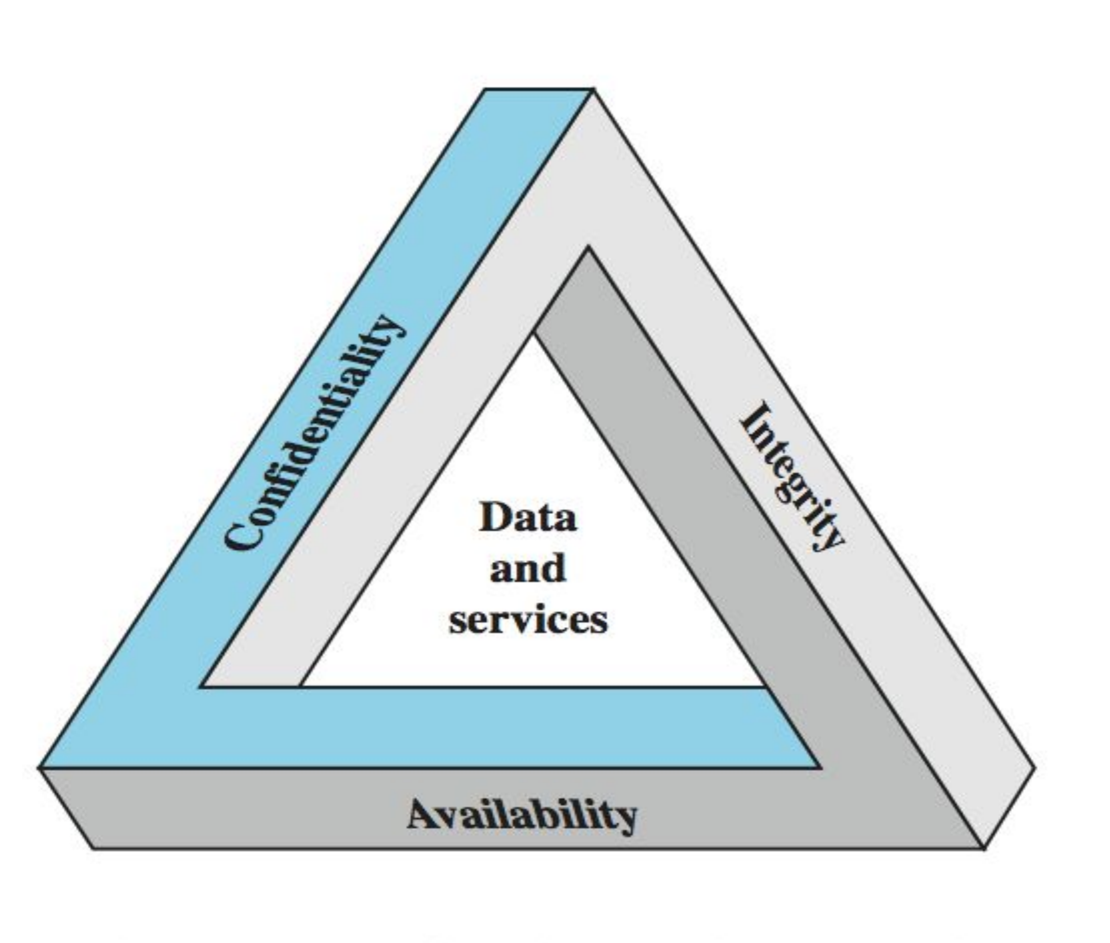
Cryptography and Network security

Module 1

Contents

- Introduction
- Services, Mechanisms, Mechanism Attacks
- The OSI security architecture
- model for network Security
- Cryptographic algorithms
  - Symmetric ciphers
  - Asymmetric encryption
- Substitution Techniques
- Transposition Techniques

Key Security Concepts



Examples of Security Requirements

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation

Aspects of Security

- 3 aspects of information security:
  - **Security attack**
  - **Security mechanism (control)**
  - **Security service**
- Note terms
  - Threat – a potential for violation of security
  - Vulnerability – a way by which loss can happen
  - Attack – an assault on system security, a deliberate attempt to evade security services

