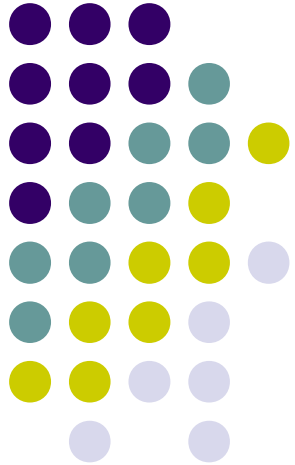
Universidade Federal de São Paulo – UNIFESP

Segurança Computacional

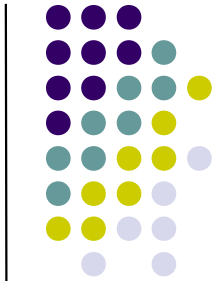
Aula 03: Criptografia, Algoritmos e Criptoanálise

Prof.
Valério Rosset



Apresentação baseada no Livro Criptografia e Segurança de Redes: Princípios e Prática, 4a Ed. de William Stallings.

Criptologia

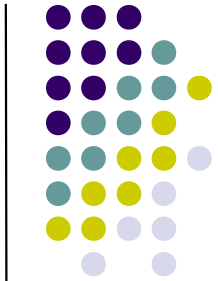


- *Criptografia*:
  - Elemento básico: **Confidencialidade**
  - Também pode garantir: Integridade, autenticidade e Controle de acesso.
- *Criptoanálise*
  - Estudo de meios p/quebrar códigos de criptografia
  - Toda cifra pode ser quebrada de alguma forma

Criptografia

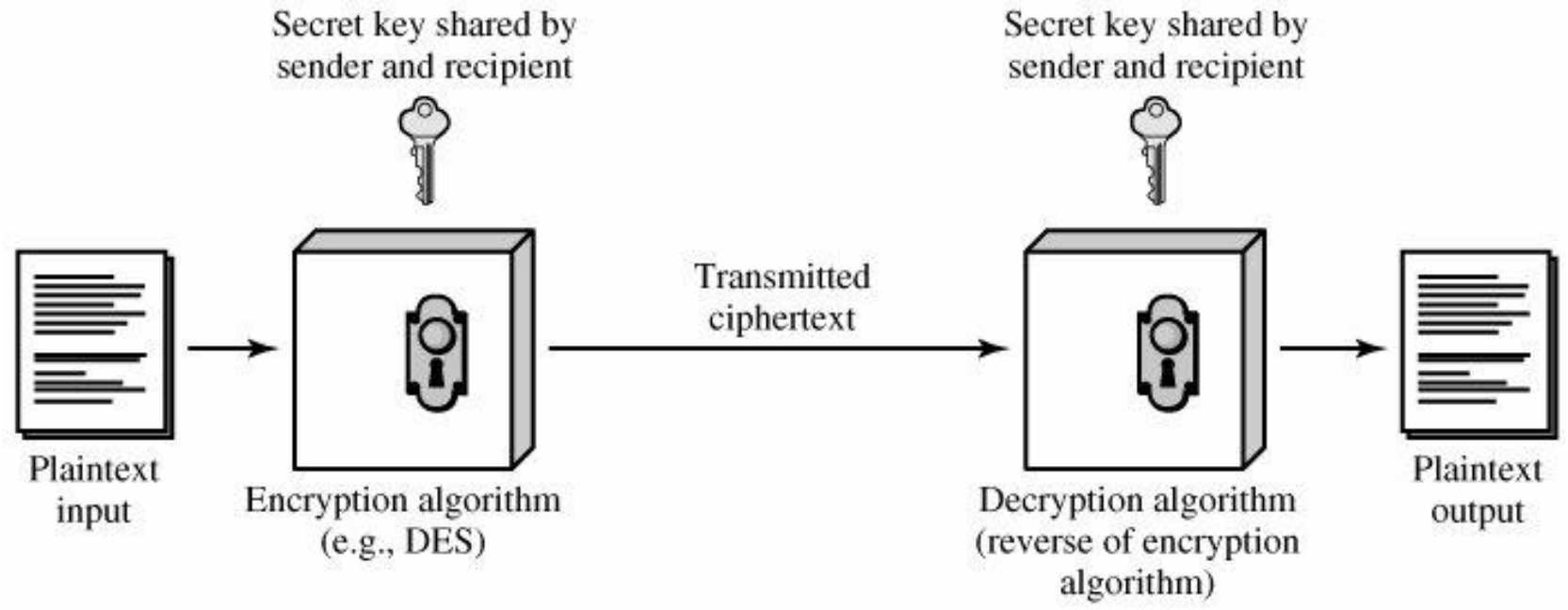
- **Cripto = oculto/escondido + Grafia = escrita**
  - Criptografia = arte de escrever oculto, em código

