



Breaking substitution ciphers

Exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Doable with a computer

Statistical analysis

Match letters together

Choose ABCDE ... and match letters

Choose ABCDE ... and match letters

# Breaking substitution ciphers

Exhaustive search	Doable with a computer
ciphertext only	Statistical analysis
known plaintext	Match letters together
chosen plaintext	Choose ABCDE ... and match letters
chosen ciphertext	Choose ABCDE ... and match letters

# Polyalphabetic ciphers (a.k.a Renaissance Cipher)

➔ Vigenere cipher

**Algorithm :** combine the message and the key

**Key :** a word

**Key space :** the length of the word

$$\begin{array}{r} \text{wearediscoveredsaveyourself} \\ + \text{deceptivedeceptivedeceptive} \quad (\text{mod } 26) \\ \hline \text{ZICVTWQNGRZGVTWAVZHCQYGLMGJ} \end{array}$$

**Advantage :** Encryption of a letter is context dependent