Criptografia Simétrica

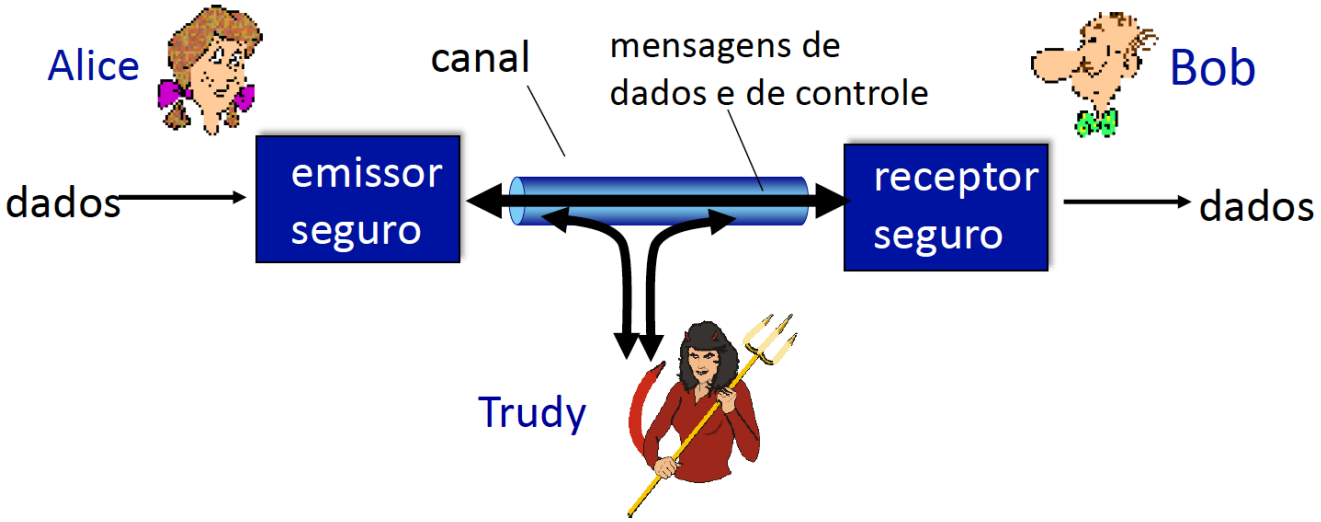
Introdução

Prof. Roberto Rodrigues-Filho
Dept. de Ciência da Computação (CIC)
Universidade de Brasília (UnB)

Criptografia Simétrica

Amigos e inimigos: Alice, Bob, Trudy

- bem conhecidos no mundo da segurança de rede
- Bob e Alice (amigos!) querem se comunicar “com segurança”
- Trudy (intrusa) pode interceptar, excluir, adicionar mensagens



roberto.filho@unb.br

Criptografia Simétrica

Amigos e inimigos: Alice, Bob, Trudy

Quem seriam Bob e Alice?

- … bem, Bobs e Alices da *vida real*!
- navegador/servidor da Web para transações eletrônicas (por exemplo, compras online)
- cliente/servidor de banco online
- servidores DNS
- roteadores BGP trocando atualizações da tabela de roteamento
- outros exemplos?

Criptografia Simétrica

Existem bandidos por aí!

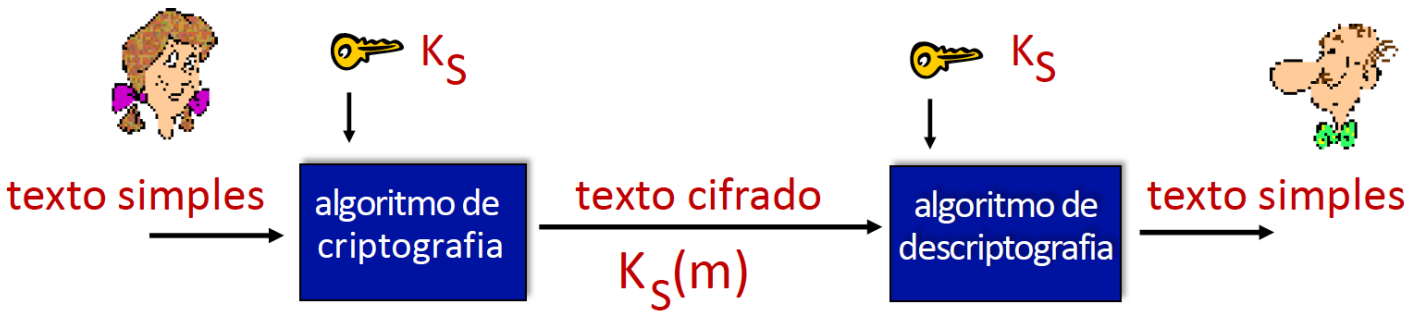
Q: O que um "cara mau" pode fazer?

