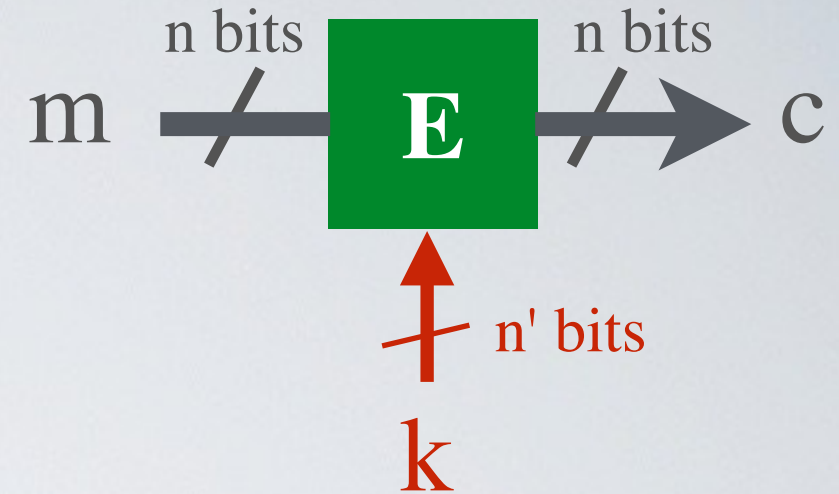


Block Cipher

Ideal block cipher



- Combines confusion (substitution) and diffusion (permutation)
 - Changing single bit in plaintext block or key results in changes to approximately half the ciphertext bits
- ➡ Completely obscure statistical properties of the original message
- ➡ A known-plaintext attack does not reveal the key