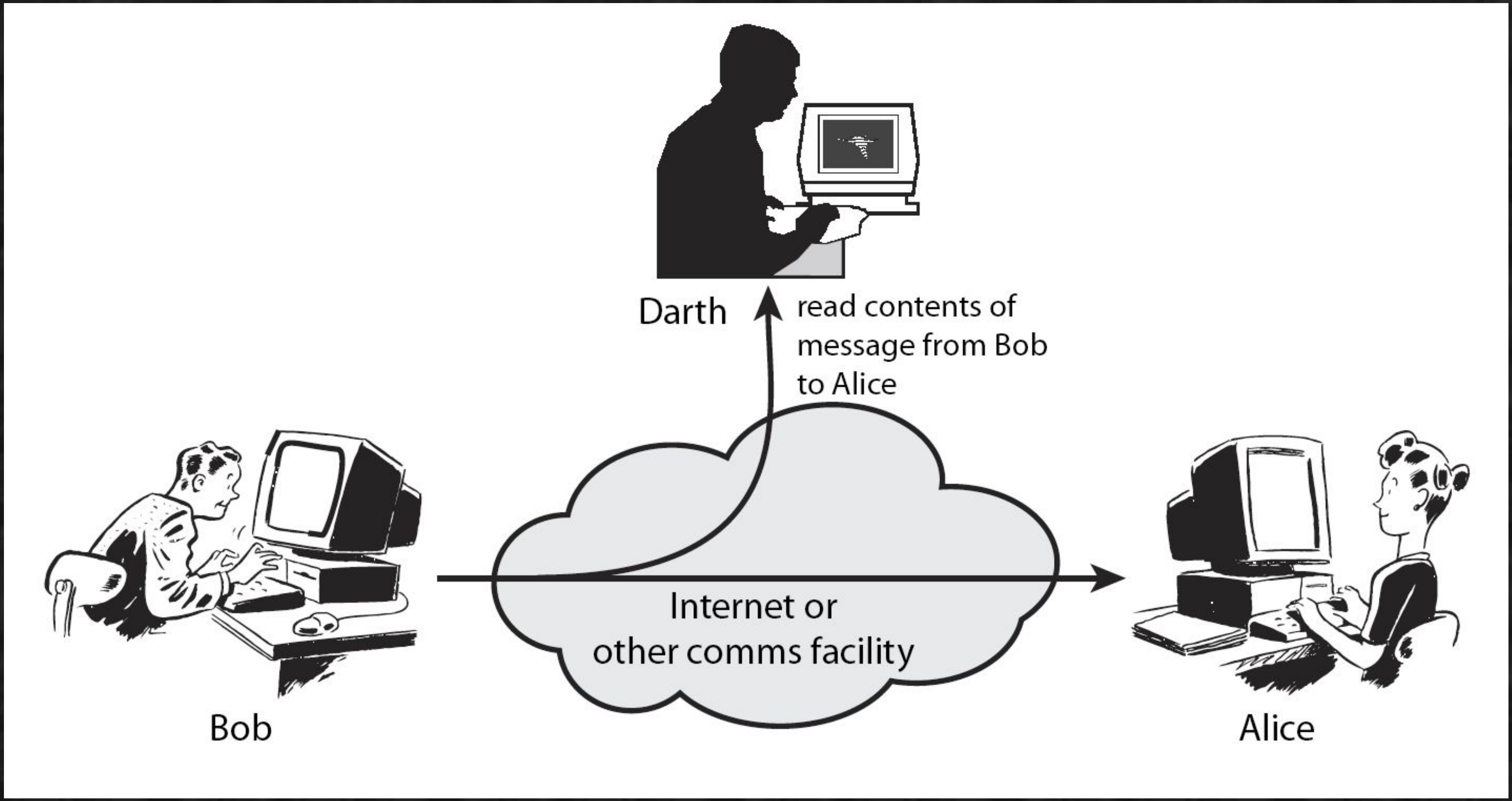
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- Defines a systematic way of defining and providing security requirements
- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

