Aula 2

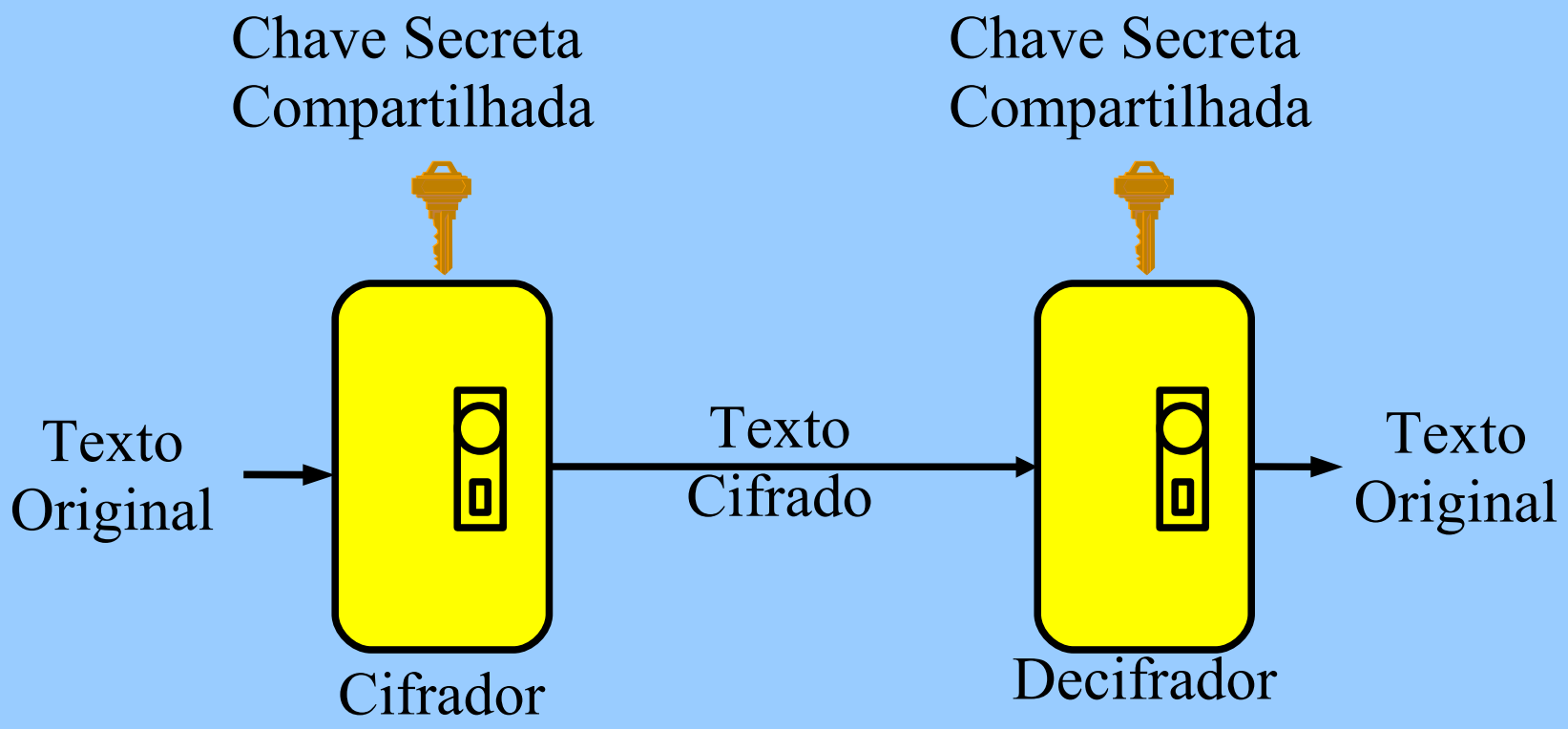
Criptografia Convencional

Técnicas Clássicas

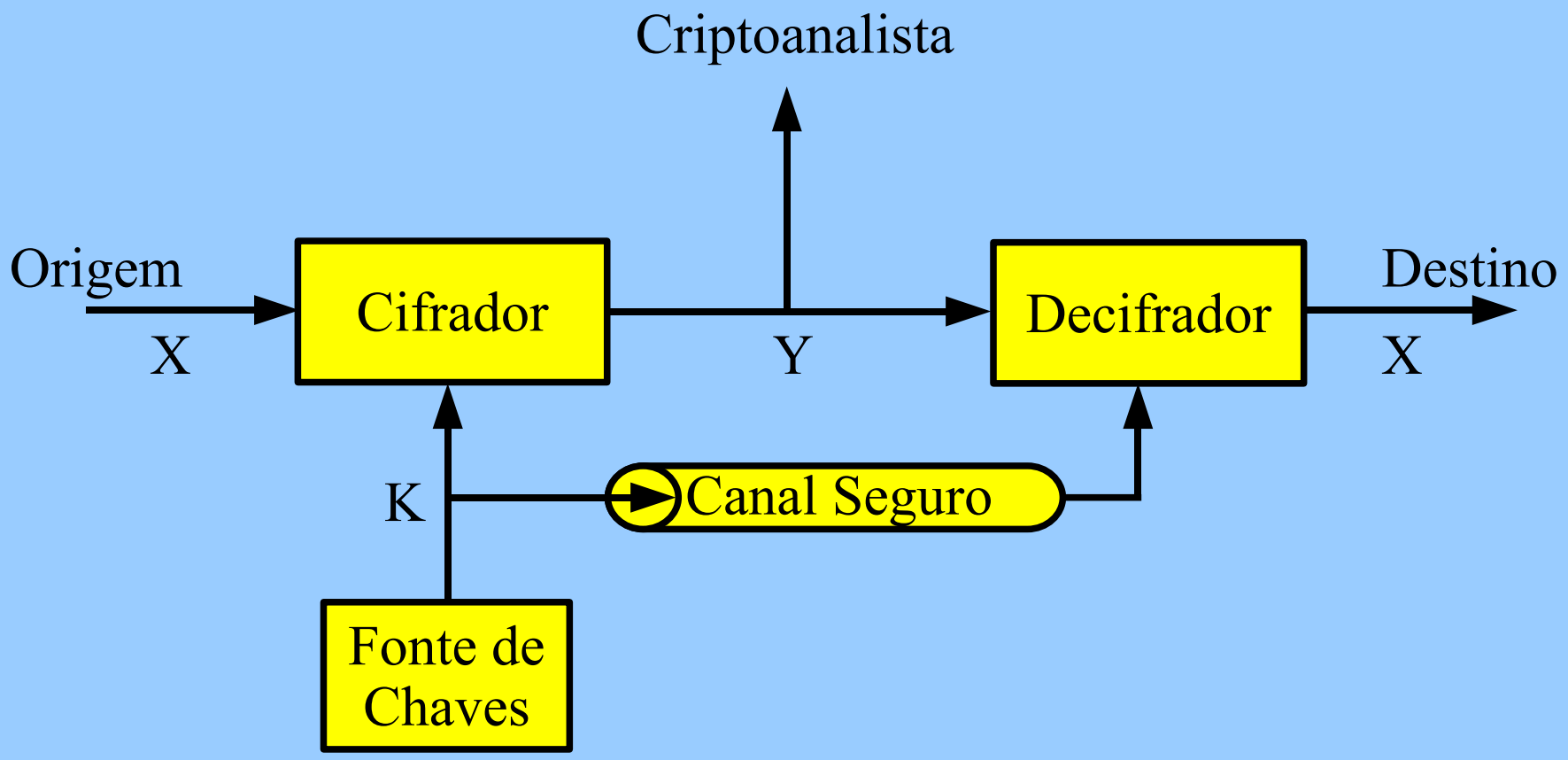
Plano de Aula

- Técnicas Clássicas
  - Cifrador de César
  - Cifradores Monoalfabéticos
  - Cifrador Playfair
  - Cifrador de Hill
  - Cifradores Polialfabéticos
- Técnicas de Transposição
- Máquinas Rotoras

Criptografia Convencional



Criptosistema Convencional



Tipos de Ataque

- 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	$2^{32}=4,3x10^9$	35,8 minutos	2,15 ms
56	$2^{56}=7,2x10^{16}$	1.142 anos	10,01 horas
128	$2^{128}=3,4x10^{38}$	$5,4x10^{24}$ anos	$5,4x10^{18}$ anos
26 caracteres permutação	$26!=4x10^{26}$	$6,4x10^{12}$ anos	$6,4x10^6$ anos

Exemplo de Texto Cifrado

(texto em portugüês)

WDPRVHVXYGDUVHJYUDQFD

Tente descobrir o que está escrito!