A: Muito! (lembre-se da seção 1.6)

- bisbilhotar (*eavesdrop*): interceptar mensagens
- inserir ativamente mensagens na conexão
- personificação: pode falsificar (*spoof*) o endereço de origem no pacote (ou qualquer campo no pacote)
- sequestro (*hijacking*): "assumir" a conexão em andamento, removendo o remetente ou o destinatário, inserindo-se no lugar
- negação de serviço (*denial of service*): impedir que o serviço seja usado por outros (por exemplo, sobrecarregando recursos)

Criptografia Simétrica

Criptografia de chave simétrica



Criptografia de chave simétrica: Bob e Alice compartilham a mesma chave (simétrica): K

- *por exemplo*, a chave é conhecer o padrão de substituição em uma cifra de substituição mono alfabética

Q: como Bob e Alice concordam com o valor da chave?

roberto.filho@unb.br

Criptografia Simétrica

Esquema de criptografia simples

cifra de substituição: substituindo uma coisa por outra

- cifra monoalfabética: substitui uma letra por outra

```
texto simples:   abcdefghijklmnopqrstuvwxyz
                 |                       |
texto cifrado:   mnbvcxzasdfghjklpoiuytrewq
```

exemplo:

```
texto simples: bob. i love you. alice
texto cifrado: nkn. s gktc wky. mgsbc
```

Chave de encriptação: mapeamento de um conjunto de 26 letras para um conjunto de 26 letras

roberto.filho@unb.br

Criptografia Simétrica

- Pontos negativos:
  - Poucas combinações: apenas 25 → ataques de força bruta
  - Análise estatística do uso de letras no alfabeto.

