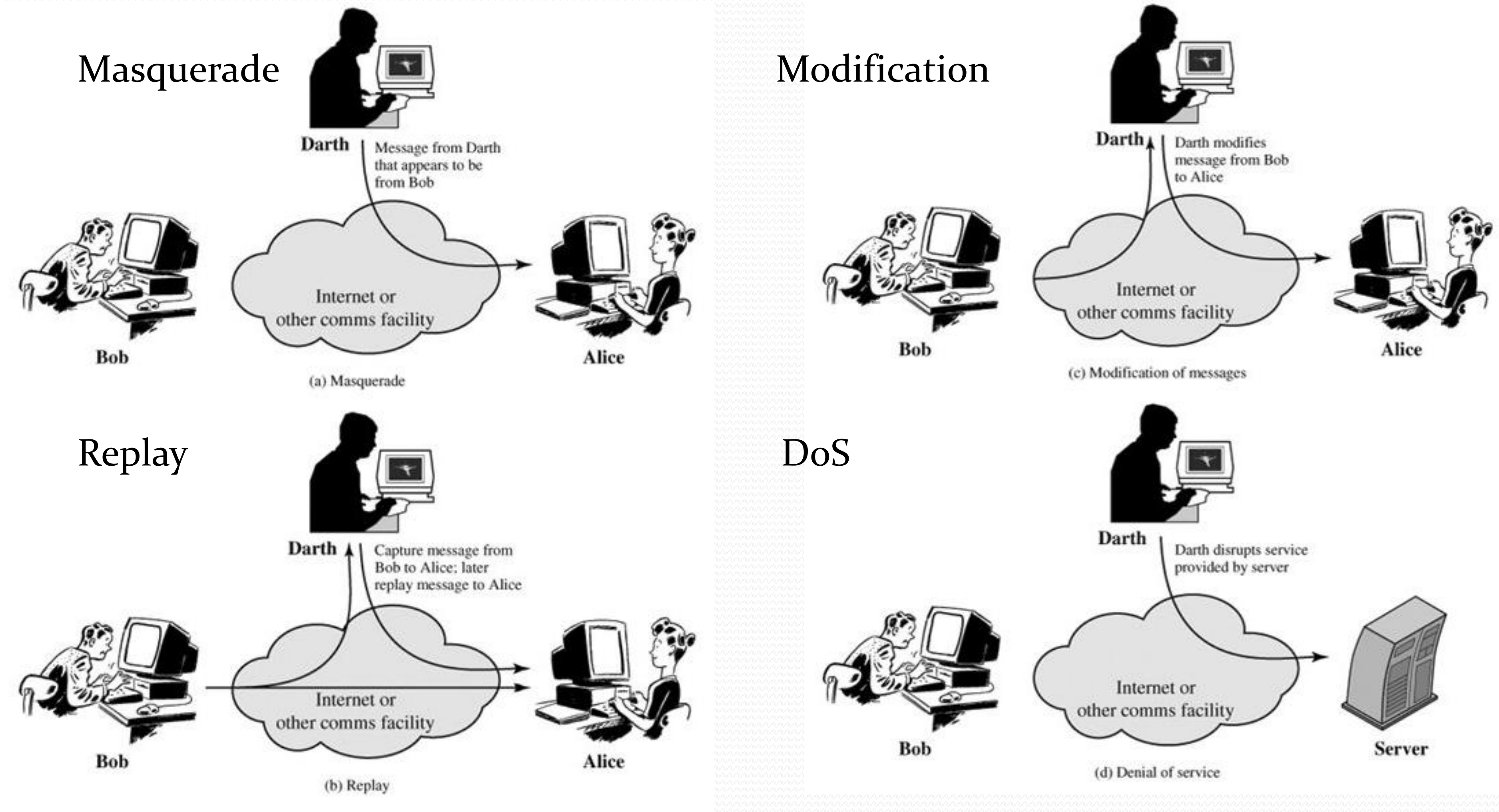
IT 422 Network Security Cryptography

Yasser F. O. Mohammad

2010.2.23

REMINDER 1: Active Attacks



Masquerade

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Modification

