de Substituição Monoalfabética

- Criptoanalista: descriptografar uma cifra monoalfabética ... ...
- Conta as frequências relativas de todas as letras do texto cifrado.
- Substitui com a letra *e* à letra mais comum e *t* à próxima letra mais comum.

Cifras de Substituição Monoalfabética

- Em seguida, os trigramas ...
- Fazendo estimativas com relação a digramas, trigramas e letras comuns ...

Cifras de Substituição Monoalfabética

- e conhecendo os prováveis padrões de vogais e consoantes, o criptoanalista pode criar um texto simples, através de tentativas, letra por letra.

Cifras de Substituição Monoalfabética

- Outra estratégia é **descobrir uma palavra ou frase provável**, a partir do conhecimento de **alguma palavra muito provável**, dentro do contexto de alguma área profissional ...

- Como, por exemplo, ***financial*** na área de contabilidade.

Força bruta na Cifra de César

- Os algoritmos de criptografia e descriptografia são conhecidos.
- Existem apenas 25 chaves a serem experimentadas.
- A linguagem do texto claro é conhecida e facilmente reconhecível.

Força Bruta

- Na maioria da vezes o algoritmo é conhecido.
- O que pode tornar a criptoanálise impraticável é o uso de um algoritmo que emprega uma chave de tamanho considerável.
- 3DES usa chave de 168 bits = 2 x E168 chaves possíveis.

Linguagem do Texto Claro

- Se a linguagem do texto claro for desconhecida, então a saída de texto cifrado pode não ser reconhecível.

- A entrada pode até ser compactada de alguma maneira ... Dificultando o reconhecimento.

