Security and Applications

Grading

- Grading
  - Quiz/Assignments/Homeworks: 15%
  - Minors (closed book): 15% + 15%
  - Project work and report 20%
    - Select your own topic
    - 10 to 15 pages report
  - Final exam (closed book): 30%
  - Class participation: 5%
- Policy
  - Do it yourself
  - Innovative outlook

Attacks, Services and Mechanisms

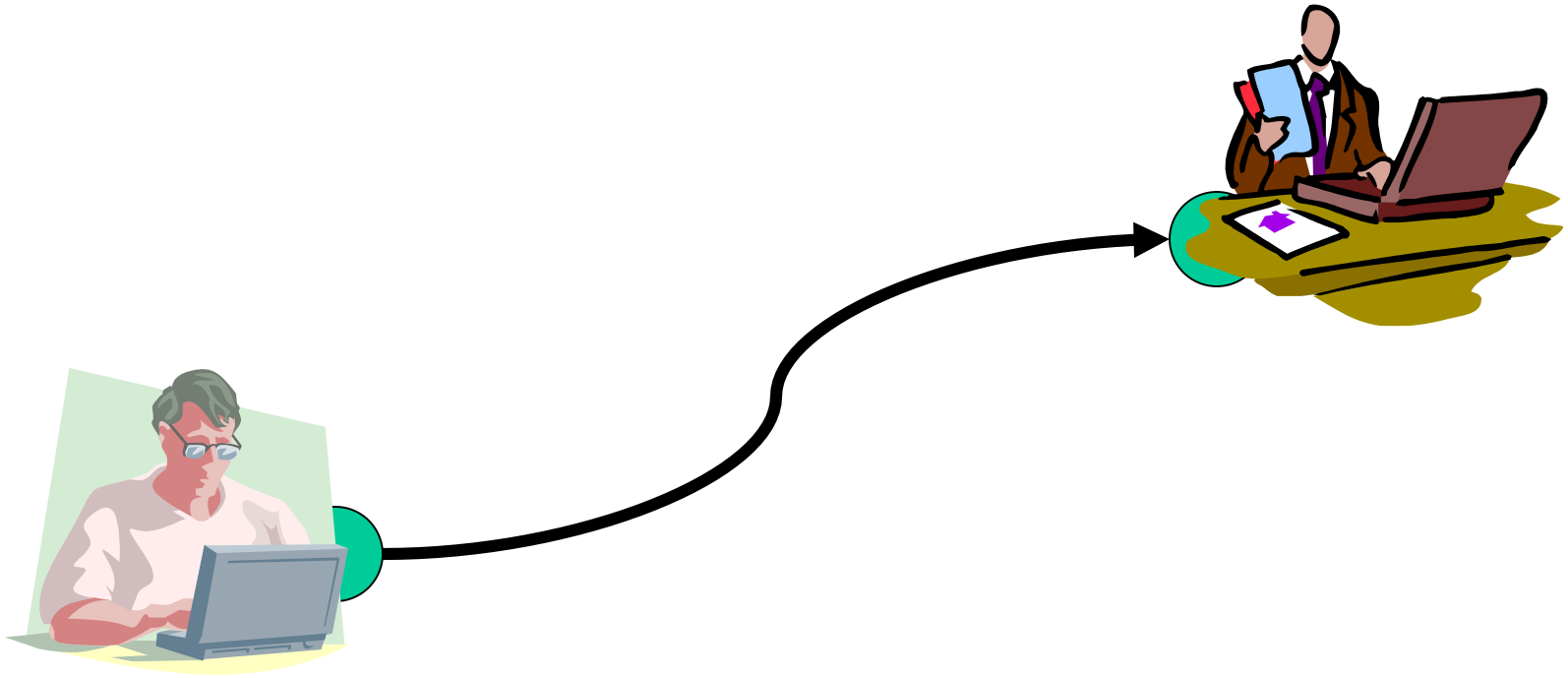
- Security Attacks
  - Action compromises the information security
- Security Services
  - Security of data processing and transferring
- Security mechanism
  - Detect, prevent and recover from a security attack

How security of systems can be compromised?