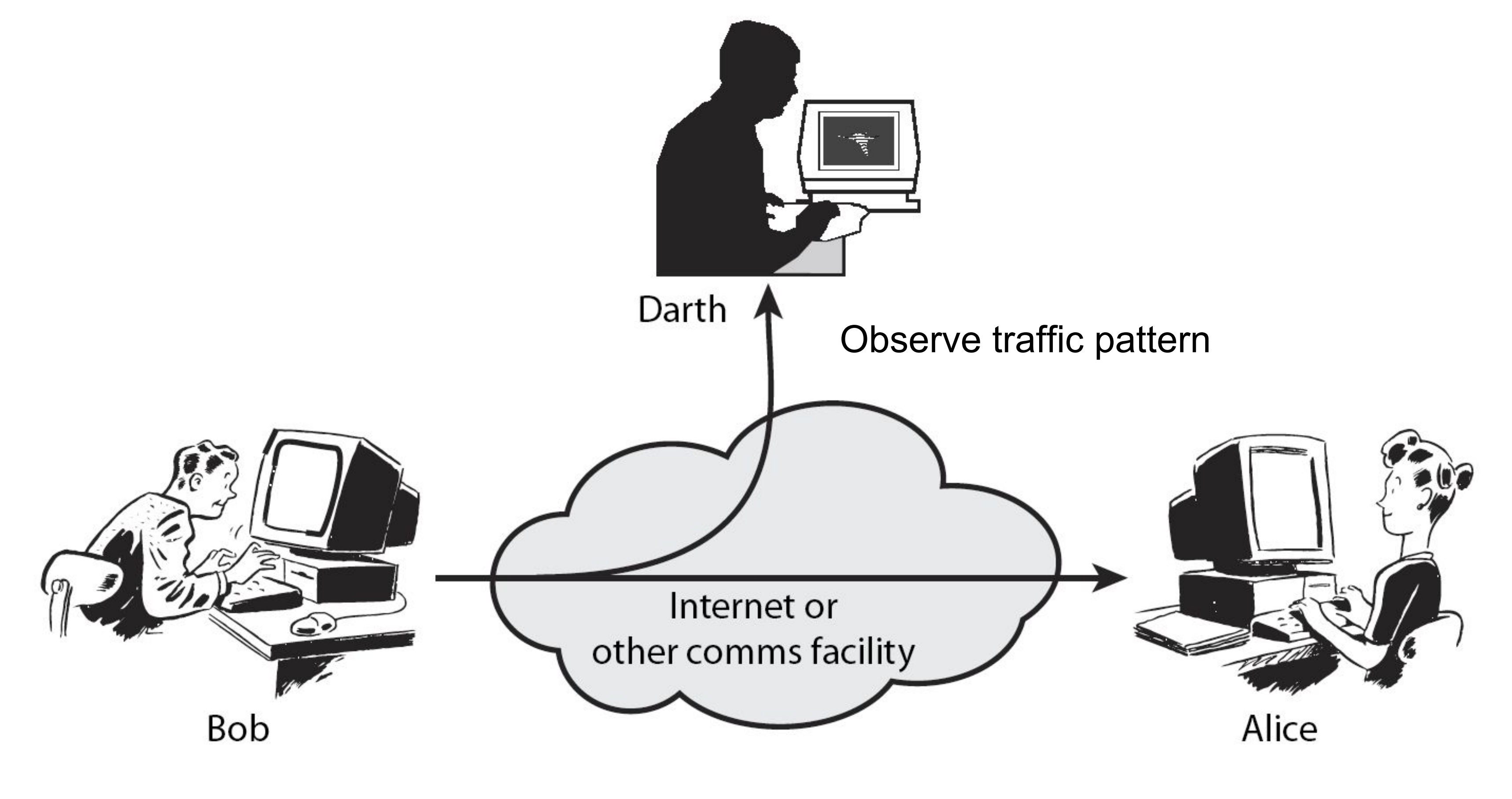
Security attack

- Any action that compromises the security of information owned by an organization.
- Passive attacks
- Active attacks

