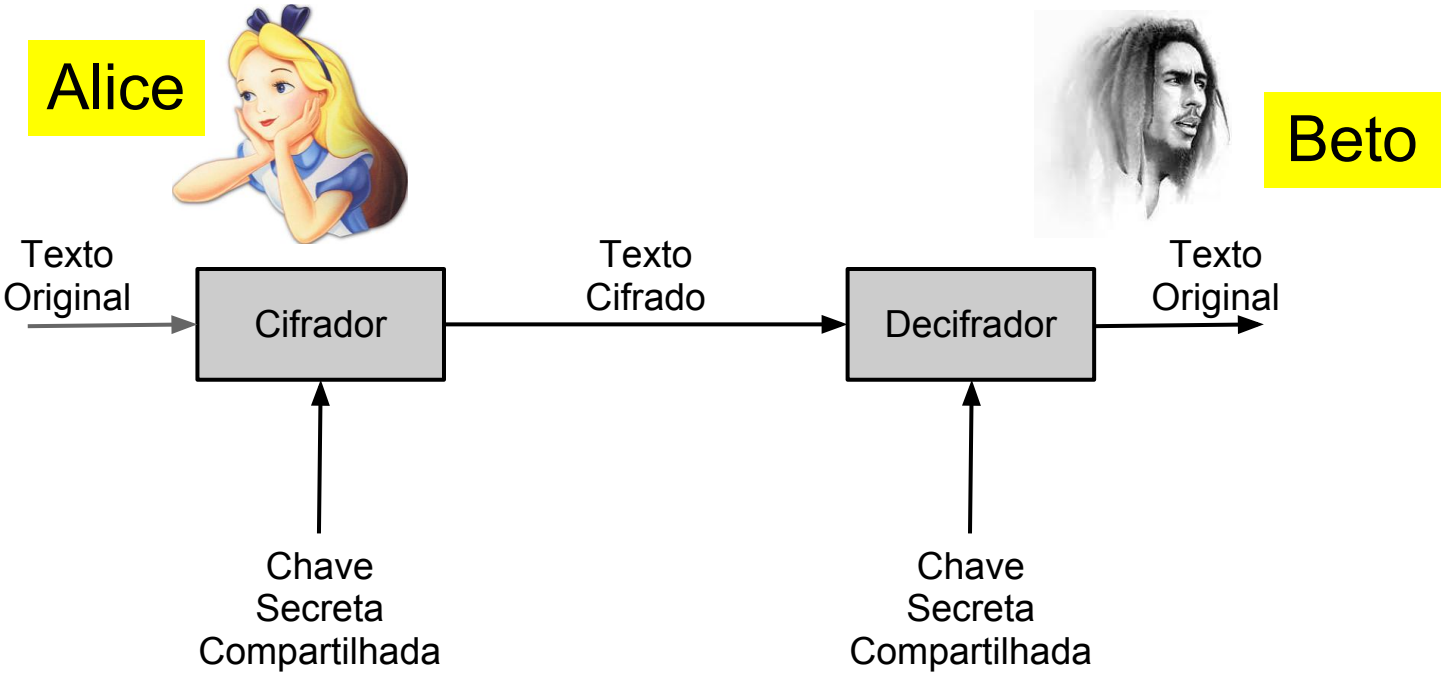
INE 5429
Criptografia Convencional

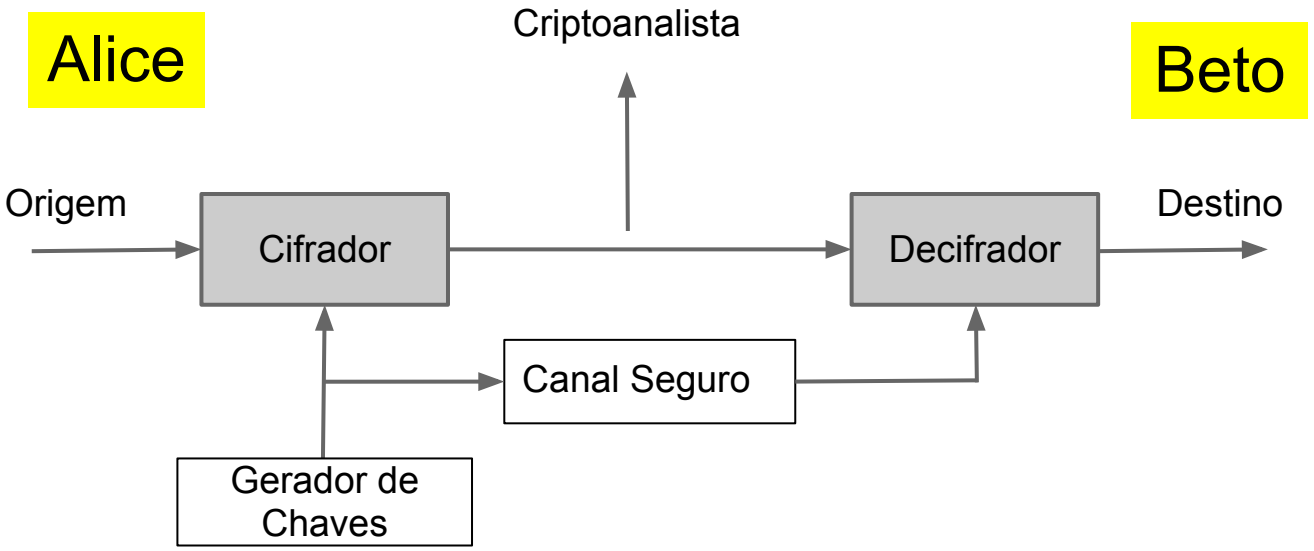
Técnicas Clássicas

Prof. Ricardo Felipe Custódio
custodio@inf.ufsc.br

Criptografia Convencional



Criptografia Convencional



Tipos de Ataques

- Somente Texto Cifrado
  - Cifra, Texto Cifrado
- Texto Original Conhecido
  - Cifra, Texto Cifrado, Um ou mais pares de Texto Original-Cifrado
- Texto Original Escolhido
  - Cifra, Texto Cifrado, Escolha do Texto Original
- Texto Cifrado Escolhido
  - Cifra, Texto Cifrado, Escolha do Texto Cifrado
- Texto Escolhido
  - Cifra, Texto Cifrado, Escolha Texto Original e Cifrado

