



Breaking Polyalphabetic Ciphers

exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

exhaustive search

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Small key length only

Statistical analysis for small key length and significant amount of ciphertext

Subtract plaintext from ciphertext

Choose AAAAAA ... and match letters

Choose AAAAAA ... and match letters

# Breaking Polyalphabetic Ciphers

exhaustive search	Small key length only
ciphertext only	Statistical analysis for small key length and significant amount of ciphertext
known plaintext	Subtract plaintext from ciphertext
chosen plaintext	Choose AAAAAA ... and match letters
chosen ciphertext	Choose AAAAAA ... and match letters

# OTP - One Time Pad

➔ Improvement over Vigenere cipher

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

**Key :** an infinite random string

**Key space :** infinite

$$\begin{array}{r} \text{whatanicedaytoday} \\ \oplus \text{yksuftgoarfwfwel} \\ \hline \text{ZZZJUCLUDTUNNWGQS} \end{array}$$

**Advantage :** **this is the perfect cipher !**

**Disadvantage :** hard to use in practice, how to transmit the key ?