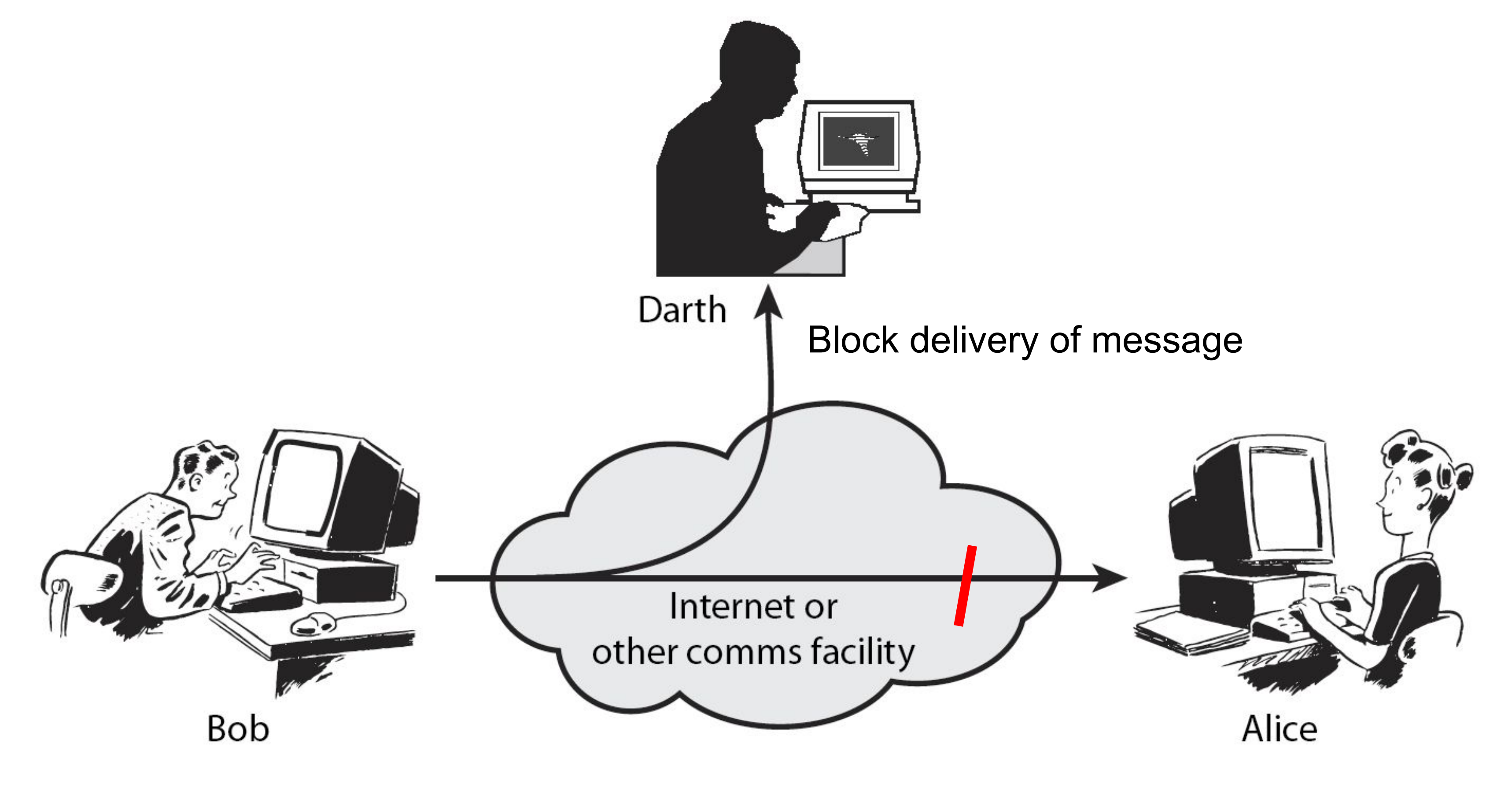
Passive Attack – Release of message



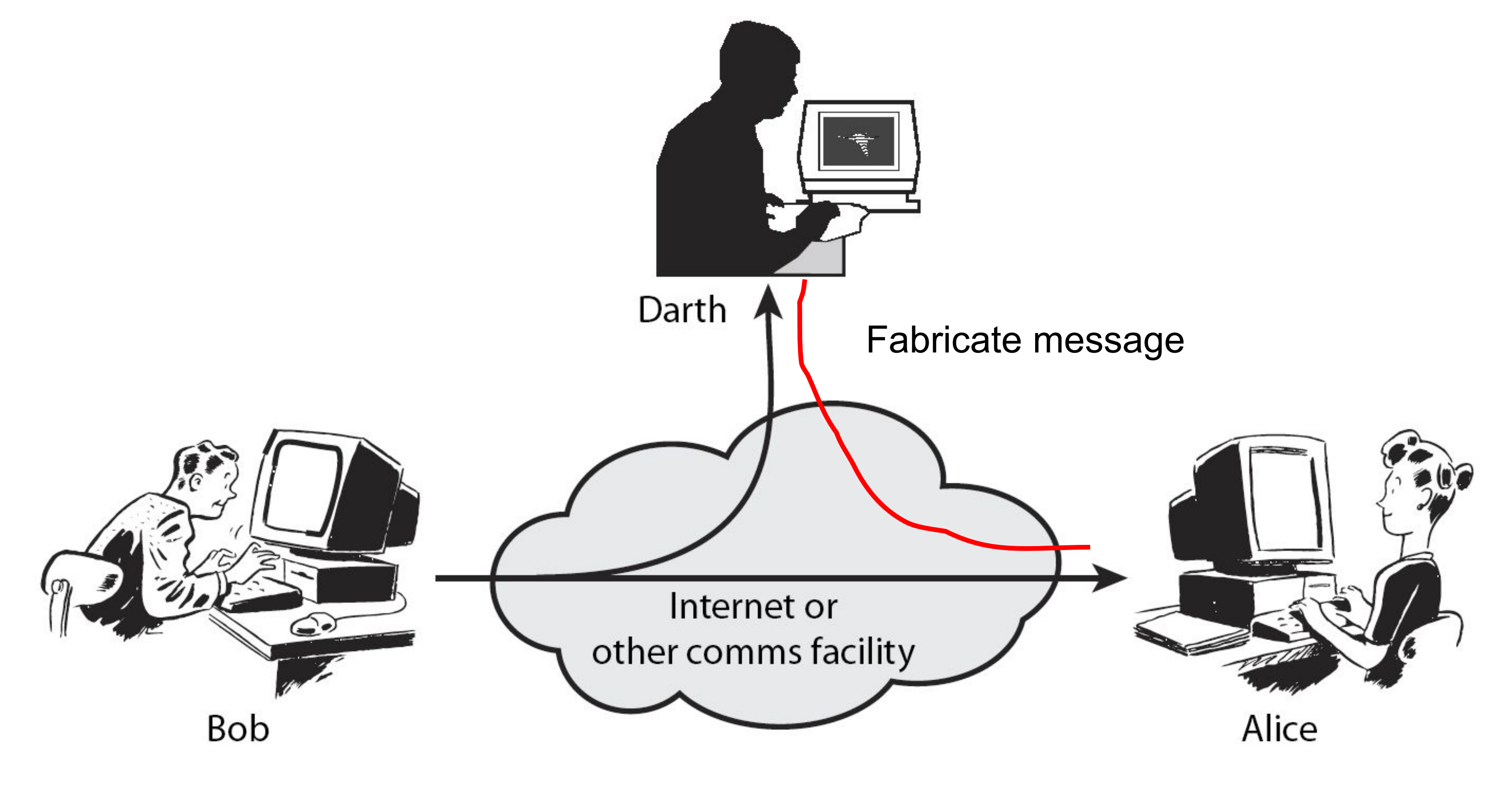
Passive Attack: Traffic Analysis