Tempo Médio de Busca Exaustiva

Tamanho da Chave	Número de Chaves	Tempo Requerido [1 cripto/μs]	Tempo Requerido [10^6 cripto/μs]
32 bits	$2^{32} = 4{,}3 \times 10^9$	35,8 minutos	2,15 ms
56 bits	$2^{56} = 7{,}2 \times 10^{16}$	1.142 anos	25 horas
128 bits	$2^{128} = 3{,}4 \times 10^{38}$	$5{,}4 \times 10^{24}$ anos	$5{,}4 \times 10^{18}$ anos
256 bits	$2^{256} = 1{,}16 \times 10^{71}$	$1{,}8 \times 10^{63}$ anos	$1{,}8 \times 10^{57}$ anos
Permutação de 26 caracteres	$26! = 4 \times 10^{26}$	$6{,}4 \times 10^{12}$ anos	$6{,}4 \times 10^{6}$ anos

Exemplo de Texto em Português Cifrado

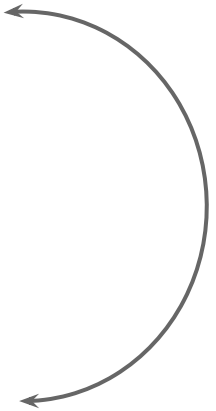
YDPRVHVWXGDUVHJXUDQFD

O que está escrito?