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Replay

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

(b) Replay

DoS

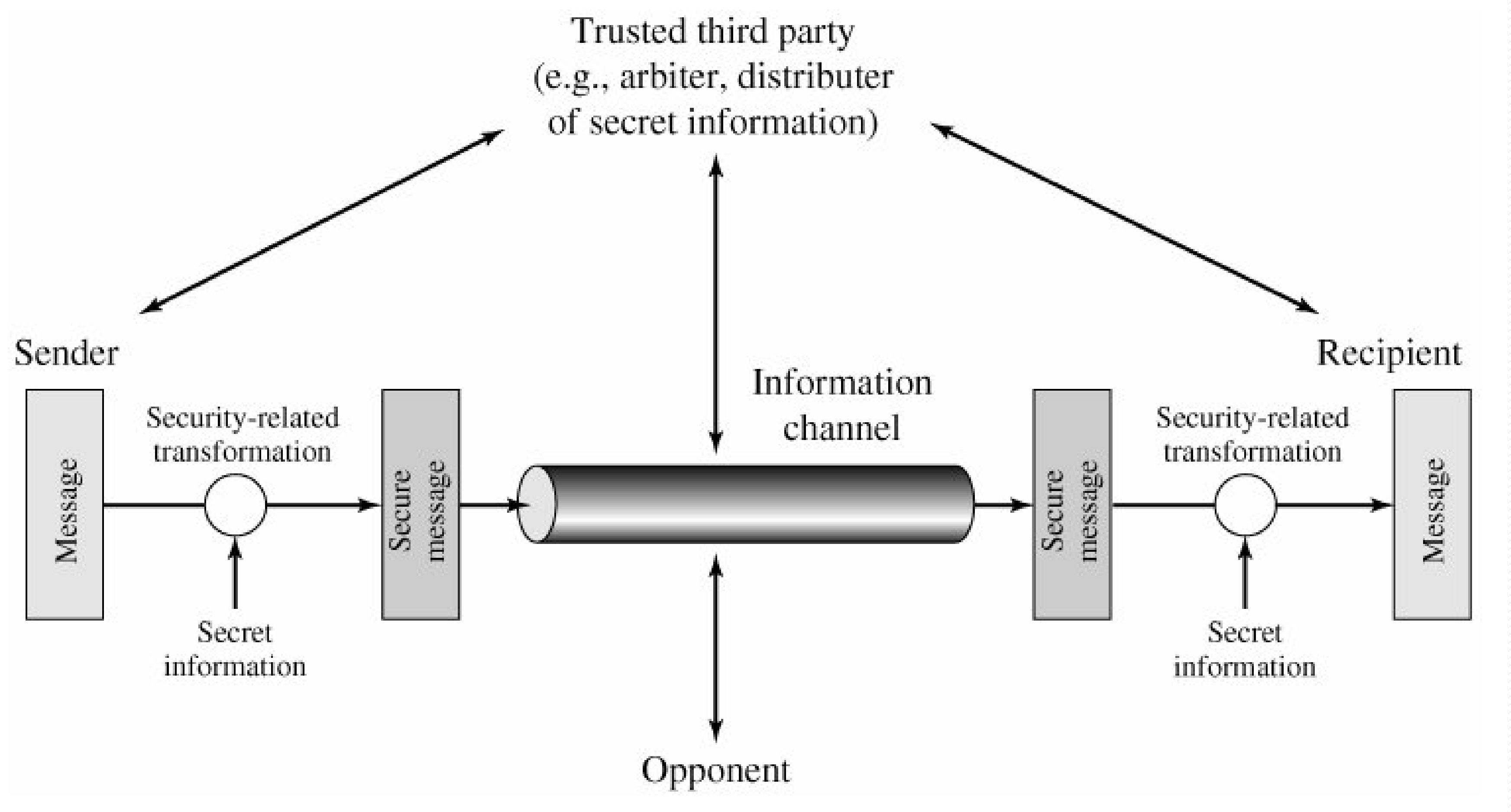
Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