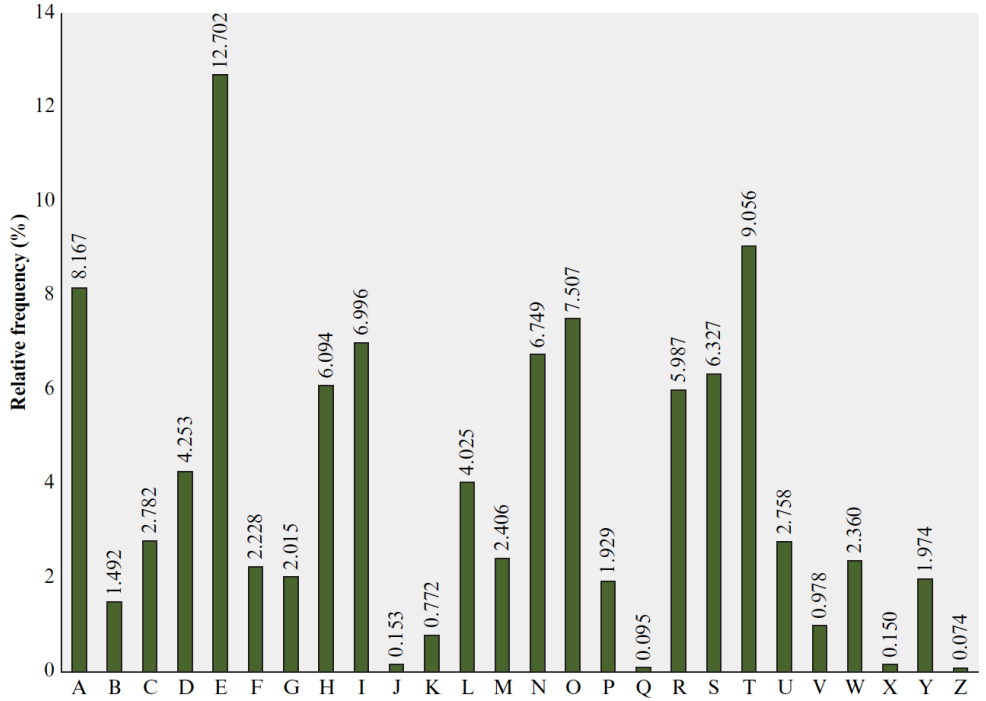


Figure 3.5 Relative Frequency of Letters in English Text

Criptografia Simétrica

- Pontos negativos:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

roberto.filho@unb.br

Criptografia Simétrica

- Pontos negativos:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

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				

Criptografia Simétrica

- Pontos negativos:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQ
EPYEPOPDZSZUFPOMBZWPFUPZHMD
```

P	13.33	H	5.83	F	3.33	B	1.67
Z	11.67	D	5.00	W	3.33	G	1.67
S	8.33	E	5.00	Q	2.50	Y	1.67
U	8.33	V	4.17	T	2.50	I	0.83
O	7.50	X	4.17	A	1.67	J	0.83
M	6.67						

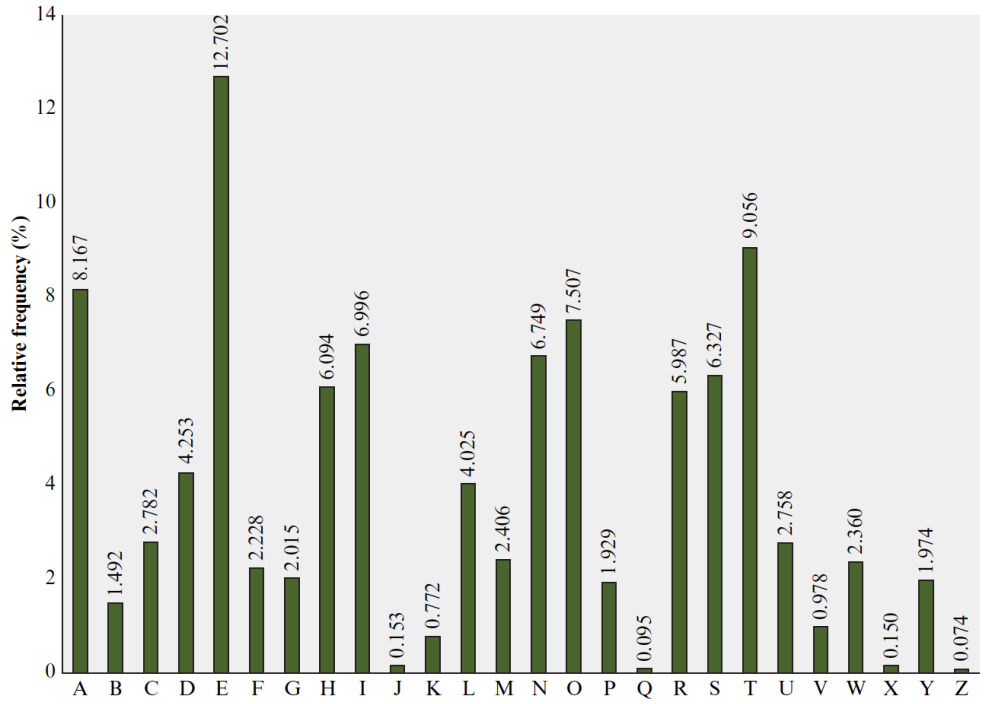


Figure 3.5 Relative Frequency of Letters in English Text

Criptografia Simétrica

- Pontos negativos:

```
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
```

P 13.33	H 5.83	F 3.33	B 1.67
Z 11.67	D 5.00	W 3.33	G 1.67
S 8.33	E 5.00	Q 2.50	Y 1.67
U 8.33	V 4.17	T 2.50	I 0.83
O 7.50	X 4.17	A 1.67	J 0.83
M 6.67			

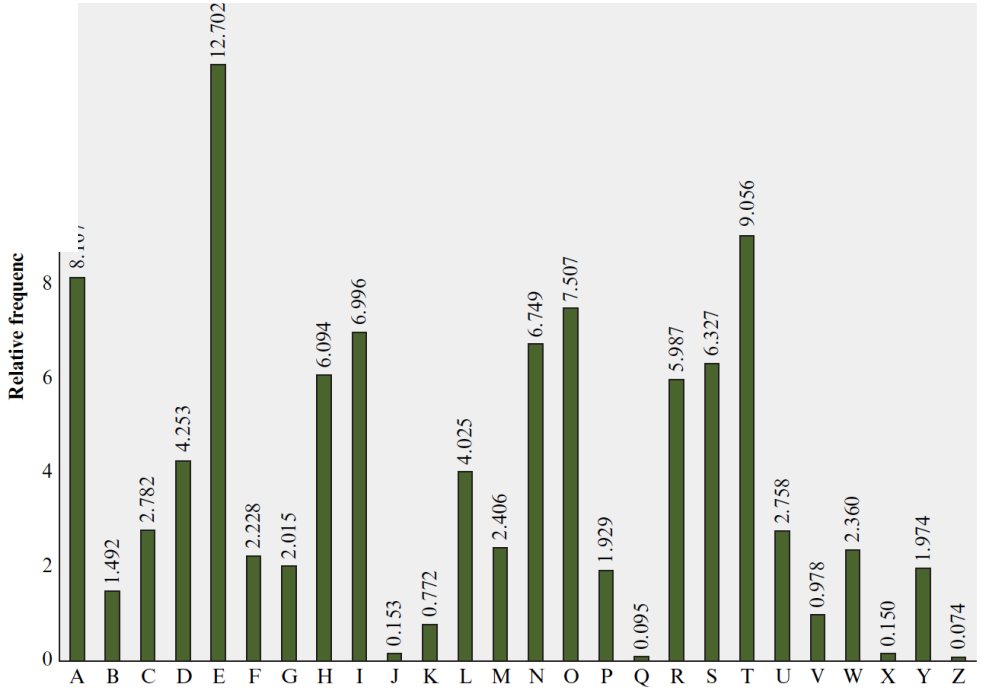


Figure 3.5 Relative Frequency of Letters in English Text

roberto.filho@unb.br

Criptografia Simétrica

- Pontos negativos:

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

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				

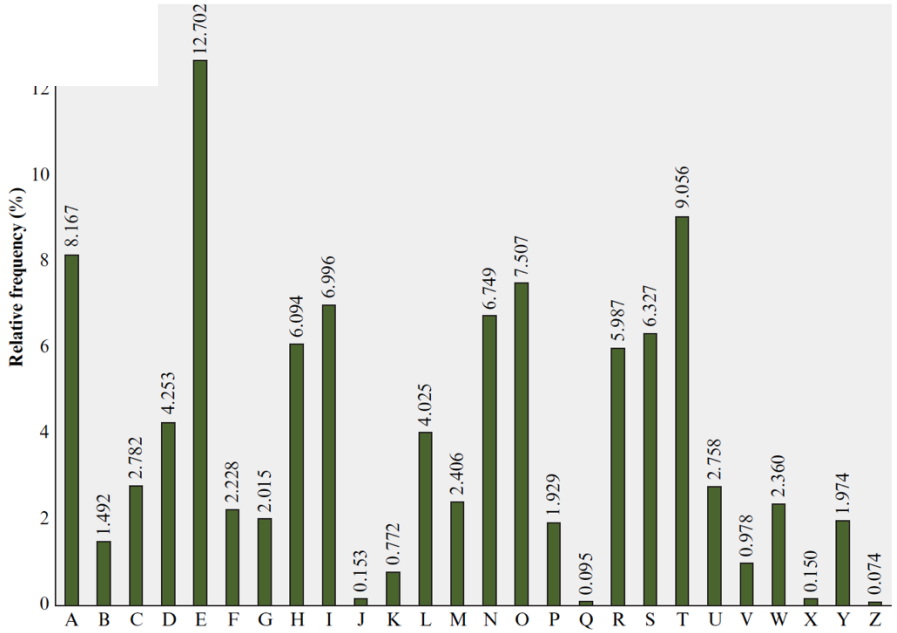
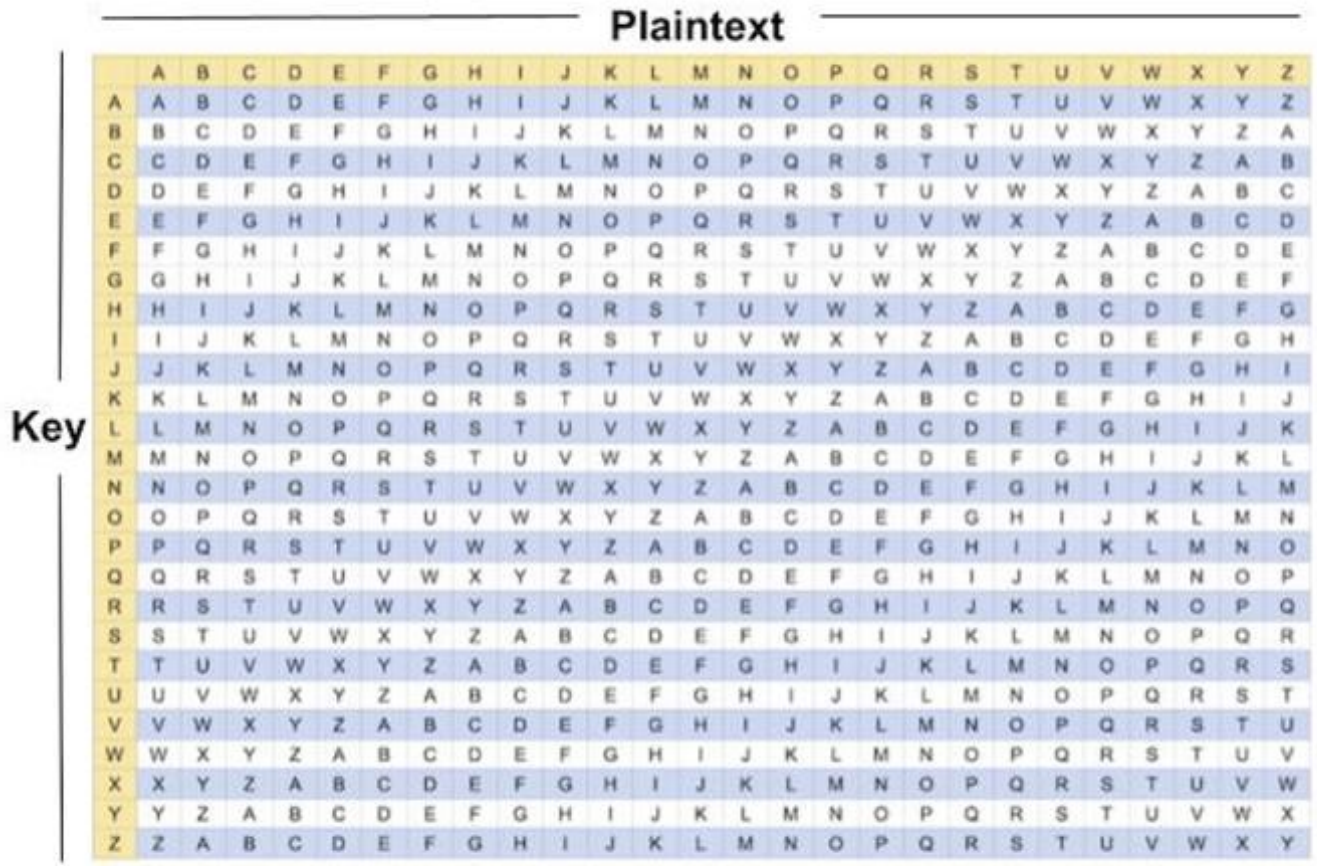


Figure 3.5 Relative Frequency of Letters in English Text

roberto.filho@unb.br

Criptografia Simétrica

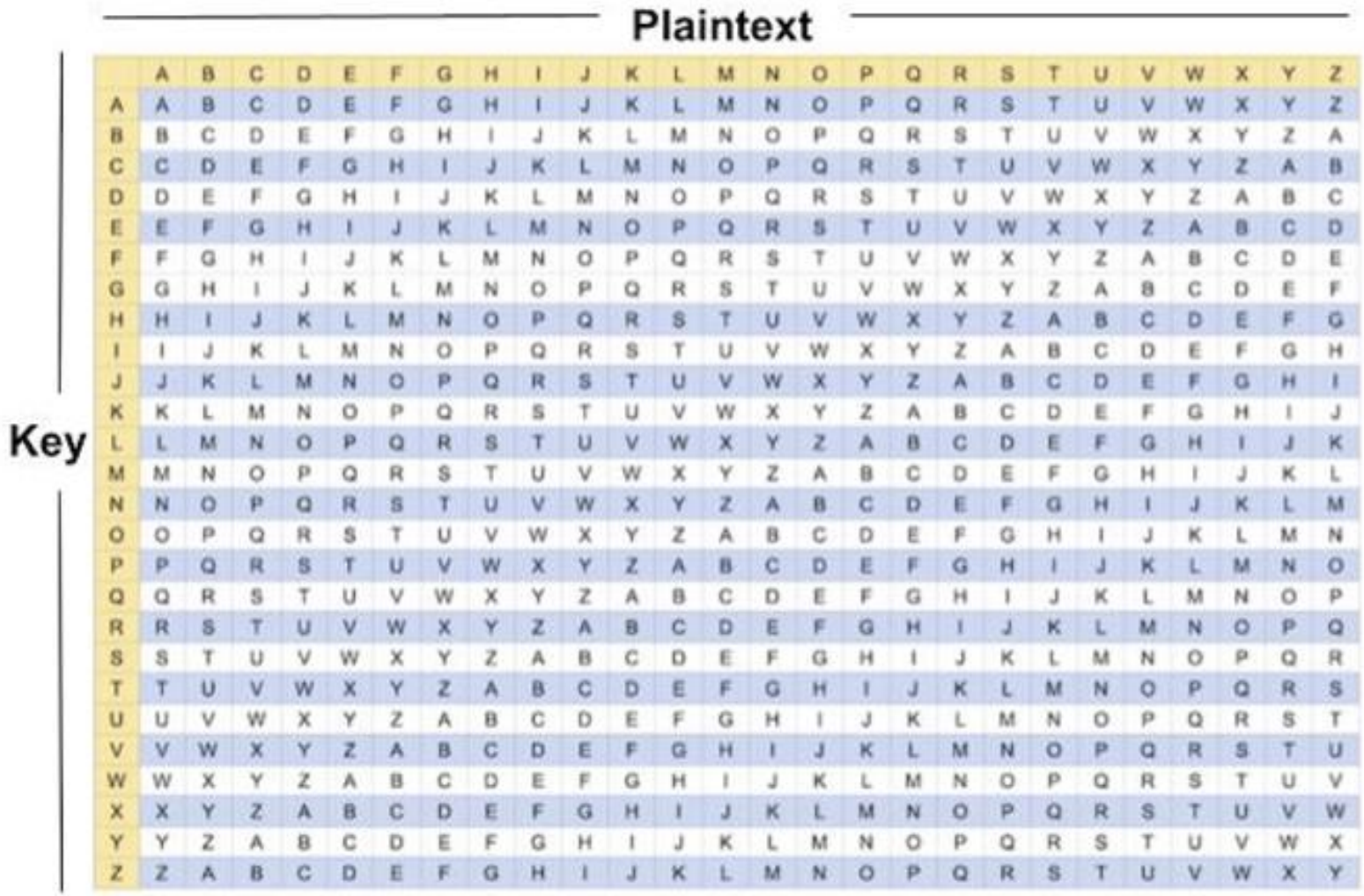
- Polialfabetica: Vigenère



	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

roberto.filho@unb.br

Criptografia Simétrica



Key \ Plaintext	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

Criptografia Simétrica

- Polialfabetica: Vigenère
  - Quando a chave é curta
    - → força bruta
    - → análise de frequência

roberto.filho@unb.br