Criptografia

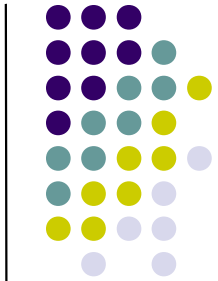


- **Elementos da criptografia**
  - ***Codificação*** (encriptação)
    - embaralhamento de um conteúdo de forma que fique ininteligível a quem não possui a “chave” para o restaurar.
  - ***Cripto-Algoritimo, Criptosistema ou Cifra***:
    - Método utilizado : substituição e transposição
  - ***Chave***:
    - elemento combinado ao algoritmo para permitir combinações/variações

Modelo Simplificado de Critografia Convencional

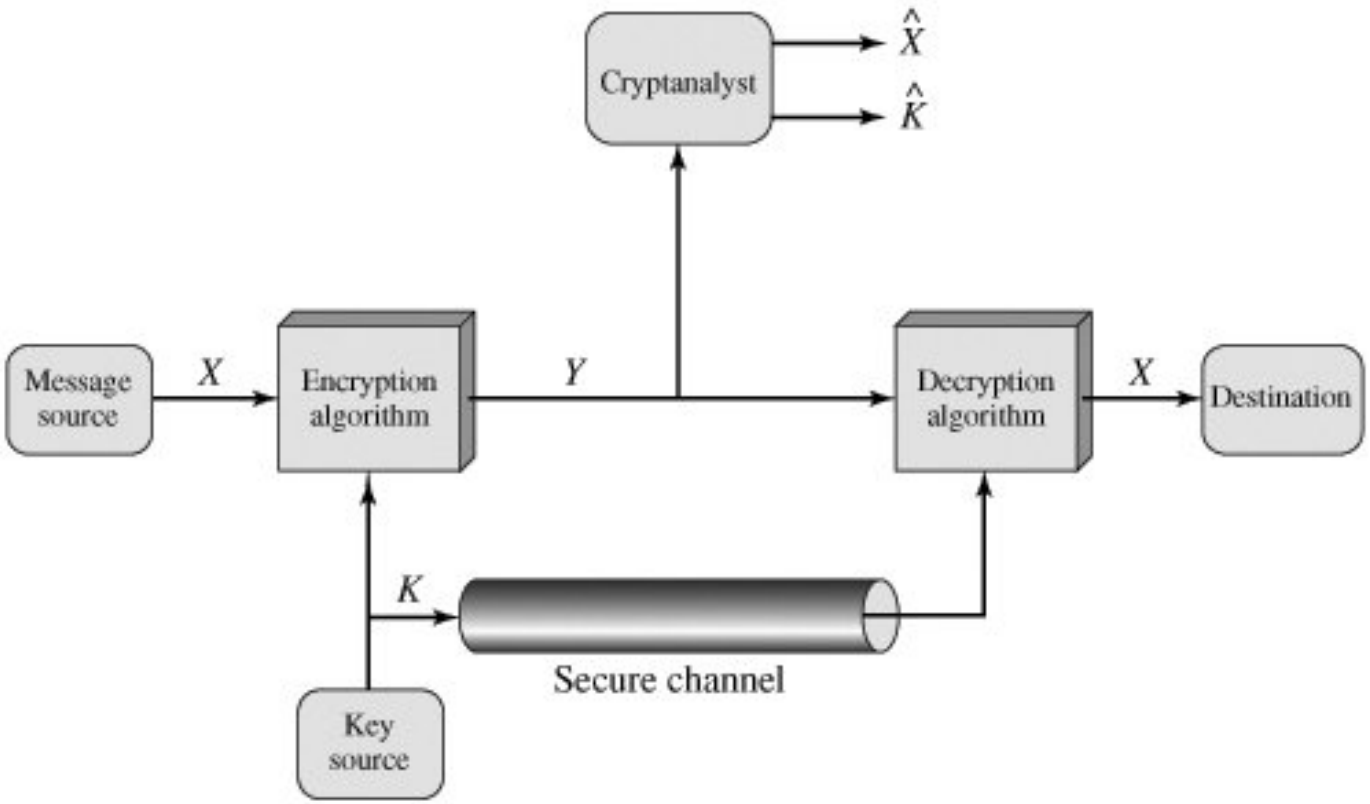


Criptoanálise



- Meios de criptoanálise
  - Força bruta: tentar todas as possibilidades
    - Algotritmo(A) e Texto cifrado (TC)
  - Mensagem conhecida:
    - A, TC e partes de texto puro/claro cifrados (TP)
  - Mensagem escolhida (conhecida e apropriada)
    - A,TC, e mensagem de texto claro cifrada escolhida pelo atacante.
  - Análise matemática e estatística
  - Engenharia social

Criptografia

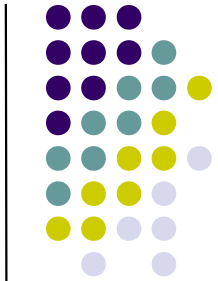


Criptografia

- Eficiência de ataques de força bruta