Cifrador de César

Texto Original → vamos estudar segurança

Texto Cifrado → YDPRV HVWXGDU VHJXUDQFD



```
abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Cifrar

C=E(p)=(p+3) mod 26

C=E(p)=(p+k) mod 26

Decifrar

C=D(p)=(p-3) mod 26

C=D(p)=(p-k) mod 26

Cifradores Monoalfabéticos

- Qualquer permutação de 26 caracteres alfanuméricos
- $26! = 4x10^{26}$ possíveis chaves

ZS UIVWE DE XSRKU
IG SEDIMSRSW MU YGVSU
RGVGIMU RUESMG WIVFW UP
MWVFSVUP.

BDGIMU GRKGZG GANDEG RUSPG,
IGU WCGESIGZG IWE RKWSFGZG:
WINUASG RUE ZUFGRSMGMW.

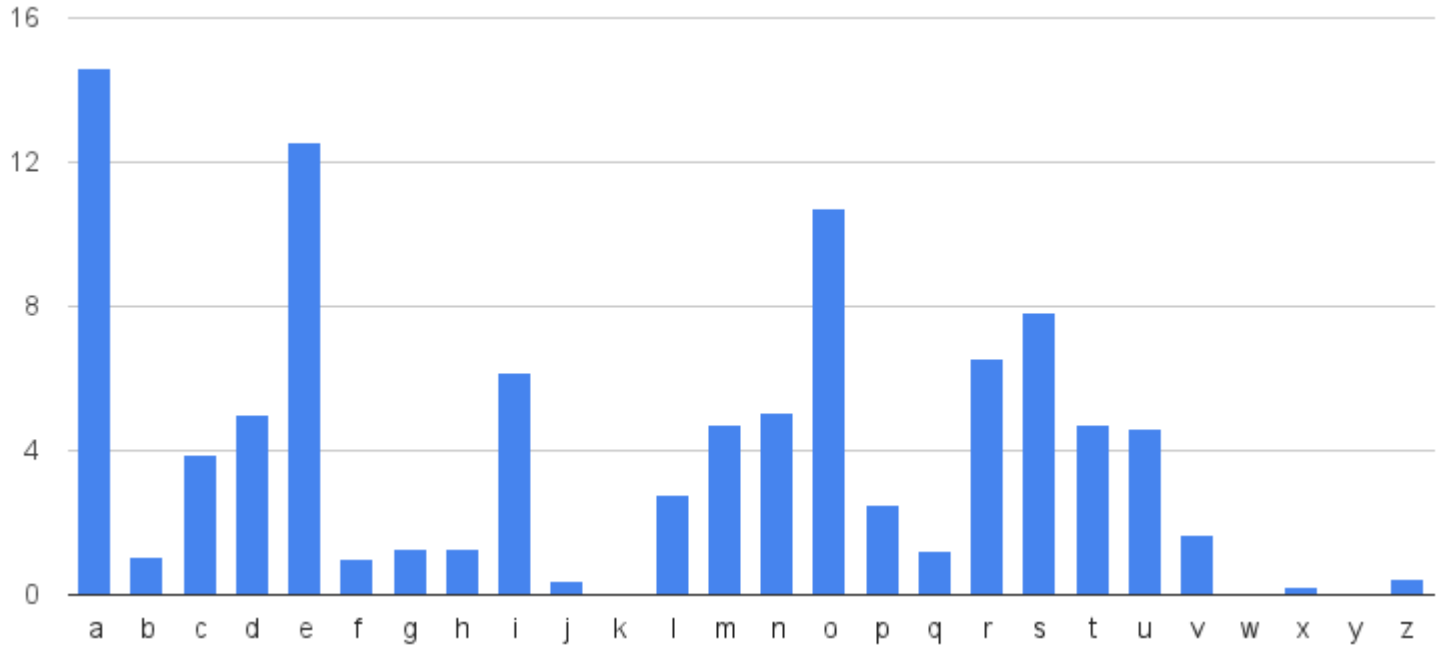
U XSRKU IGU WFG DE RGU,
IGU WFG DE NGVU,
IGU WFG DE FGVU.

U XSRKU, EWD MWDP, WFG DE
KUEWE.

G	16,32	R	6,32	K	3,16	A	1,05	Q	0,00
U	13,16	D	5,26	Z	2,63	C	0,53	T	0,00
W	8,95	F	4,74	P	2,11	B	0,53	O	0,00
E	7,89	M	4,74	N	1,58	Y	0,53	L	0,00
S	7,89	V	4,21	X	1,58	H	0,00	J	0,00
I	6,84								

Frequência das Letras em Português

	%
a	14,63
b	1,04
c	3,88
d	4,99
e	12,57
f	1,02
g	1,3
h	1,28
i	6,18
j	0,4
k	0,02
l	2,78
m	4,74
n	5,05
o	10,73
p	2,52
q	1,2
r	6,53
s	7,81
t	4,74
u	4,63
v	1,67
w	0,01
x	0,21
y	0,01
z	0,47



Exercício

Desenvolver um programa e analisar textos em português para obter

- frequência de letras
- frequência de duplas
- frequência de triplas

Cifrador Playfair

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

- A senha não pode ter letra repetida
- Letras repetidas usa-se um caractere preenchedor
- Se falar uma letra, use um caracter preenchedor
- Letras na mesma linha trocadas pela seguinte
- Letras na mesma coluna trocadas pela seguinte
- Para o restante, usa-se a coluna do outro

Exemplo

de pa rt am en to de in fo rm át ic ax

HA QL TU BK SO UN HA KO HM XR SQ PI BW