Attacks

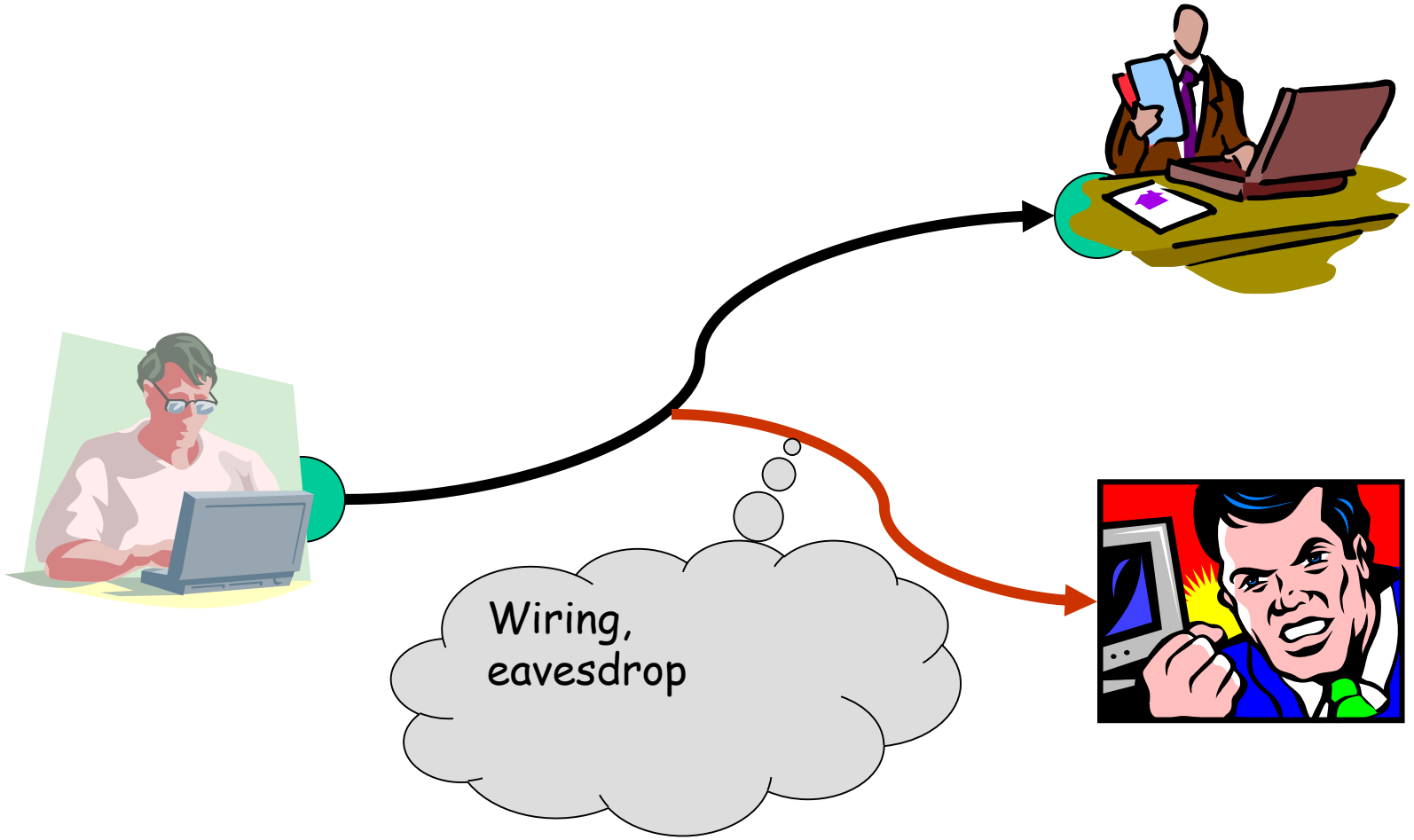
- Malware
- Cybersquatting
- Phishing
- Cyber vandalism
- Masquerading or spoofing
- Denial of Service