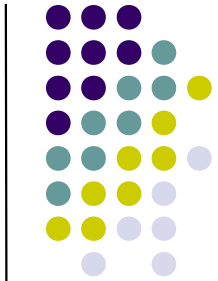
Key size (bits)	Number of alternative keys	Time required at 1 decryption/μs	Time required at 10^6 decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Criptografia



- Algoritmo computacionalmente seguro
  - ***Custo*** de quebrar excede o ***valor da informação***
  - O ***tempo*** para quebrar excede a ***vida útil*** da informação. (ou do atacante ☺)

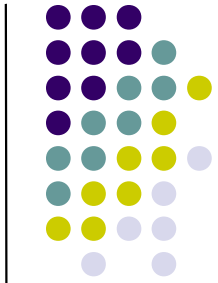
Criptografia



- **Conceitos para bom algoritmo de criptografia**
  - ***Confusão***
    - transformações na cifra de forma irregular e complexa.
  - **Difusão**
    - pequena mudança na mensagem, grande na cifra

Criptografia

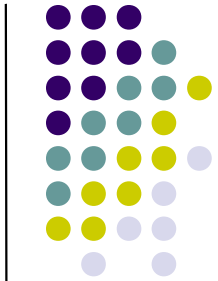
Métodos de Substituição



- **Cifra de César:**
- Consiste em substituir as letras do texto claro por outras letras através de um deslocamento de ***n*** elementos.
- **Nesse caso n=3 posições:**
  - *Claro: a b c d e f g h … z*
  - *Cifra: d e f g h i j k … c*
- **Vulnerabilidade:** *25 chaves a serem testadas, fácil criptoanálise.*

