

HISTORY ABOUT CRYPTOGRAPHY

EXEMPLOS HISTÓRICOS:

1- Cifra de substituição MONOALFABÉTICA

$K :=$

a	→	c
b	→	w
:		:

ex) Cifra de César (sem chave)

n deslocamentos

a	→	d
b	→	e
:		:

$a+n$
 $b+n$

→ não é bem uma cifra

Como quebrar essa cifra?

- Frequência de letras → No inglês, a letra + frequente: E

No português, a letra + frequente: A

seguir essa ideia →
por segundo, terceiro, ...;
letra.

a letra que mais aparecer provavelmente é o E ou A cifrados.

- Frequência de pares de letras: no inglês → IS
HE
THE

POLIALFABÉTICA

ex) Vigenere

$K = \text{CRYPTO}$ \rightarrow repete a chave até
 $+ \text{mod } 26$

$M = \text{WHAT AN NICE}$

$C = \text{ZZZJUC LUDT}$

ex) Máquinas

enigma

