History About CRYTOGRAPHY

EXEMPLOS HISTÓRICOS:

1- Cifra de substituição

MONOALFABÉTICA

K := a → c
b → w
⋮

ex) Cifra de César (sem chave) → não é bem uma cifra

n deslocamentos

a → d → a+n
b → e → b+n
⋮

Como quebrar essa cifra?

- Frequência de letras → No inglês, a letra + frequente: E
  No português, a letra + frequente: A
  a letra que mais aparecer provavelmente é o E ou A cifrado.
  ↳ seguir essa ideia para segunda, terceira, ...; letra.
- Frequência de pares de letras: no inglês → IS, HE, THE

POLIALFABETICA

ex) Vigenere

K = CRYPTO → replica a chave até CRYP

+mod 26

m = WHAT AN NICE

c = ZZZJVCLVDT

ex) Máquinas

enigma