Design principles (reminder)

1. **Kerkoff Principle**
   The security of a cryptosystem must not rely on keeping the algorithm secret

2. **Diffusion**
   Mixing-up symbols

3. **Confusion**
   Replacing a symbol with another

4. **Randomization**
   Repeated encryptions of the same text are different

The attacker's model

- **Exhaustive Search**
  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**