Information Transferring

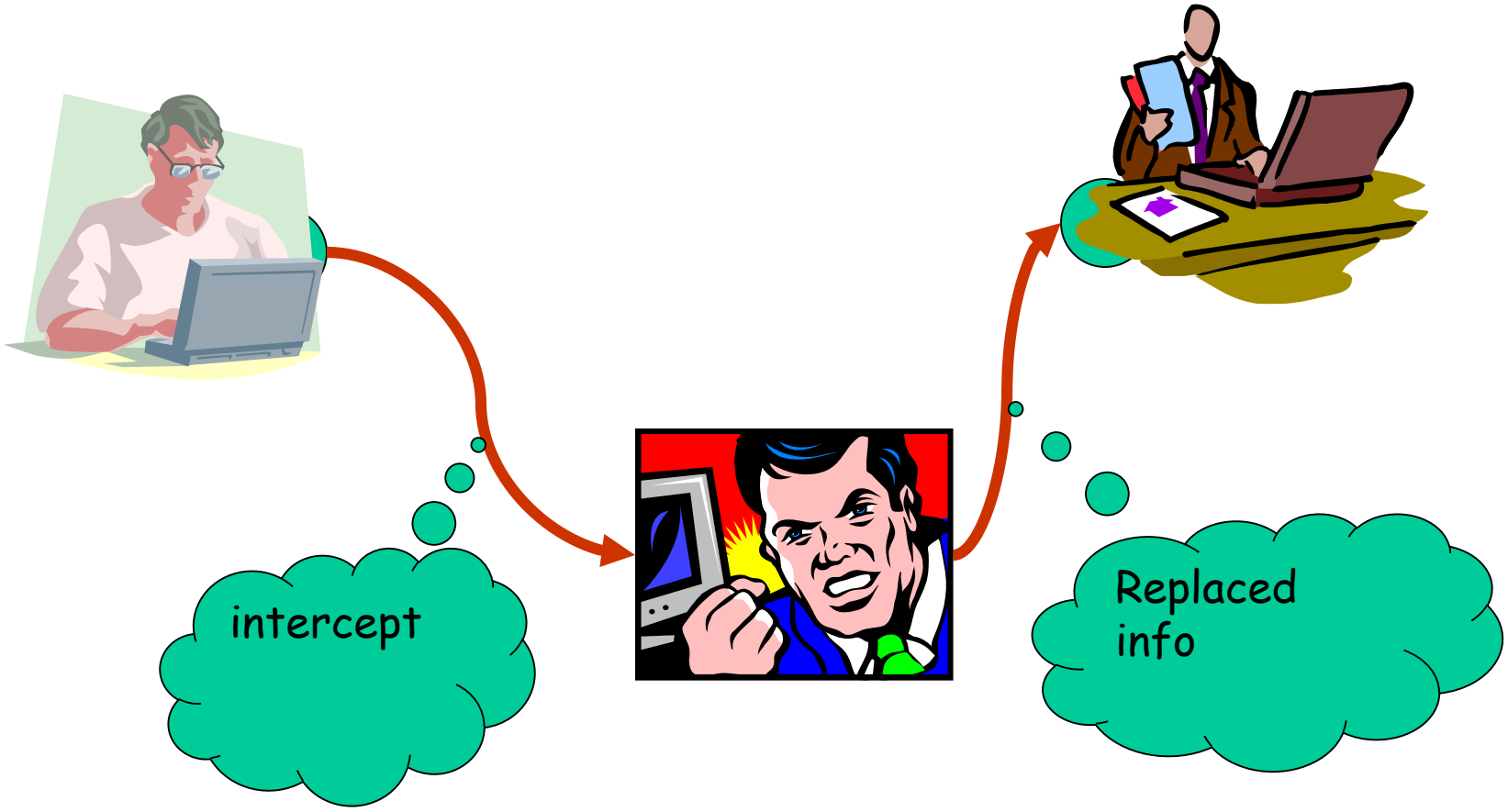


How an adversary can compromise communication

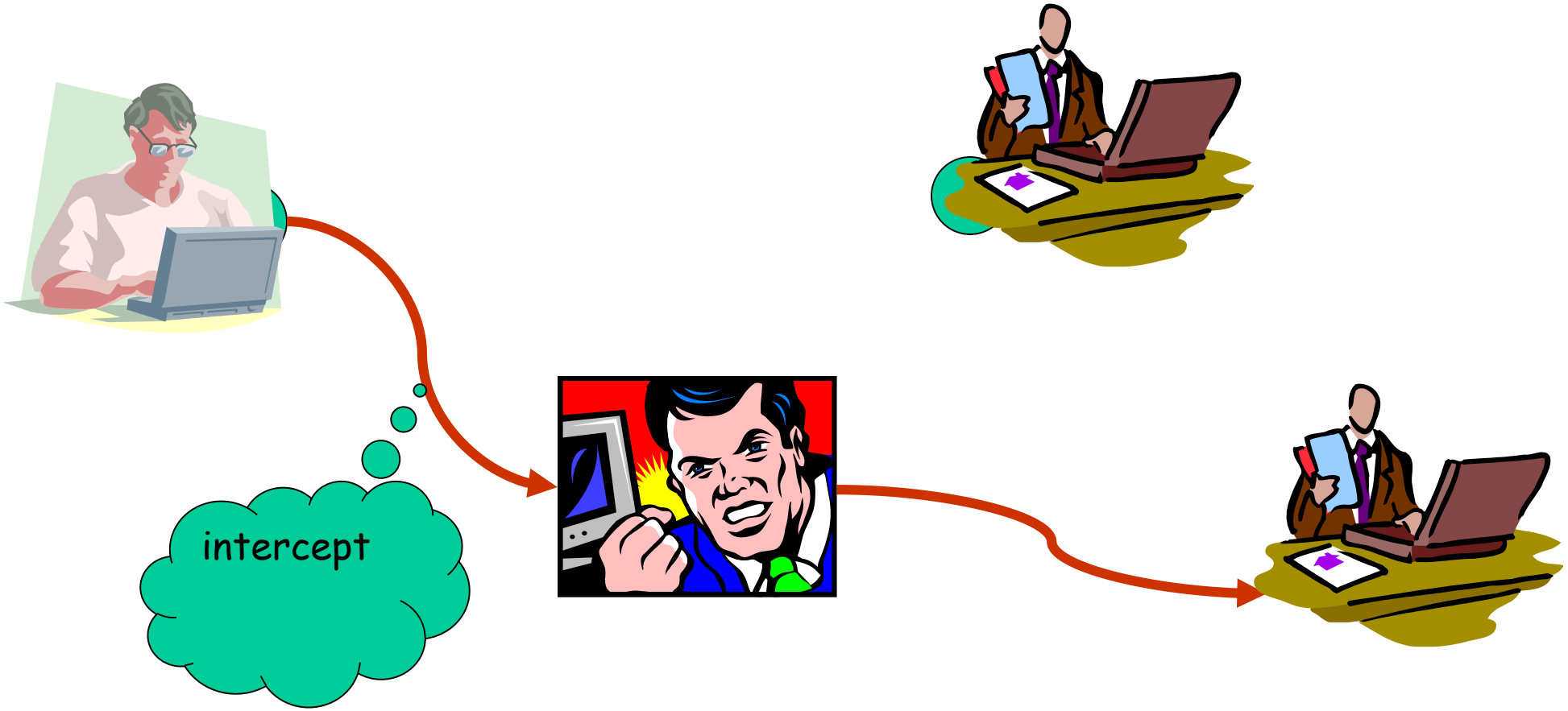
Attack: Interception



Attack: Modification



Attack: change of recipient

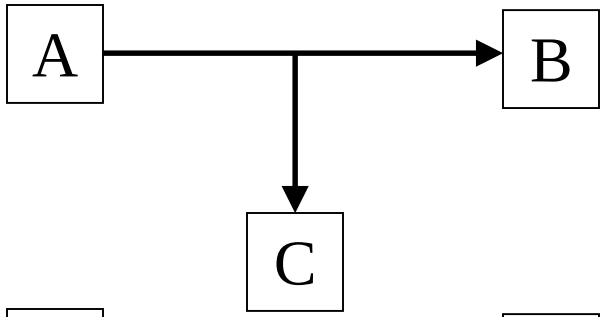


Attack: Fabrication

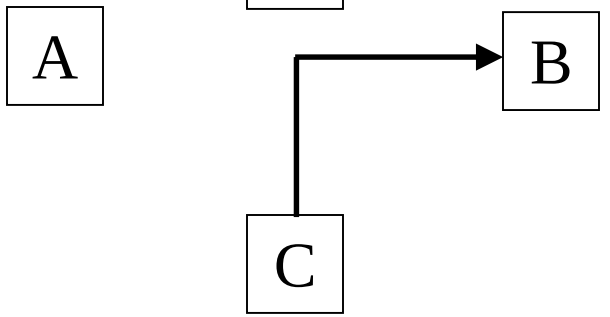
Also called impersonation

Information Transfer: Security Services

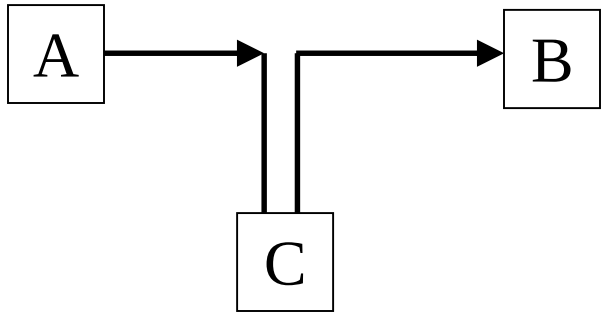
Confidentiality



Authenticity



Integrity



Secure Communication

1. Confidentiality (Secrecy)
   - Only intended receiver understands the message
2. Authentication
   - Sender and receiver need to confirm each others identity
3. Message Integrity
   - Ensure that their communication has not been altered, either maliciously or by accident during transmission
4. Non-repudiation:
   - the sender should not be able to deny sending the message.

