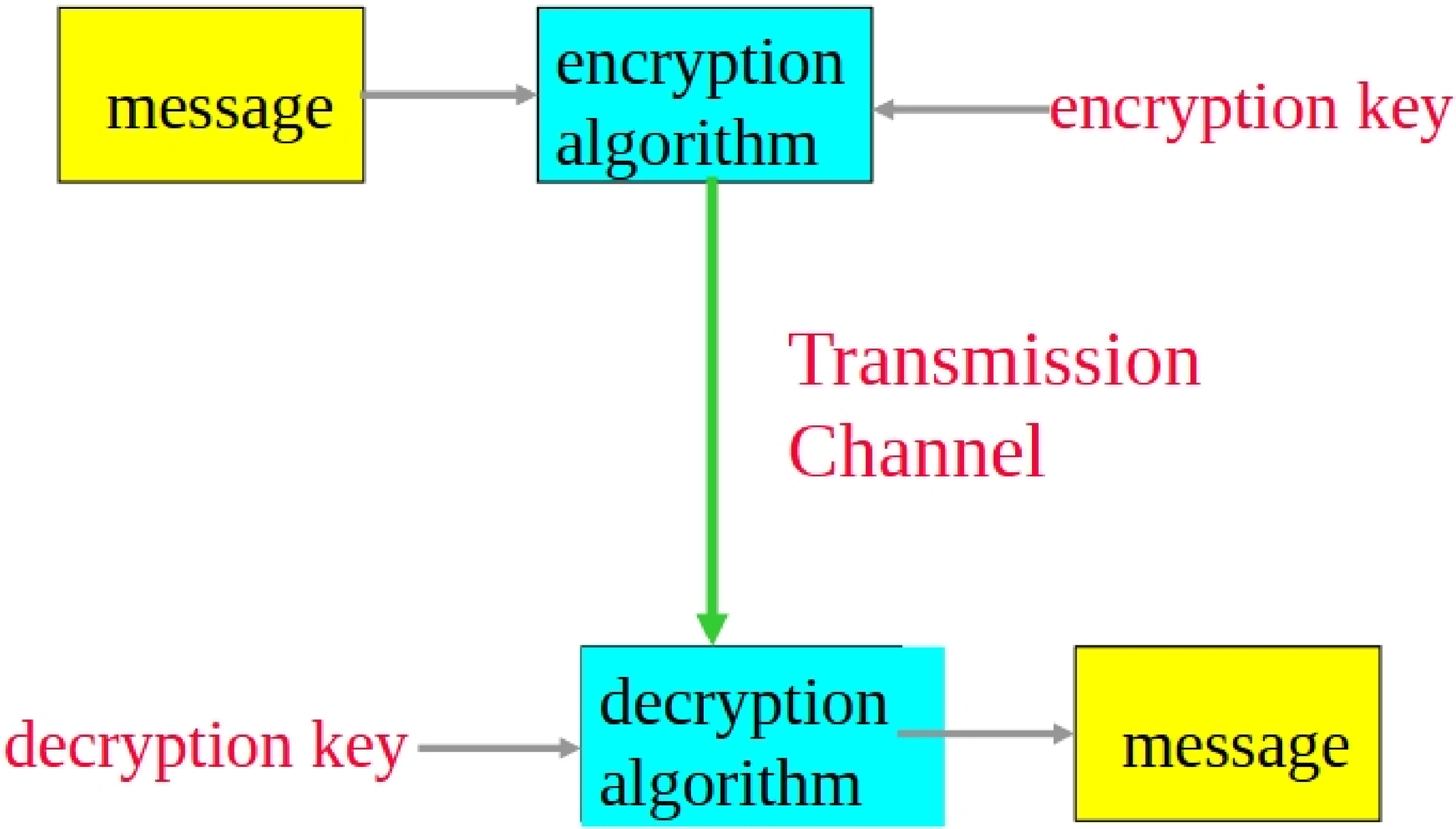
Hard Problems

- Some problems are hard to solve.
  - No polynomial time algorithm is known.
    - E.g., NP-hard problems such as machine scheduling, bin packing, 0/1 knapsack.
- Is this necessarily bad?
- Data encryption relies on difficult to solve problems.

Cryptography



Public Key Cryptosystem (RSA)

- A public encryption method that relies on a public encryption algorithm, a public decryption algorithm, and a public encryption key.
- Using the public key and encryption algorithm, everyone can encrypt a message.
- The decryption key is known only to authorized parties.
- Asymmetric method.
  - Encryption and decryption keys are different; one is not easily computed from the other.