# 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

# Transposition Cipher

**Algorithm :** switch letters around a permutation

**Key :** a set of permutation

**Key space :** the set of permutations

```
helloworld
LOLHERDLWO
```