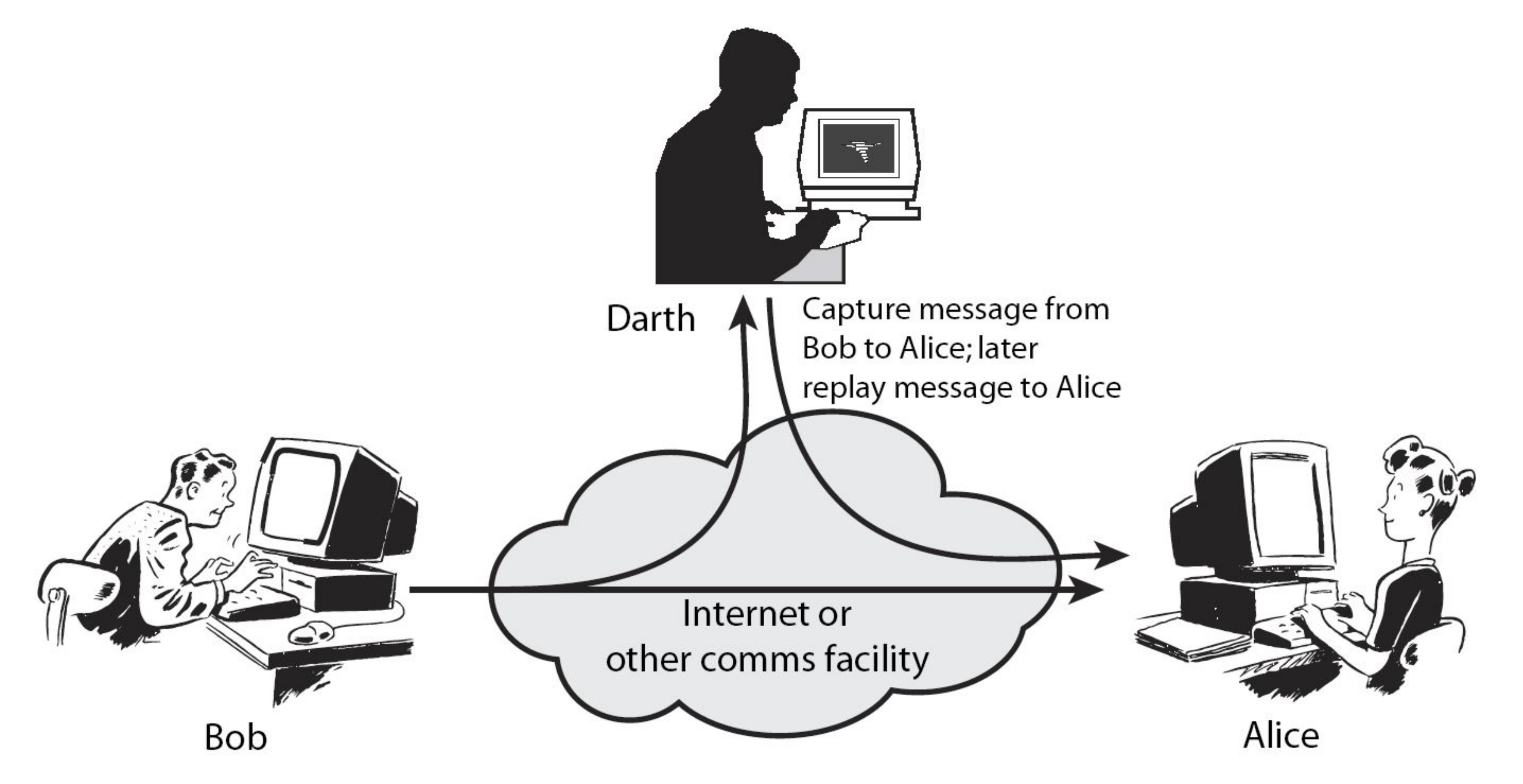
Active Attack: Denial of service



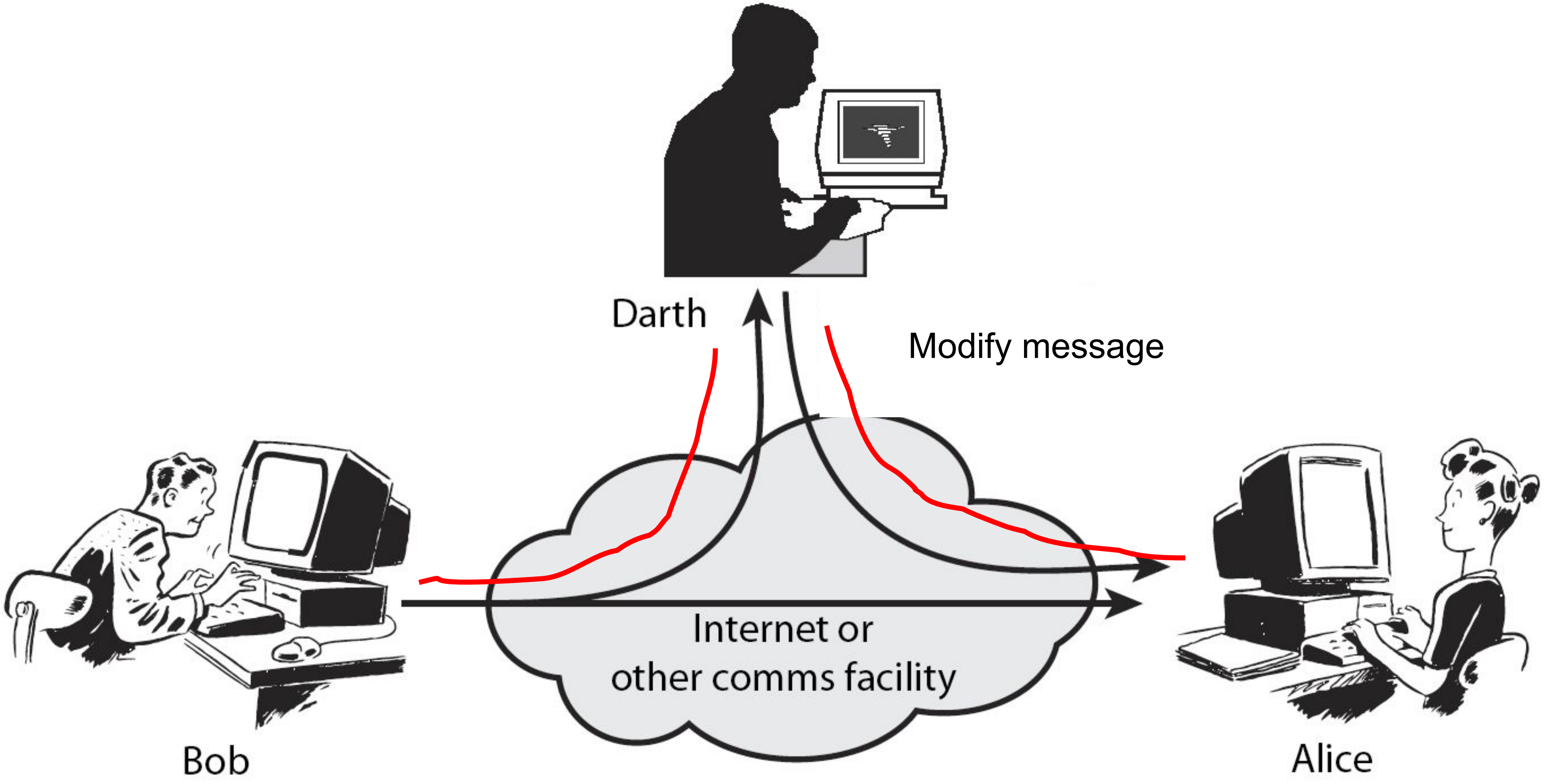
Active Attack: Masquerade



Active Attack: Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