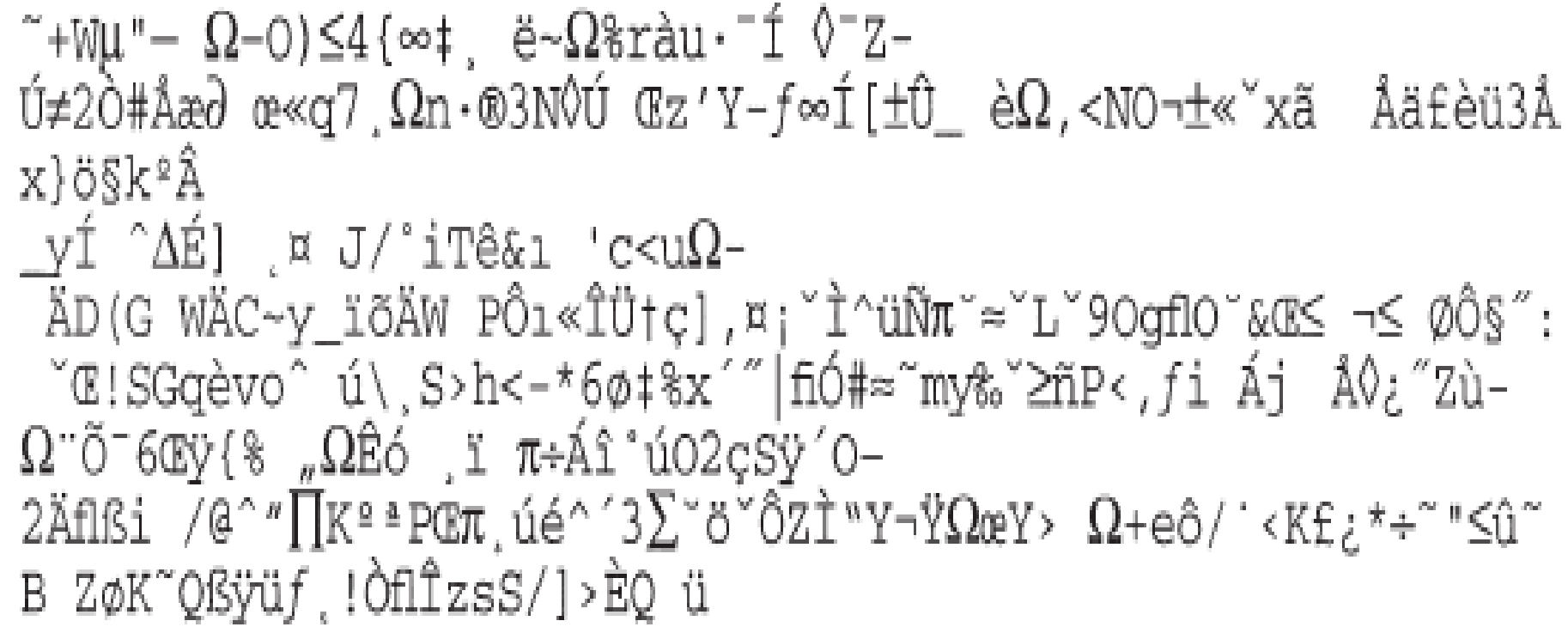


Figura 2.4 Exemplo de texto compactado.

Cifra Polialfabética

- Um modo de melhorar a cifra monoalfabética.

Key: *deceptivedeceptivedeceptive*

wearediscoveredsaveyourself

Cifra de Vigènere

ZICVTWQNGRZGVTWAVZHCQYGLMGJ

- Ver tabela de Vegenère a seguir.

Tabela 2.3 A tabela de Vigenère moderna

Chave	Texto 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
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

Cifra de Transposição

- **Cifras de Transposição** reordenam os símbolos, mas não os disfarçam.

- Exemplo: cifra de transposição de colunas.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

- A cifra se baseia numa chave que é uma palavra ou uma frase que não contém letras repetidas.
- Seja a chave: MEGABUCK
- O objetivo da chave é numerar as colunas de modo que a coluna 1 fique abaixo da letra da chave mais próxima do início do alfabeto e assim por diante.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

- O texto simples é escrito horizontalmente, em linhas.
- O texto cifrado é lido em colunas, a partir da coluna cuja letra da chave tenha a ordem mais baixa no alfabeto.
- A numeração abaixo da chave, significa a ordem das letras no alfabeto.

Exemplo de Cifra de Transposição

Fonte: Redes de Computadores, A. S. Tanenbaum, Cap. 8

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Confusão x Difusão

- Diz-se que uma substituição acrescenta “confusão” à informação.
- Diz-se que uma “transposição” acrescenta “difusão” à informação.

Confusão

- “Confusão” torna a relação entre a chave k e um texto cifrado, mais complexa, de modo que seja difícil para um criptoanalista deduzir qualquer propriedade da chave k, a partir do texto cifrado.

Difusão

- “Difusão” embaralha os bits do texto legível para que qualquer redundância seja eliminada no texto cifrado.

Elementos básicos de Cifras

- Caixa P (Transposição é obtida por Permutação)
- Caixa S (Substituição)
- Cifra de Produto (Junta-se Permutações e Susbstituições)