REMINDER 2: Security Services in X.800

1. Authentication
   - Pear entity authentication
   - Data origin authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Nonrepudiation
6. Availability

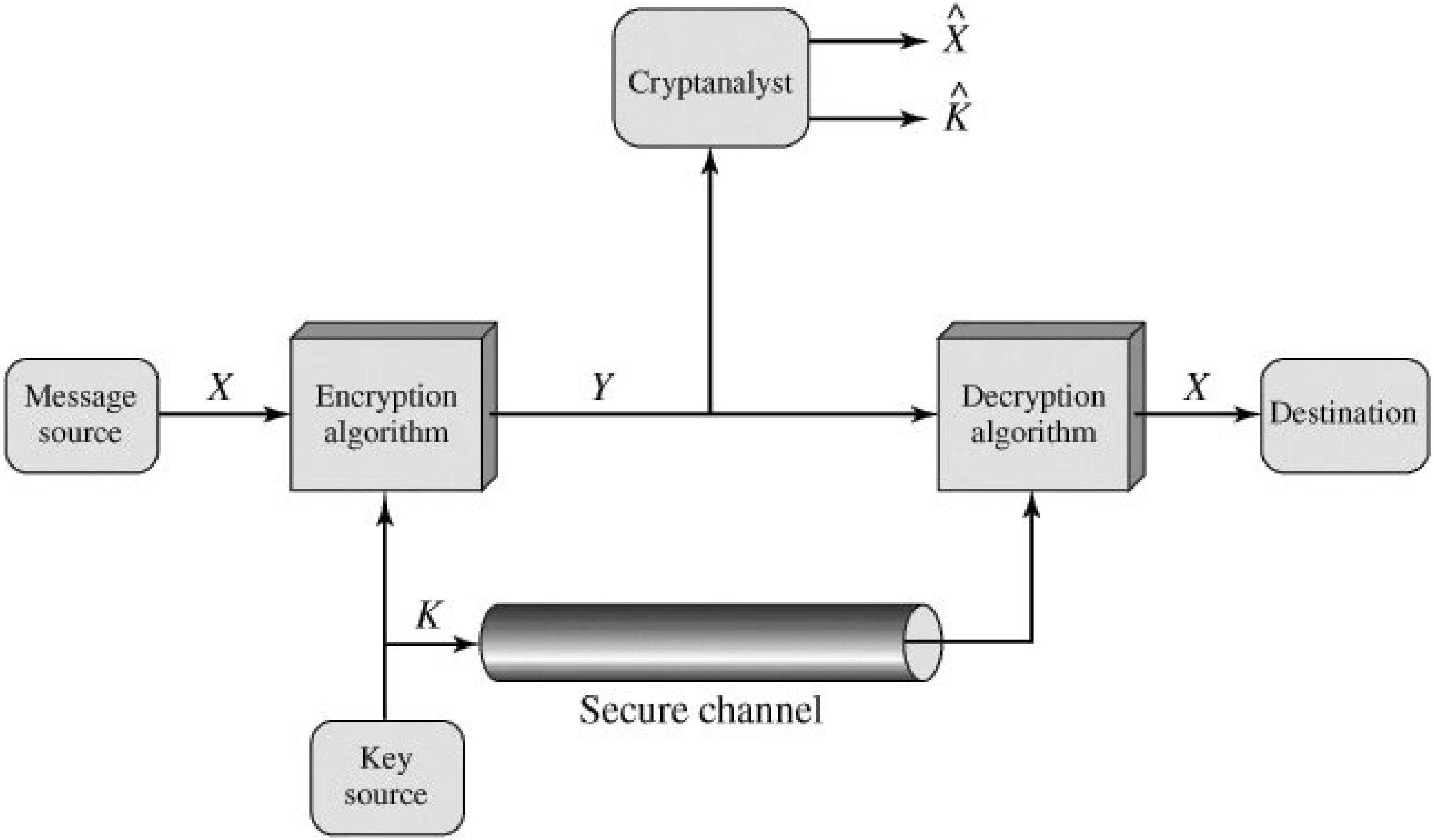
REMINDER 3: Model For Network Security



Basic Terms

- Plain Text
- Encipher/ciphertext
- Cryptography
- Cryptanalysis

Operational of Conventional Cryptosystem



Types of Cryptographic Systems

- Type of Operation
  - Substitution
