The Kerckhoffs' principle (1883)

"The enemy knows the system" - the security of a communication should not rely on the fact that the algorithms are secrets

➡ A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

No security by obscurity

Breaking the cipher - the attacker's model

- **Exhaustive Search** (a.k.a brute force)
  Try all possible n keys (in average it takes n/2 tries)

- **Ciphertext only**
  You know one or several random ciphertexts

- **Known plaintext**
  You know one or several pairs of random plaintext and their corresponding ciphertexts

- **Chosen plaintext**
  You know one or several pairs of chosen plaintext and their corresponding ciphertexts

- **Chosen ciphertext**
  You know one or several pairs of plaintext and their corresponding chosen ciphertexts

➡ **A good crypto system resists all attacks**