OTP - One Time Pad

➡ Improvement over Vigenere cipher

Algorithm : combine the message and the key

Key : an infinite random string

Key space : infinite

```
  whatanicedaytoday
⊕ yksuftgoarfwpfwel
------------------
  ZZZJUCLUDTUNNWGQS
```

Advantage : this is the perfect cipher !

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

The impossibility of breaking OTP

The ciphertext bears no statistical relationship to the plaintext

➡ No statistical analysis

For any plaintext and ciphertext, there exists a key mapping one to the other, and all keys are equally probable

➡ A ciphertext can be decrypted to any plaintext of the same length