  - Transposition
  - Product Systems

- Number of Keys
  - Single (Shared) Key
  - Two (public) Key

- Processing Technique
  - Block Cipher
  - Stream Cipher

Types of Cryptanalysis

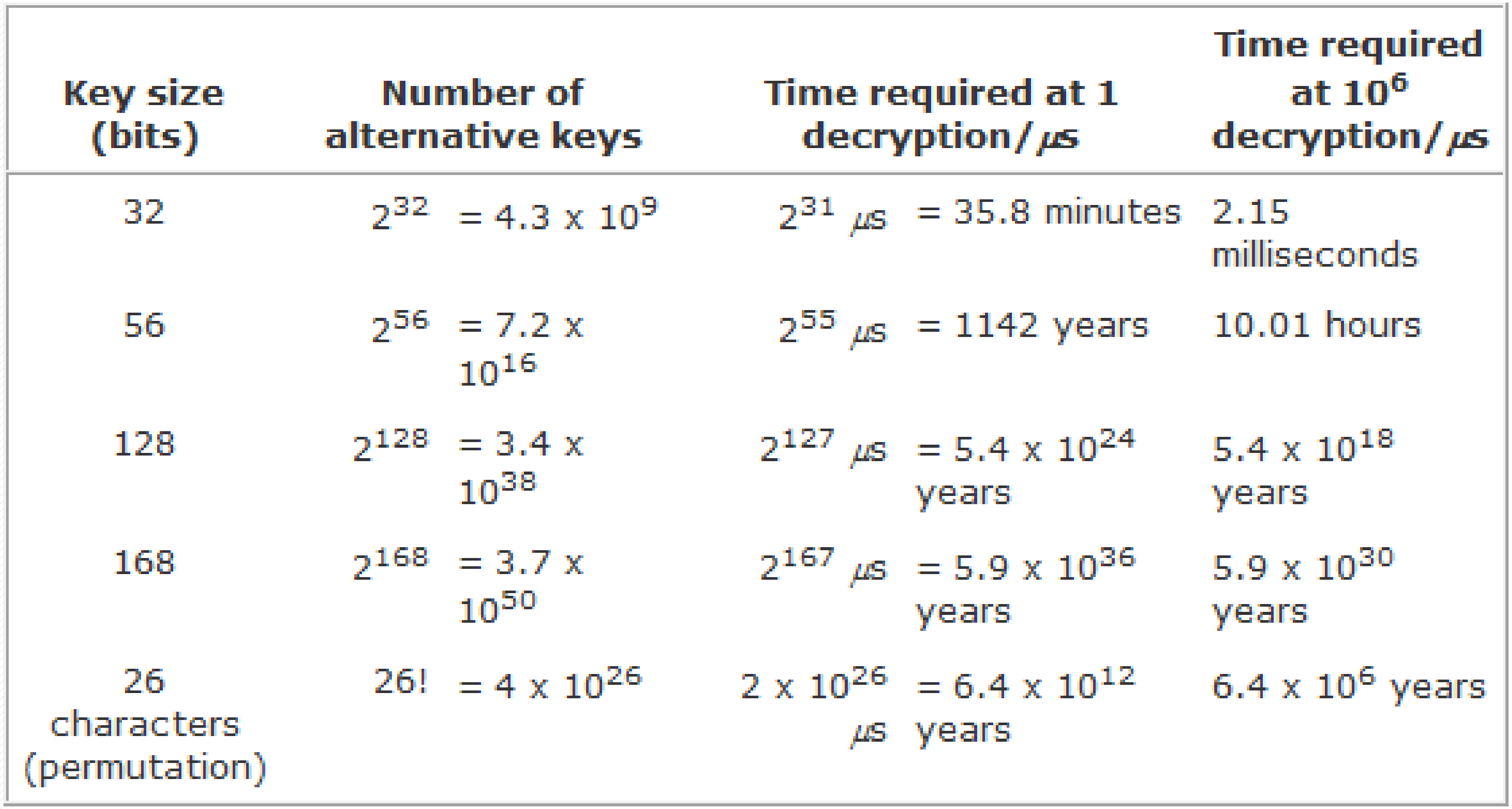
- Intelligence Level
  - Cryptanalysis (per se)
  - Brute-Force Attack
- Available Information
  - Ciphertext only
  - Known plaintext (Full/Partial)
  - Chosen plaintext (Differential Cryptanalysis)
  - Chosen ciphertext
  - Chosen text