attack: Modification



Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

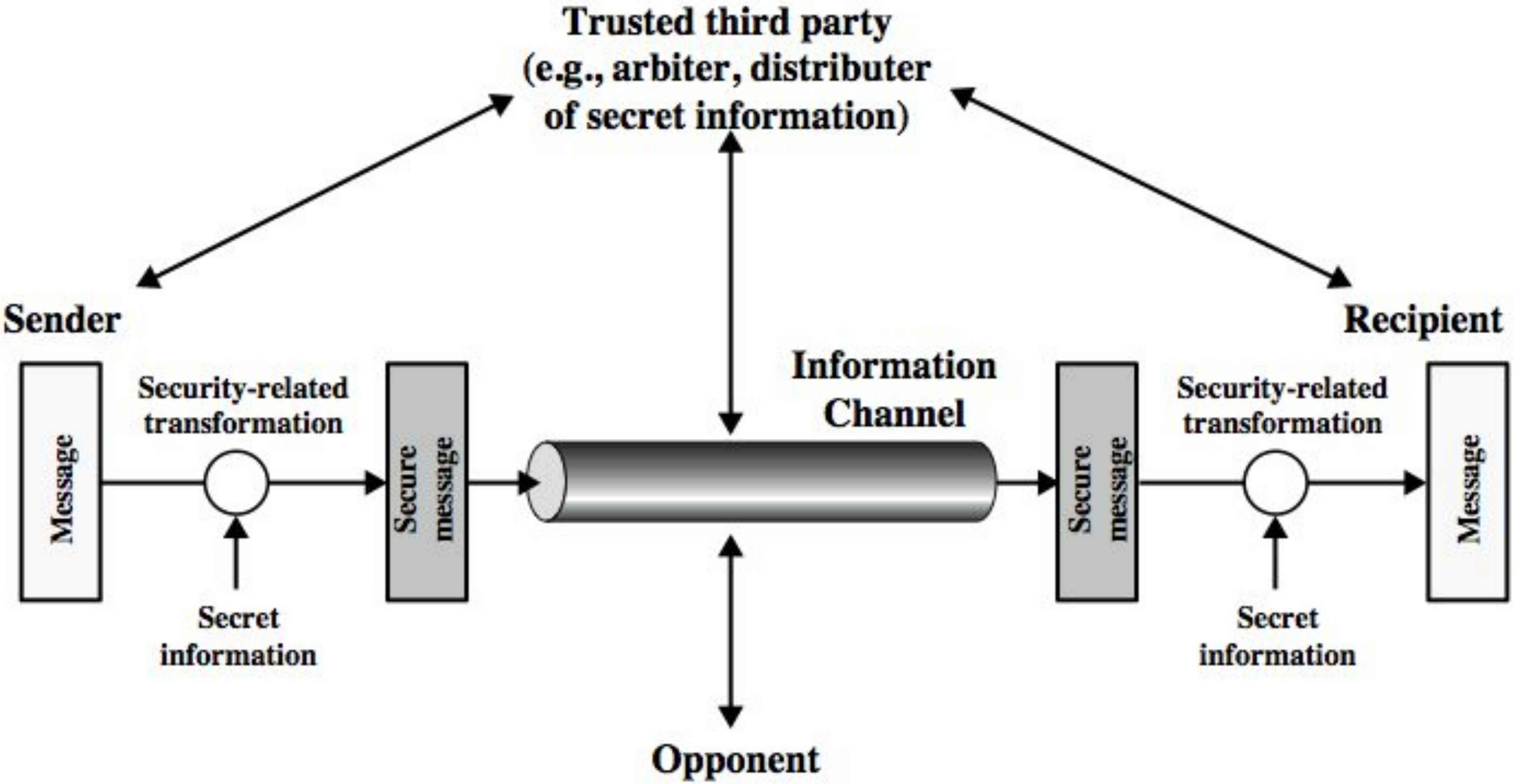
Security Services (X.800)

