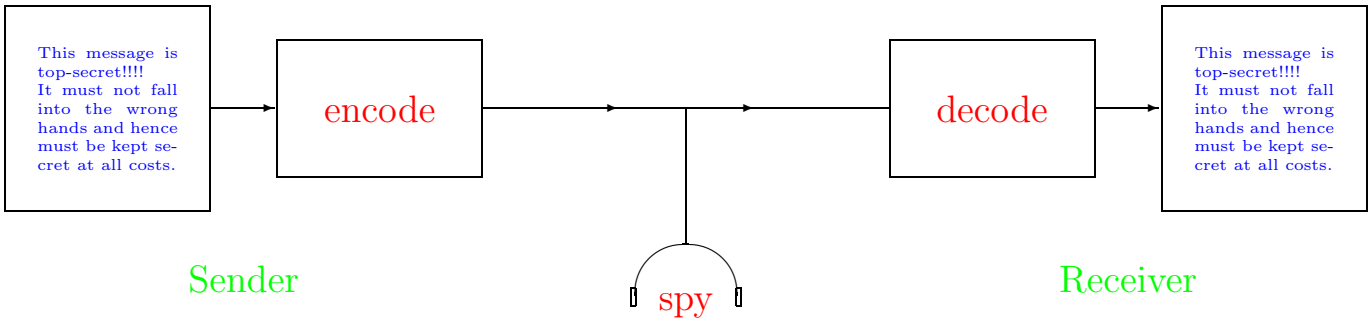
# Public Key Cryptography




## 1. Data Security – Aims/Attacks:

1. **Secrecy:** An unauthorized person (spy) should not be able to read/interpret the message. (Passive attack)
2. **Authentication:** An unauthorized person should not be able to secretly alter (or send) the message. (Active attack)

**Example:** The Dancing Men by A. C. Doyle (1903/04)

- A client shows Sherlock Holmes a set of pictures (a child's drawings?) which terrify the client's wife, Elsie.
- Holmes realizes that these are encrypted messages, and applies a frequency analysis to try to decode the messages. (E.g., 'e' is the most frequently used letter in the English language.)
- He needs only 5 messages to crack the code and to understand the messages (passive attack).
- He can then send a $6^{th}$ message, pretending to be Elsie, and thus traps the person sending the messages. (Active attack).

# 2. Basic Cryptographic Strategies

1. **Symmetric Cryptosystems:** The encoding and decoding procedure use (in essence) the same key.
   Advantage: Fast implementation.
   Disadvantage: Difficult to communicate the encoding procedure to the sender (without sacrificing security).

2. **Asymmetric (Public Key) Cryptosystems:** The encoding procedure is public, the decoding procedure is secret.
   Disadvantage: Presently1000x slower than symmetric systems.

3. **Cryptographic Hashfunctions:** A (quickly evaluable) function which attaches to each message a "fingerprint", i.e. a number of fixed length (128 or 256 bits).

   Idea: Different messages have different fingerprints.

**In practice:** Use a hybrid cryptosystem, i.e. a cryptosystem which combines all three strategies:

- Use a symmetric system for communicating text (but change the key frequently).
- Use a public key system to send the new key.
- Use a hashfunction and a public key to check authenticity of message and of sender. ($\longrightarrow$ Digital Signatures)