Elementos básicos de Cifras

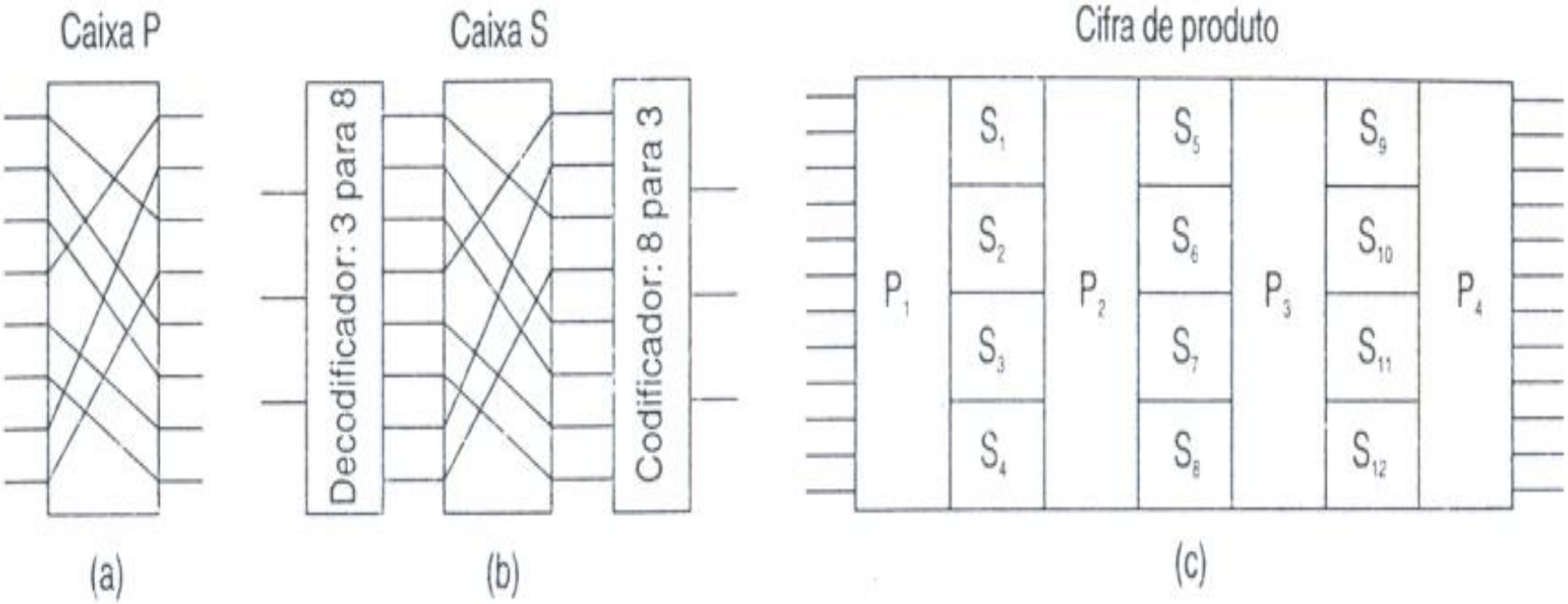


Figura 8.6 Elementos básicos de cifras de produtos.
(a) Caixa P. (b) Caixa S. (c) Produto

Chave de Uso Único

- Na realidade, é uma chave de uso único (one-time-pad).
- Uma cifra inviolável, cuja técnica é conhecida há décadas.
- Começa com a escolha de uma chave de bits aleatórios.

Chave de Uso Único

- Exemplo de como as chaves únicas são usadas:
  - Seja o **texto claro 1**: *“I love you”.*
  - Converter o **texto claro 1** em código ASCII.
  - Escolher uma **chave 1** de bits aleatórios.
  - Encontrar um **texto cifrado 1**, fazendo **XOR** entre o **texto claro 1** com a **chave 1**.

Chave de Uso Único

```
Mensagem 1:       1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Chave 1:          1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado:    0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Chave 2:          1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto simples 2:  1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011
```

Figura 8.4 O uso de uma chave única para criptografia e a possibilidade de conseguir qualquer texto simples que seja possível a partir do texto cifrado pela utilização de alguma outra chave

Chave de Uso Único

- Escolher outra chave, a **chave 2**, diferente da **chave 1** usada somente uma vez.

- Fazer **XOR** da **chave 2** com o **texto cifrado 1,** e encontrar, em ASCII, um possível texto claro

Chave de Uso Único

```
Mensagem 1:       1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Chave 1:          1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado:    0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Chave 2:          1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto simples 2:  1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011
```

Figura 8.4 O uso de uma chave única para criptografia e a possibilidade de conseguir qualquer texto simples que seja possível a partir do texto cifrado pela utilização de alguma outra chave

Chave de Uso Único

- O **texto cifrado 1 não pode ser violado** porque, em uma amostra suficientemente grande de texto cifrado, **cada letra ocorrerá com a mesma frequência** (decorrente da escolha de uma chave de bits aleatórios).

- O mesmo para digramas e cada trigrama.