- A service that enhances the security of the data processing systems and the information transfers of an organization
- **Authentication** - assurance that communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques

Model for Network Security



Model for Network Security

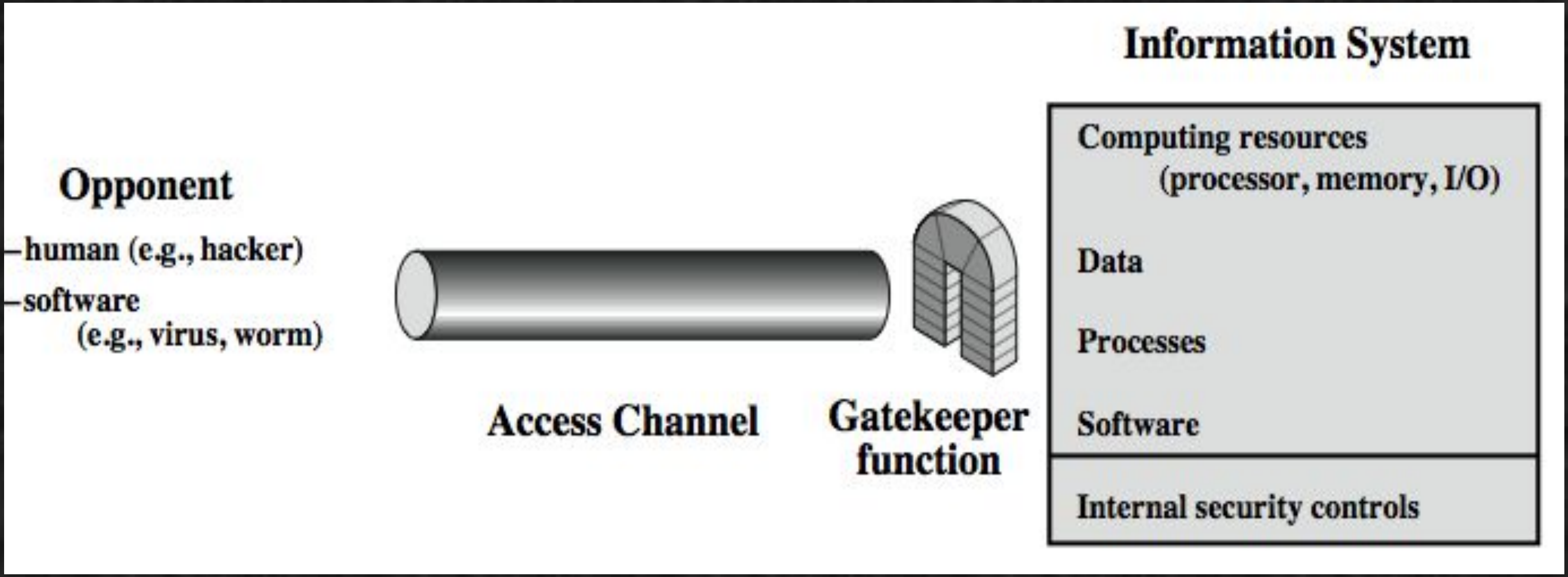
- All the techniques for providing security have two components:

1. A security-related transformation on the information to be sent
2. Some secret information shared by the two principals and, it is unknown to the opponent
3. A trusted third party may be needed to achieve secure transmission

Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

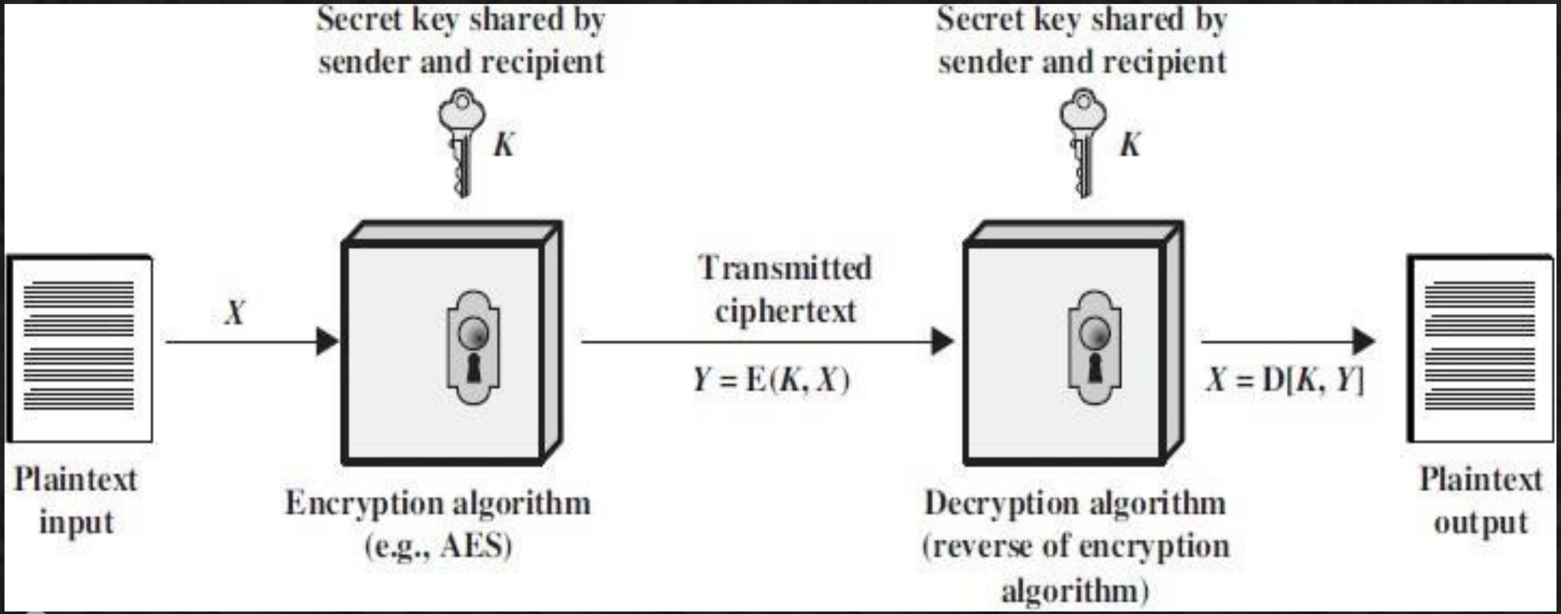
Model for Network Access Security



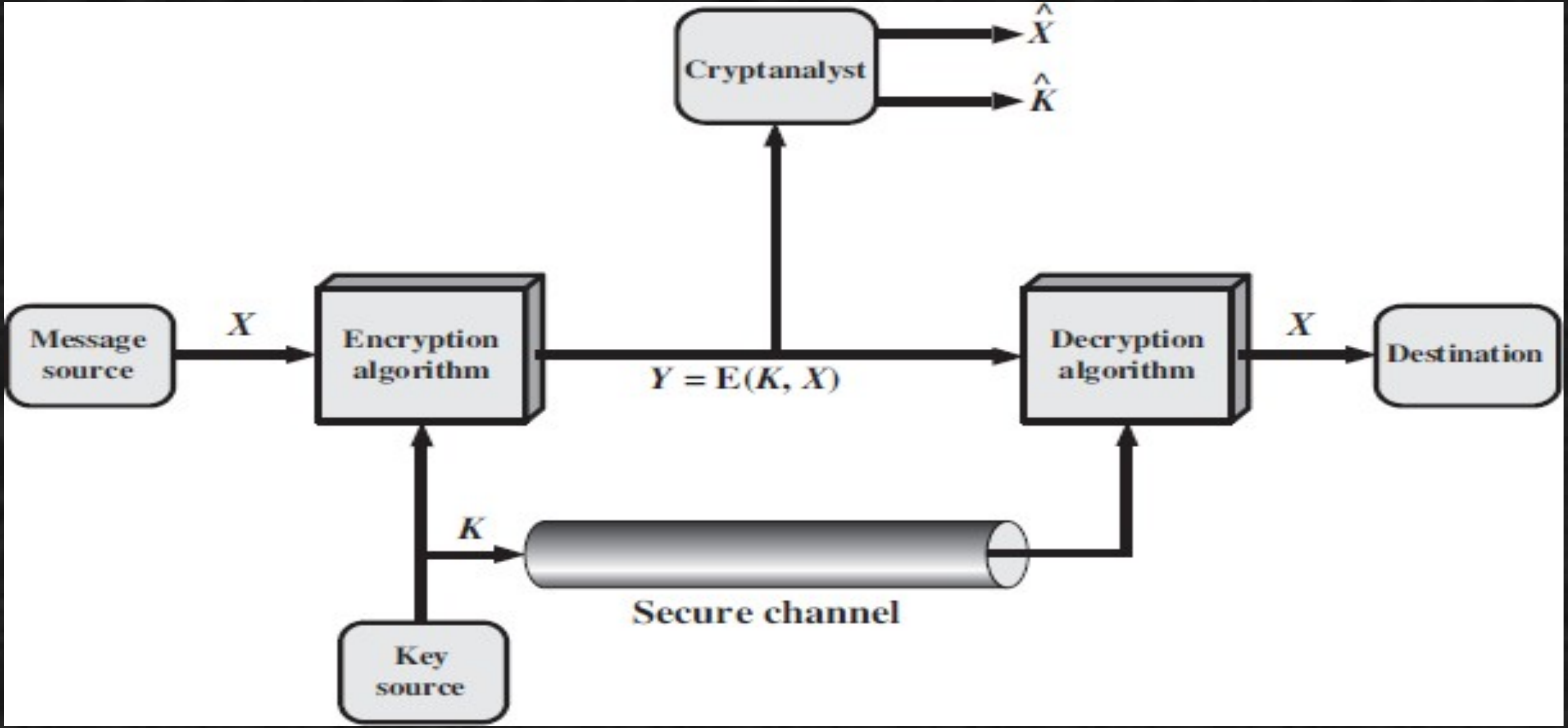
Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources

Symmetric Cipher Model


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Model of symmetric crypto system



Model of symmetric crypto system

Two requirements for secure use of symmetric encryption:

- A strong encryption algorithm
- A secret key known only to sender / receiver

Plaintext, $X = [X1, X2\dots XM]$

Key, $K = [K1, K2\dots KJ]$

Encryption, $Y = E_K(X)$

Decryption, $X = D_K(Y)$