Criptografia Simétrica

- Cifra de Transposição
  - Cifras de Transposição reordenam os símbolos, mas não os disfarçam.
  - Texto: “o ataque foi adiado para as 3 pm”
  - Chave: 31245

roberto.filho@unb.br

Criptografia Simétrica

- Cifra de Transposição
  - Cifras de Transposição reordenam os símbolos, mas não os disfarçam.
  - Texto: “o ataque foi adiado para as 3 pm”
  - Chave: 31245

o	a	t	a	q
u	e	f	o	i
a	d	i	a	d
o	p	a	r	a
a	s	3	p	m

roberto.filho@unb.br

Criptografia Simétrica

- Cifra de Transposição
  - Texto: “oataquefoiadiadoparaas3pm”
  - Chave: 31245
  - Cifra: “tfia3ouaoaaedpsaoarpqidam”

o	a	t	a	q
u	e	f	o	i
a	d	i	a	d
o	p	a	r	a
a	s	3	p	m

roberto.filho@unb.br

Criptografia Simétrica

- Uma cifra monoalfabética

Letra no texto aberto:	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
Letra no texto cifrado:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

- Uma cifra polialfabética que utiliza duas cifras de César

Letra do texto aberto:	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
$C_1(k = 5)$:	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
$C_2(k = 19)$:	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

- Uma cifra de bloco de 3 bits específica

Entrada	Saída	Entrada	Saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

roberto.filho@unb.br

Criptografia Simétrica

- Uma cifra monoalfabética

Letra no texto aberto:	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
Letra no texto cifrado:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

- Uma cifra polialfabética que utiliza duas cifras de César

Letra do texto aberto:	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
$C_1(k = 5)$:	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
$C_2(k = 19)$:	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

- Uma cifra de bloco de 3 bits específica

Entrada	Saída	Entrada	Saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

roberto.filho@unb.br

Criptografia Simétrica

- Cifra de bloco
  - Divide o a mensagem em blocos. Ex.: k = 64
  - Cada bloco tem seu mapeamento
  - A chave é o mapeamento (criptografa e descriptografa)
  - Ex.: k = 3. Possível mapeamento. Tamanho de mapeamento: 8.Total de mapeamentos: 8! = 40.320.