Designing Service

1. Design an algorithm
2. Generate secret information
3. Develop methods for the distribution and sharing of secret information
4. Specify a protocol to be used

Attacks

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

Attack Surfaces

- System
  - Open ports
  - Firewall
  - Code processing email,XML,docs
  - Interfaces, SQL
  - Employee
- Software
  - Application
  - OS code
  - Webserver software
- Human
  - Personnel
  - Outsiders
  - Social Engineering
  - Human Error

Enabling Secure Communication

- Code
- Steganography
- Cryptography

Code	Meaning
Hat	boat
Has been sent	arrives
Friday	tomorrow

Steganography

- Conceal the existence of message
  - Character marking
  - Invisible ink
  - Typewriter correction ribbon

Steganography

- Least significant bits of picture frames
  - 2048x3072 pixels with 24-bits RGB info
  - Able to hide 2.3M message
- Drawbacks
  - Large overhead
  - Virtually useless if system is known

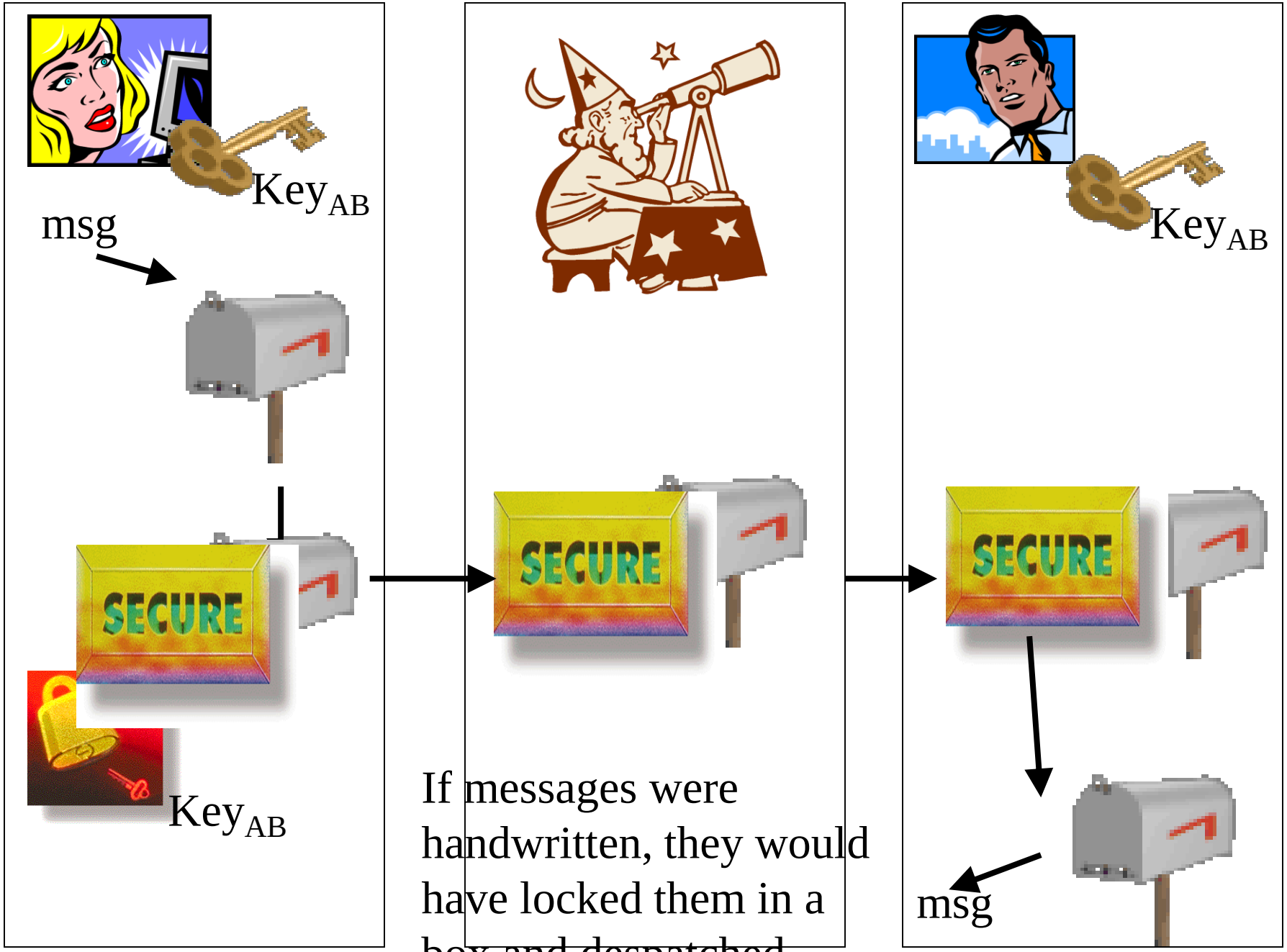
Cryptography

- **Cryptography** (from Greek *kryptós*, "hidden", and *gráphein*, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge — the art of *encryption*.
- **Secret (crypto-) writing (-graphy)**

msg

msg

Alice and Bob do not want anyone in the middle to know about their messages



If messages were handwritten, they would have locked them in a box and despatched

Cryptography Algorithms

- A crypto algorithm transforms an intelligible message into one that is unintelligible, and then retransforming that message back to its original form, so that:-
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  - Verify the correctness of a message to the recipient (**authentication**)