Criptografia

Métodos de Substituição

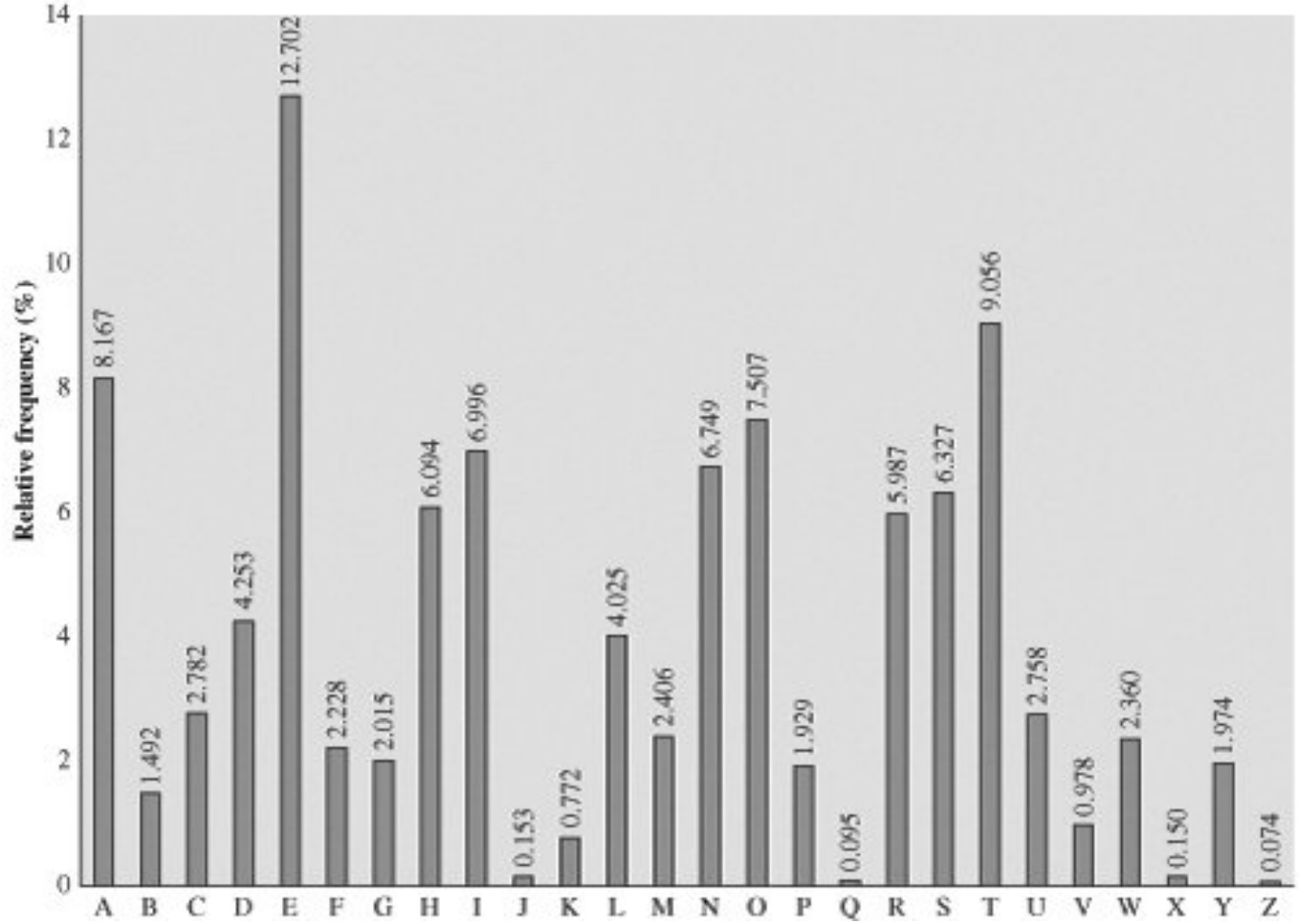


- **Cifras monoalfabéticas**
  - Permutação de caracteres para gerar a chave de substituição: 4 x 10E26 possibilidades de chaves diferentes.
  - Vulnerabilidade: frequência relativa de letras.