Entrada	Saída	Entrada	Saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Criptografia Simétrica

- Cifra de bloco
  - Divide o a mensagem em blocos. Ex.: k = 64
  - Cada bloco tem seu mapeamento
  - A chave é o mapeamento (criptografa e descriptografa)
  - Ex.: k = 3. Possível mapeamento. Tamanho de mapeamento: 8.Total de mapeamentos: 8! = 40.320.
  - **DEVE SER REVERSÍVEL**

Reversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	00
11	01

Irreversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	01
11	01

Criptografia Simétrica

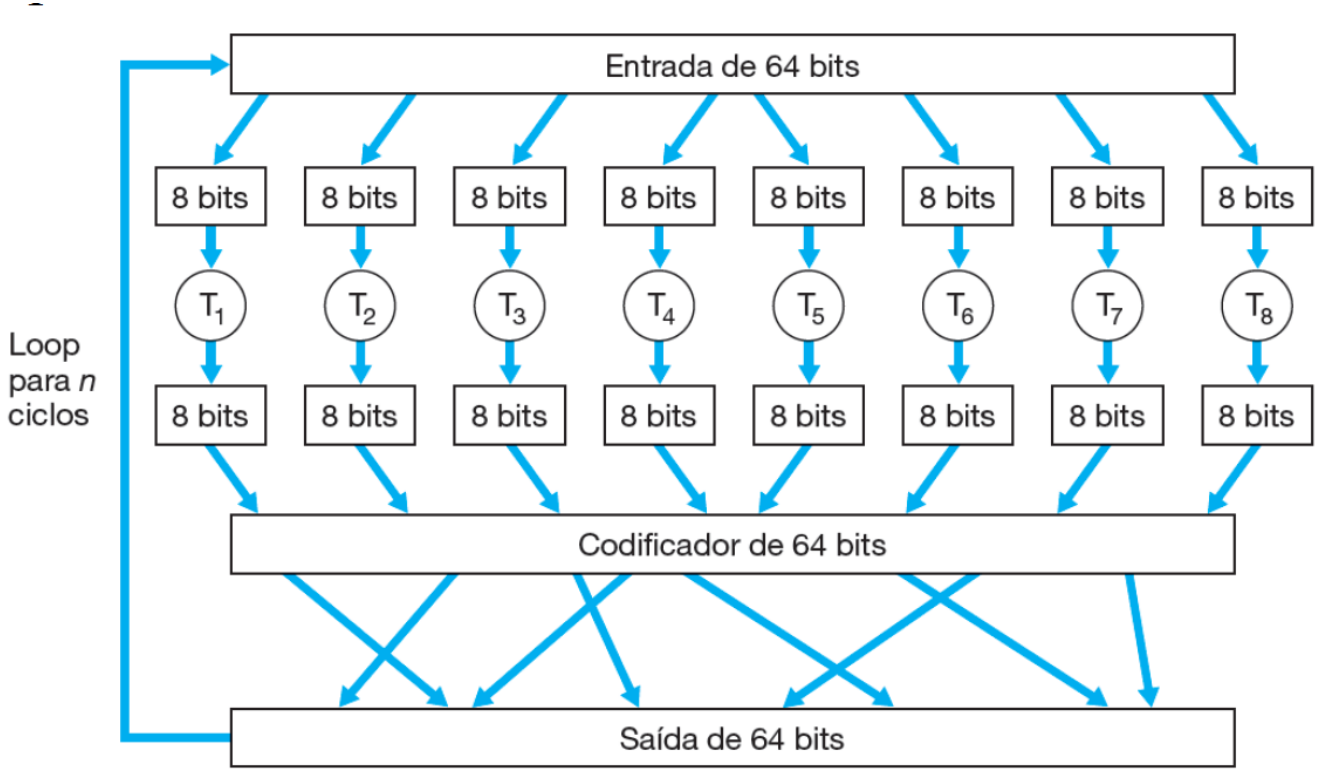
- Cifra de bloco
  - Tamanho da tabela para blocos de tamanho k:
    - Tamanho = 2^k
  - Quantidade possibilidades (força bruta)
    - 2^k!
  - Suficientemente grande para k = 64.
  - Dificuldade de implementa!
    - Precisa de tabelas grandes. Ex.: 2^64, p/ k = 64
    - Ruim manter essa quantidade de informação na memória.
    - Ruim fazer troca de chave (transmitir por rede, etc.).

Criptografia Simétrica

- Cifra de bloco
  - Usamos funções para simular a tabela.