Chave de Uso Único

- Neste exemplo, a chave única, **chave 2**, poderia ser experimentada, resultando no texto simples 2, que está em ASCII e que pode ser ou não plausível.

Chave de Uso Único

- Isto é, todos os textos simples 2 possíveis, com o tamanho dado, são igualmente prováveis.

- De fato, para cada texto simples 2 com código ASCII de 11 caracteres (texto simples 2), existe uma chave única que o gera.

Chave de Uso Único

- Por isso é que se diz que não existe nenhuma informação no texto cifrado.

- É possível obter qualquer mensagem com o tamanho correto a partir do texto cifrado.

Chave de Uso Único – Imune a ataques

- Esse método é imune a todos os ataques atuais e futuros, independente da capacidade computacional do intruso.

- A razão deriva da Teoria da Informação:

  simplesmente, porque não existe nenhuma informação no **texto simples 2**, suficiente para se chegar de volta à mensagem original.

Chave de Uso Único – Dificuldades Práticas

- As chaves únicas são ótimas na teoria, mas tem várias desvantagens na prática.

- As chaves, em binário, são difíceis de ser memorizadas.

Chave de Uso Único - Dificuldades Práticas

- A quantidade total de dados que podem ser transmitidos é limitada pelo tamanho da chave disponível.

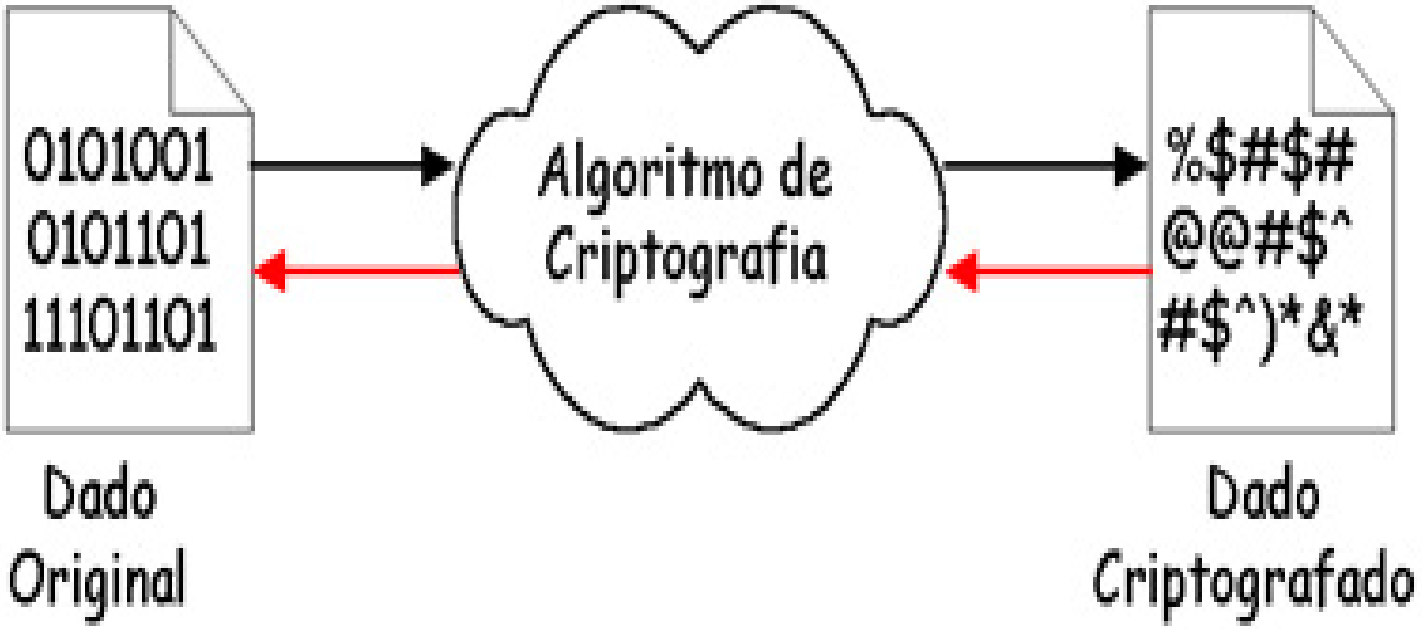
Chave de Uso Único – Dificuldades Práticas

- Insensibilidade do método quanto a caracteres perdidos ou inseridos.