Criptografia

Métodos de Substituição

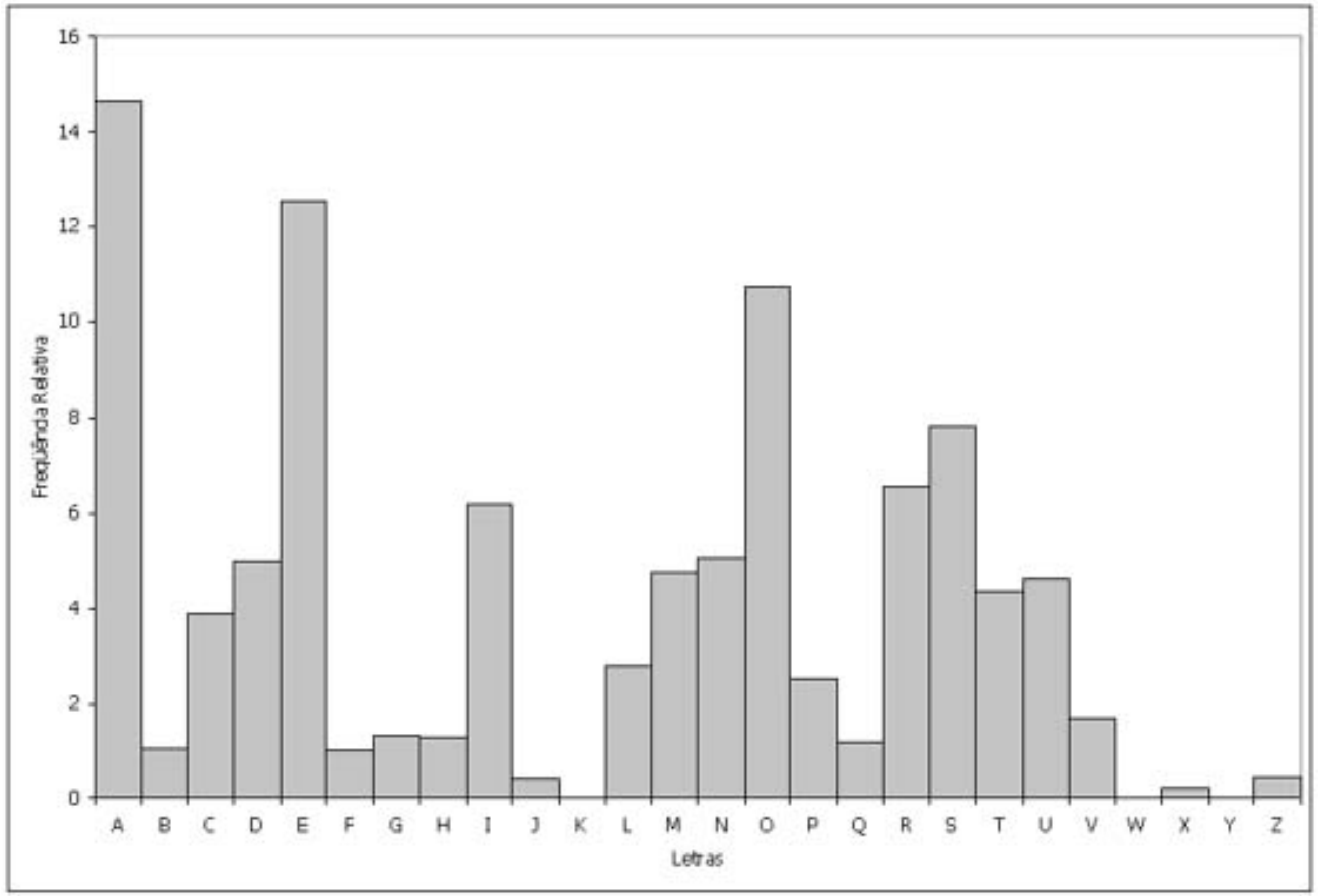
- Frequência relativa do uso de letras (Inglês)



Criptografia

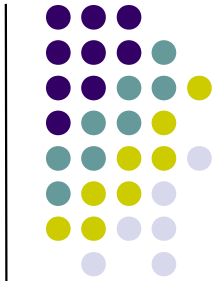
Métodos de Substituição

- Frequência relativa do uso de letras (Português)