  - Dividimos os 64 bits em 8 blocos de 8 bits
  - Aplicamos tabelas de mapeamento de 8 bits para 8 bits (tamanho gerenciável)
  - Após cada bloco ser substituído, ele é embaralhado
  - Esse processo é executado várias vezes para aumentar a robustez do método.

roberto.filho@unb.br

Criptografia Simétrica – Estrutura de Feistel



Criptografia Simétrica

- Encadeamento de blocos de cifra
  - Em alguns casos, como por exemplo em redes, um texto plano pode se repetir. Ex.: HTTP/1.1
  - Assim, o mesmo texto, aparecendo na mesma posição, vai ter o mesmo resultado.
  - Ideia principal:
    - c(i) = K(m(i) + r(i)), onde + (neste slide) significa XOR
    - r(i) bits aleatórios gerados na hora de criptografar
    - Dado quando trafegado precisa conter c(i) e r(i)
    - **PROBLEMA**

Criptografia Simétrica

- Encadeamento de blocos de cifra
  - Ideia principal:
    - c(i) = K(m(i) + r(i)), onde + (neste slide) significa XOR
    - r(i) bits aleatórios gerados na hora de criptografar
    - Dado quando trafegado precisa conter c(i) e r(i)
    - **PROBLEMA**
    - Manda c(i) + Vetor de Inicialização