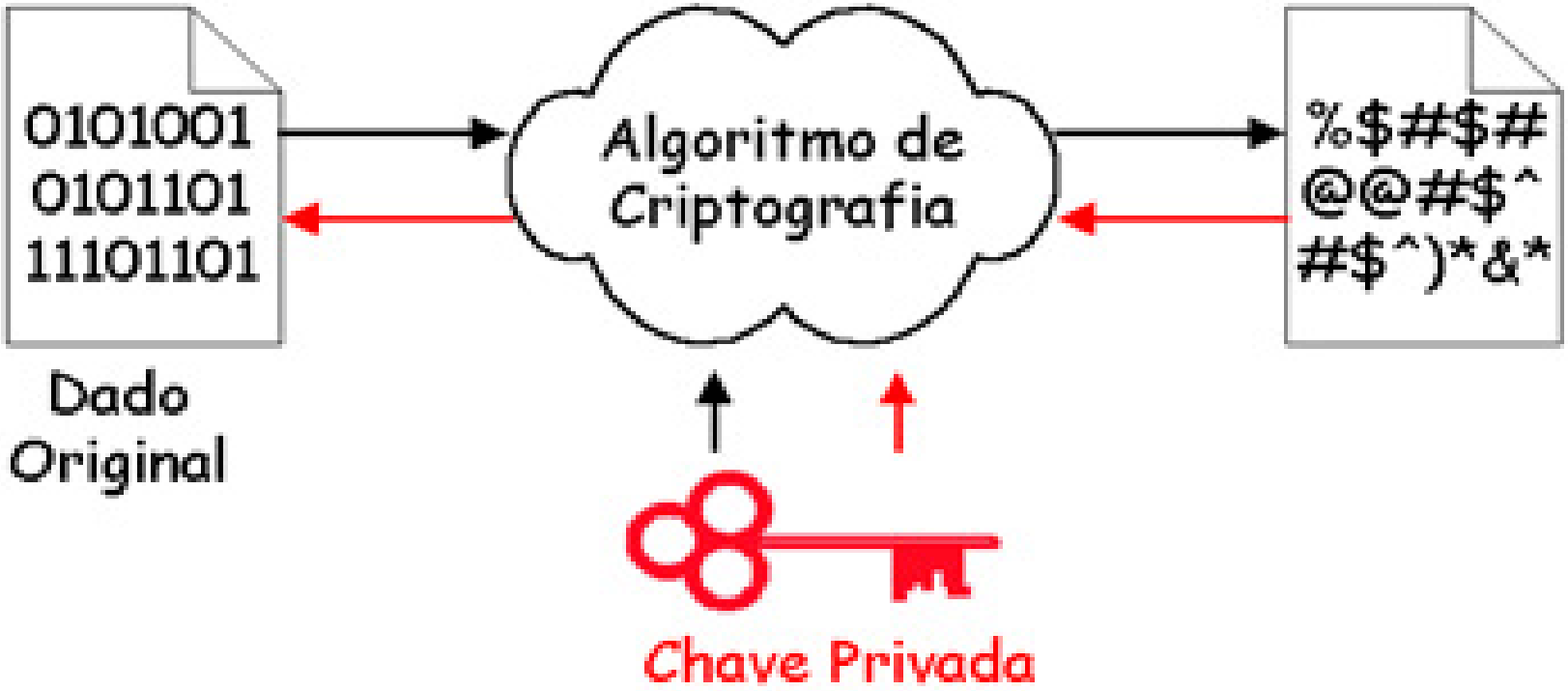
- Se o transmissor e o receptor ficarem sem sincronismo, todos os caracteres a partir desse momento parecerão adulterados.