Técnicas Clássicas
Cifrador de César

```
original:    vamos estudar seguranca
cifrado:     WDPRV HVXYGDU VHJYUDQFD

original:    abcdefghijklmnopqrstuvwxyz
cifrado:     DEFGHIJKLMNOPQRSTUVWXYZABC
```

Cifrar

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

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

Decifrar

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

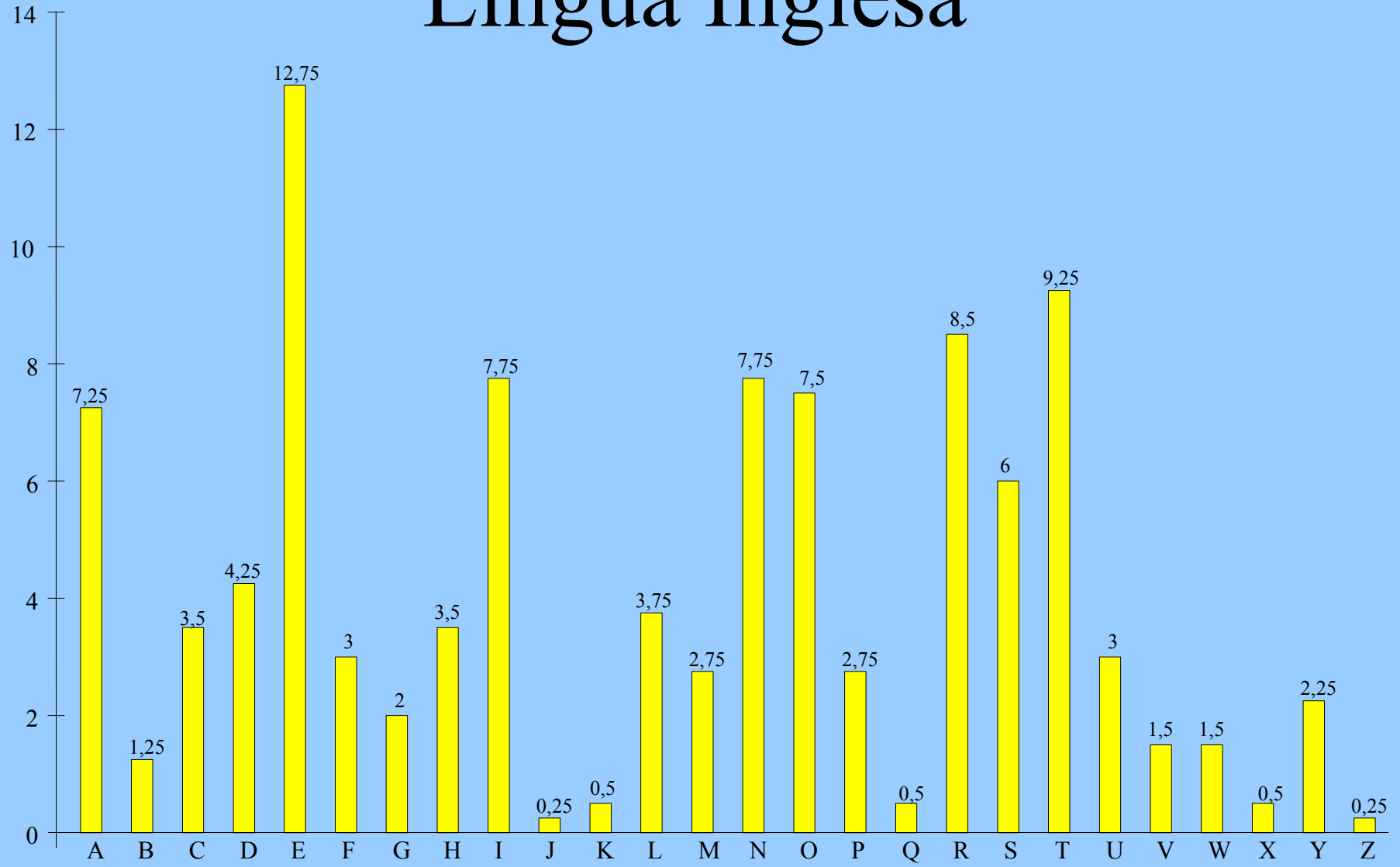
Cifradores Monoalfabéticos

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

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHDMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
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				

Freqüência Relativa das Letras na Língua Inglesa

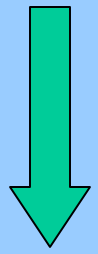


Criptoanálise

- ***P*** e ***Z*** são equivalentes a ***e*** e ***t***
- ***S, U, O, M*** e ***H*** -> {***r,n,i,o,a,s***}
- ***A, B, G, Y, I*** e ***J*** -> {***w,v,b,k,x,q,j,z***}
- Digramas, Trigramas
  - ***th*** é o mais comum -> ***ZW***
  - ***P -> e*** (***ZWP -> the***)
- ***ZWSZ -> th_t*** ***S->a*** ***That***

Criptoanálise

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHDMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ



Criptoanálise

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

Trabalho

Desenvolver um programa e analisar textos em português para obter:

a) as letras do alfabeto mais comuns;

b) as duas letras mais comuns;

c) as três letras mais comuns.