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

The seeds of modern cryptography

1. **Diffusion**
   Mix-up symbols
   Transposition Cipher

2. **Confusion**
   Replace a symbol with another
   Polyaphabetic Cipher

3. **Randomization**
   Repeated encryption of the same text are different
   OTP