Criptografia convencional

- Os procedimentos de criptografar e decriptografar são obtidos através de um algoritmo de criptografia.



Criptografia Simétrica



Modelo Simplificado de Criptografia Convencional

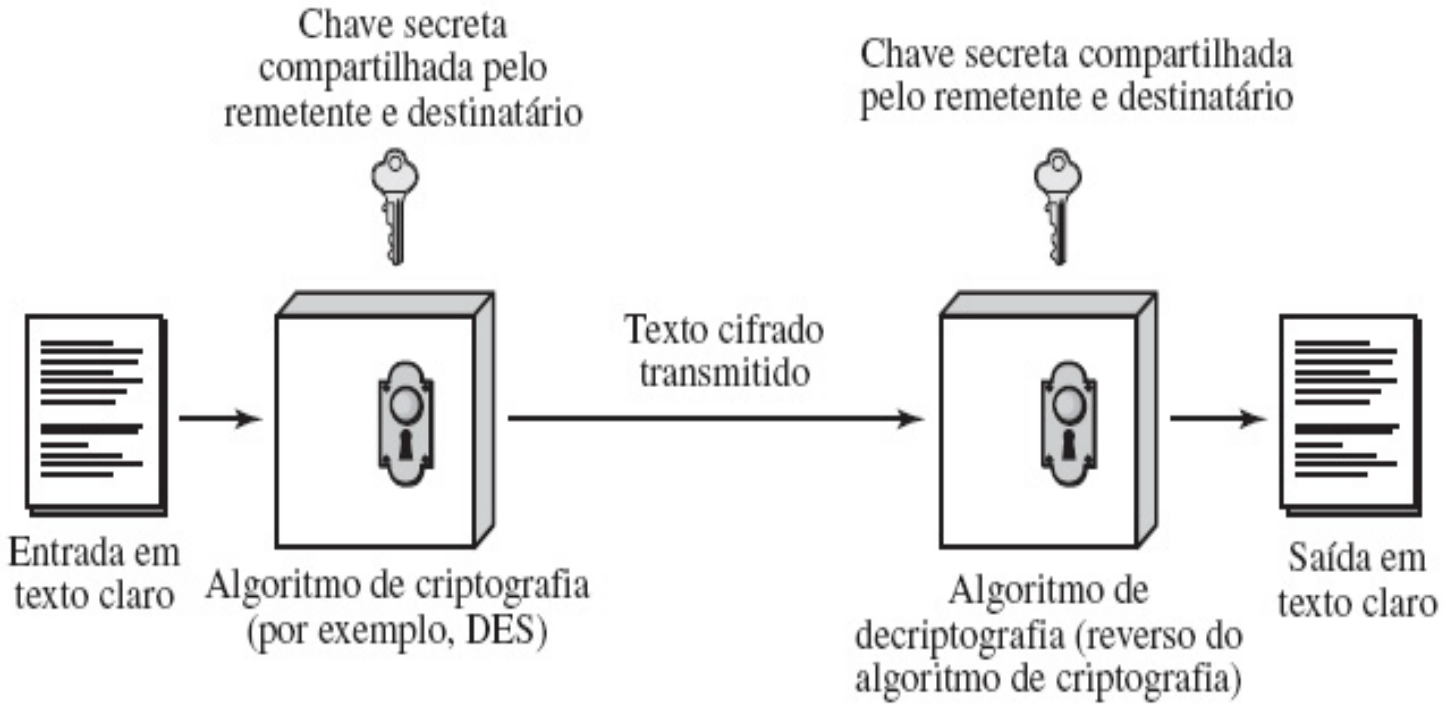
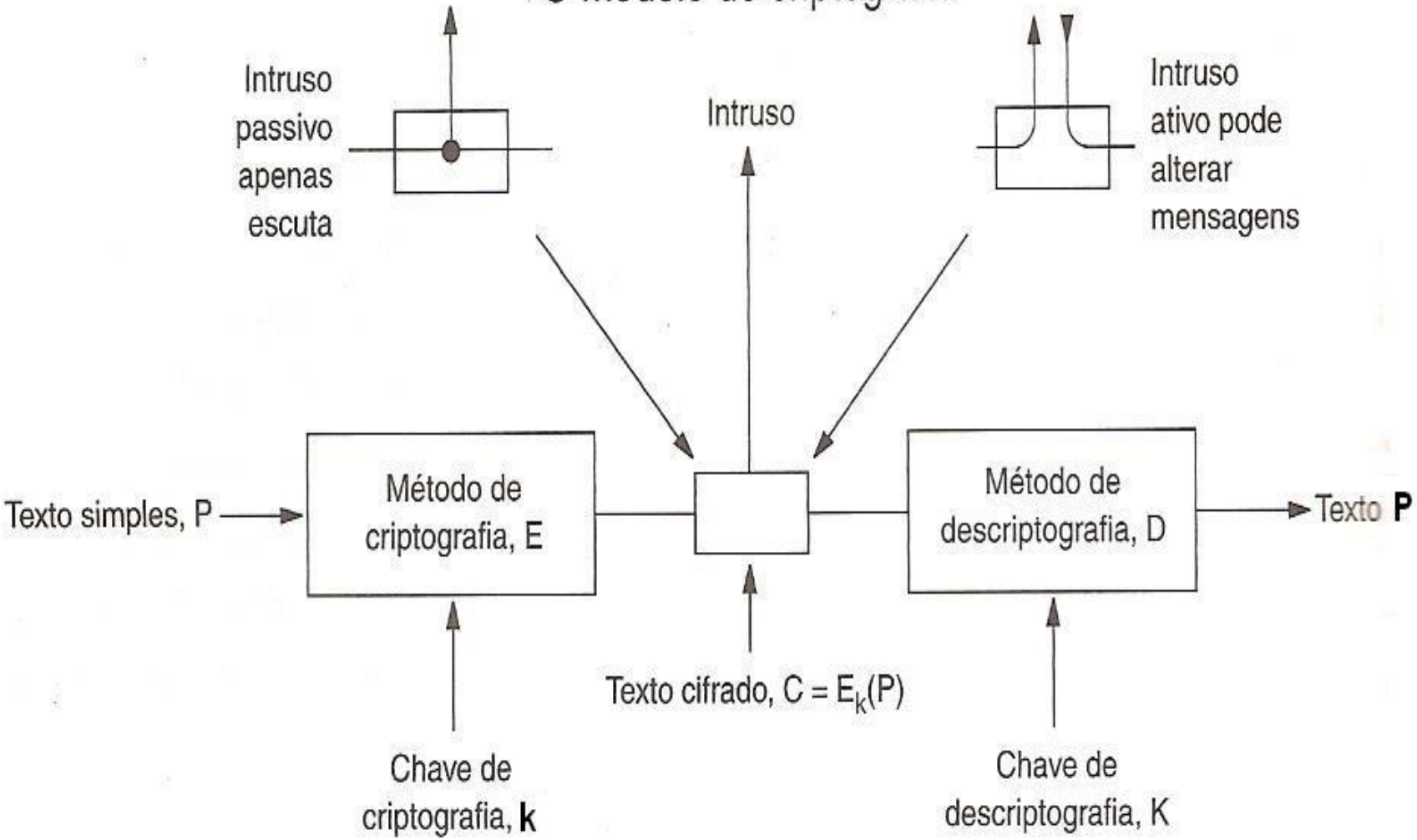


Figura 2.1 Modelo simplificado da criptografia convencional.

O modelo de criptografia



Equações da Criptografia

$$D_k (E_k(P)) = P$$

E e D são funções matemáticas

K é uma **chave**

Técnicas envolvendo criptografia simétrica

- Garantia de Confidencialidade
- Garantia de Privacidade
- Existem vários algoritmos conhecidos.

Técnicas envolvendo criptografia simétrica

- **Algoritmos de Criptografia de Chave Simétrica,**
- **Modos de Cifra**
- **Gerenciamento de Chaves Simétricas**