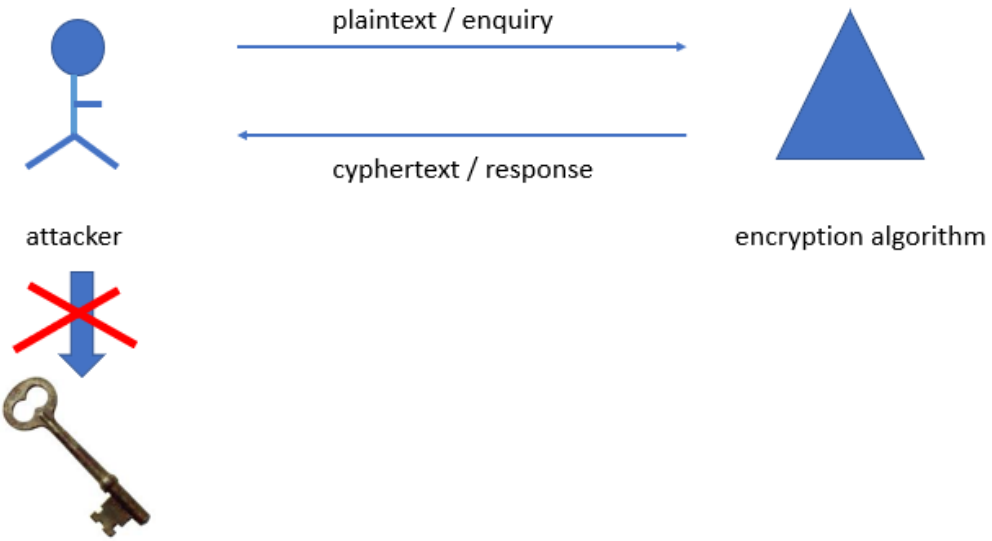
A strong encryption algorithm



Secure Encryption Scheme

- **Unconditional security:** no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **Computational security**
  - ➢ the cost of breaking the cipher exceeds the value of the encrypted information;
  - ➢ or the time required to break the cipher exceeds the useful lifetime of the information

Desired characteristics

- Cipher needs to completely obscure statistical properties of original message
- More practically Shannon suggested combining elements to obtain:
  - ➢ Confusion: changing a bit of the key affect the ciphertext
  - ➢ Diffusion: changing one bit of the plaintext affects the ciphertext?

Ways to achieve

- Symmetric Encryption:substitution / transposition / hybrid
- Asymmetric Encryption:
  - ➢ Mathematical hardness - problems that are efficient to compute in one direction, but inefficient to reverse by the attacker.
  - ➢ Examples: Modular arithmetic, factoring, discrete logarithm problem, Elliptic Logs over Elliptic Curves