Crypto-graphy, -analysis, -logy

- The study of how to circumvent the use of cryptography is called *cryptanalysis*, or *codebreaking*.
- Cryptography and cryptanalysis are sometimes grouped together under the umbrella term **cryptology**, encompassing the entire subject.

Cryptanalysis: Strength of Encryption

Unconditionally secure

- If it is impossible determine uniquely P from C, no matter how much ciphertext is available.

Practically secure

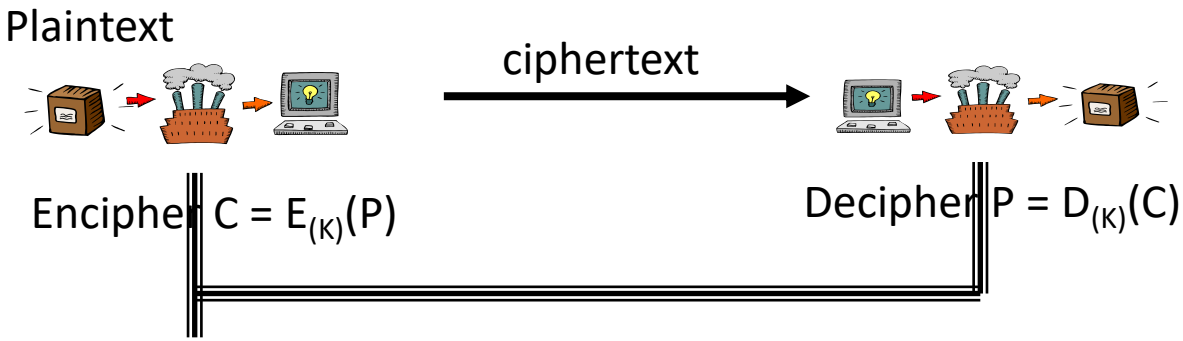
- Cost of breaking cipher exceeds the value of information.
- The time required is very high (> age of info or universe)

Computational security

- Given limited computing resources, the cipher cannot be broken in a reasonable time

Cryptography

- It has two main Components:
  1. Encryption-Decryption
     - Practice of hiding messages so that they can not be read by anyone other than the intended recipient



  2. Authentication & Integrity
     - Ensuring that users of data/resources are the persons they claim to be and that a message has not been surreptitiously altered

Ingredients of Cryptographic System

- **Plaintext**
  - The original intelligible message
- **Ciphertext**
  - The transformed message
- Message
  - Is treated as a non-negative integer hereafter
- **Cipher**
  - An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution
- **Key**
  - Some critical information used by the cipher, known only to the sender & receiver
- **Encipher** (encode)
  - The process of converting plaintext to ciphertext
- **Decipher** (decode)
  - The process of converting ciphertext back into plaintext