Criptografia

Métodos de Substituição

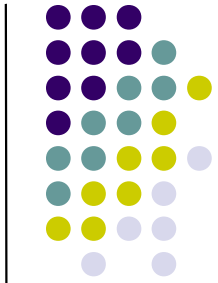


- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

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

Método de Substituição



- **Substituindo as letras mais frequentes:**

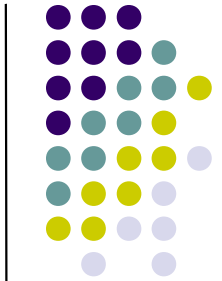
```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a          e  e te  a that e e a         a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee   a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

- **Texto original :**

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

Criptografia

Métodos de Substituição

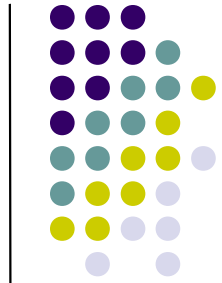


- **Cifras polialfabéticas**
- Usa um conjunto de regras de substituição monoalfabéticas.

- **Cifra de Vigenère:**
  - 26 cifras de César com deslocamentos de 0 – 25 . Cada cifra é indicada por uma letra-chave (da chave) que substitui a letra do texto claro: vide tabela.

Criptografia

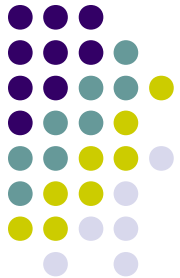
Tabela de Vigenère



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

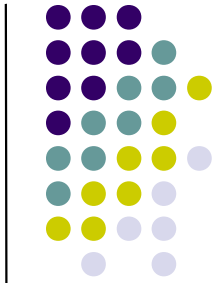
Método de Substituição



- **Cifrando com palavra-chave** : ***deceptive***
- key: d e c e p t l v e d e c e p t l v e
- plaintext: w e a r e d l s c o v e r e d s a v
- C-text: Z l CVTWQNG R ZGVT WA V Z
- **Sistema de Auto-chave** :
- key: d e c e p t l v e w e a r e d l s c o v
- Plaintext w e a r e d i s c o v e r e d s a v e y
- C-text: Z l C VTWQNGK ZE I l G AS XS T

Criptografia

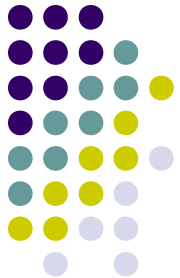
Método de Substituição



- One-Time Pad
  - Cifra que utiliza chaves tão grandes quanto o texto claro, porém com geração aleatória de chaves.
  - Vantagem: impossível quebrar
  - Desvantagem: dificuldade de gerar chaves puramente aleatórias e também sua distribuição.

Criptografia

Métodos de Transposição

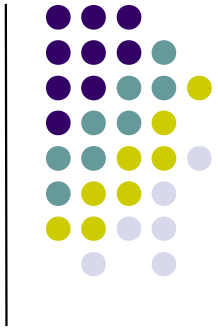


- **Mapeamento de texto claro é obtido através de uma permutação de posições.**
- ***Rail Fence*:**
  - **Texto é escrito em uma sequência de diagonais e lido em uma sequência de linhas.**
  - **Ex:**
  - **m e m a t r h t g p r y**
  - **e t e f e t e o a a t**

meet me after the toga party

Criptografia

Métodos de Transposição



- **Rail Fence é trivial**
- **Permutação de colunas:**

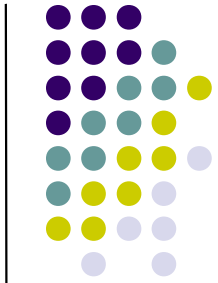
attack postponed
until two am xyz

```
Key:            4 3 1 2 5 6 7
Plaintext:      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
Ciphertext:     TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- **Mesmo assim a transposição pode ser facilmente reconhecida por análise de frequência.**

Criptografia

Métodos de Transposição



- **Transposição múltipla (n-vezes: mesma chave):**
- **Disposição inicial :**

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

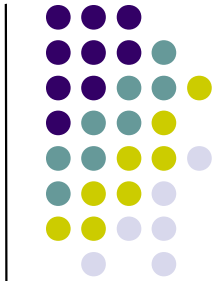
- **Primeira permutação**

```
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

- **Segunda Permutação**

```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

Exercício



- **Prática 2:**

1) Desenvolva um programa em java/C/C++ que implemente a criptografia de um texto através das cifra de Cesar.

2) Desenvolva um programa em java/C/C++ que implemente a criptografia de um texto através das cifra de Vigenère.