Breaking Transposition ciphers

brute force

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

brute force

ciphertext only

known plaintext

chosen plaintext

chosen ciphertext

Small key length only

Hard for large permutations

Match letters together

Choose ABCDE … and match letters

Choose ABCDE … and match letters

Breaking Transposition ciphers

brute force	Small key length only
ciphertext only	Hard for large permutations
known plaintext	Match letters together
chosen plaintext	Choose ABCDE … and match letters
chosen ciphertext	Choose ABCDE … and match letters

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