Encryption Scheme Security

- Unconditional Security
  - Information is not there in the ciphertext
  - One-Time Pad

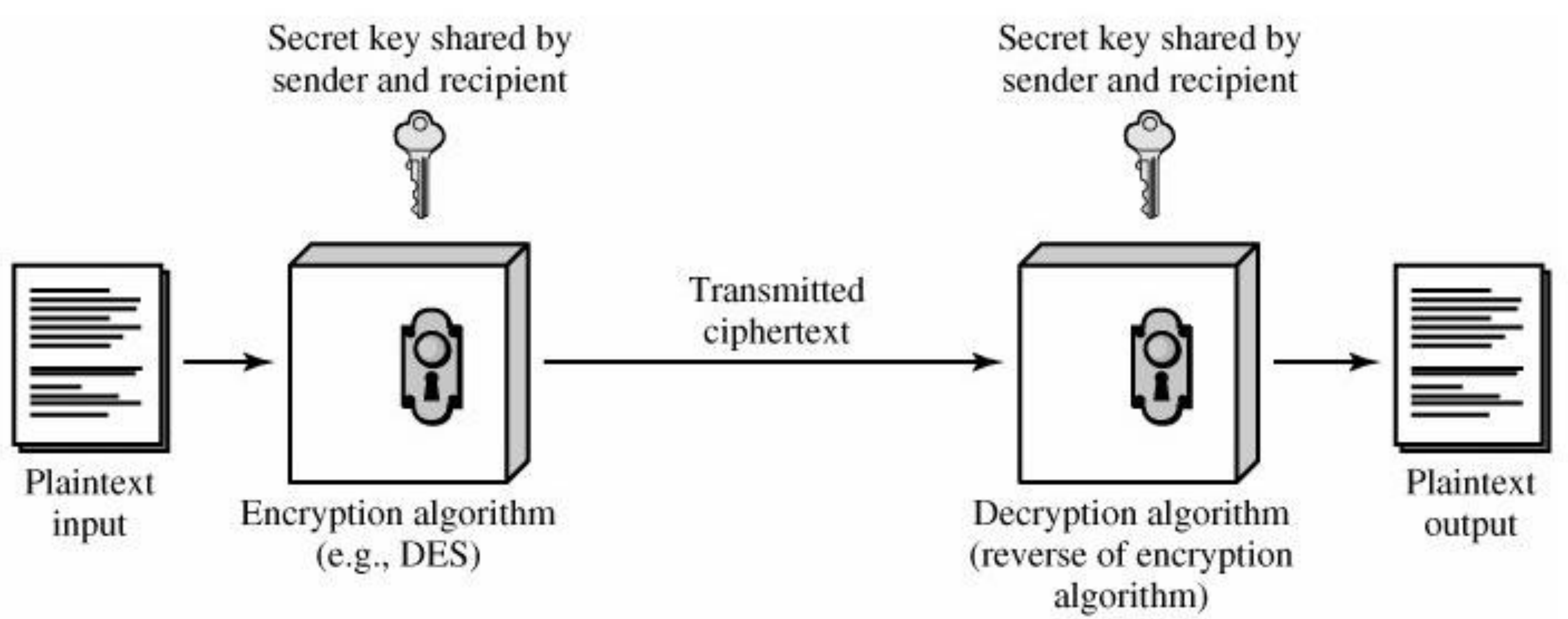
- Conditional Security
  - Cost
  - Time

Brute-Force Attack

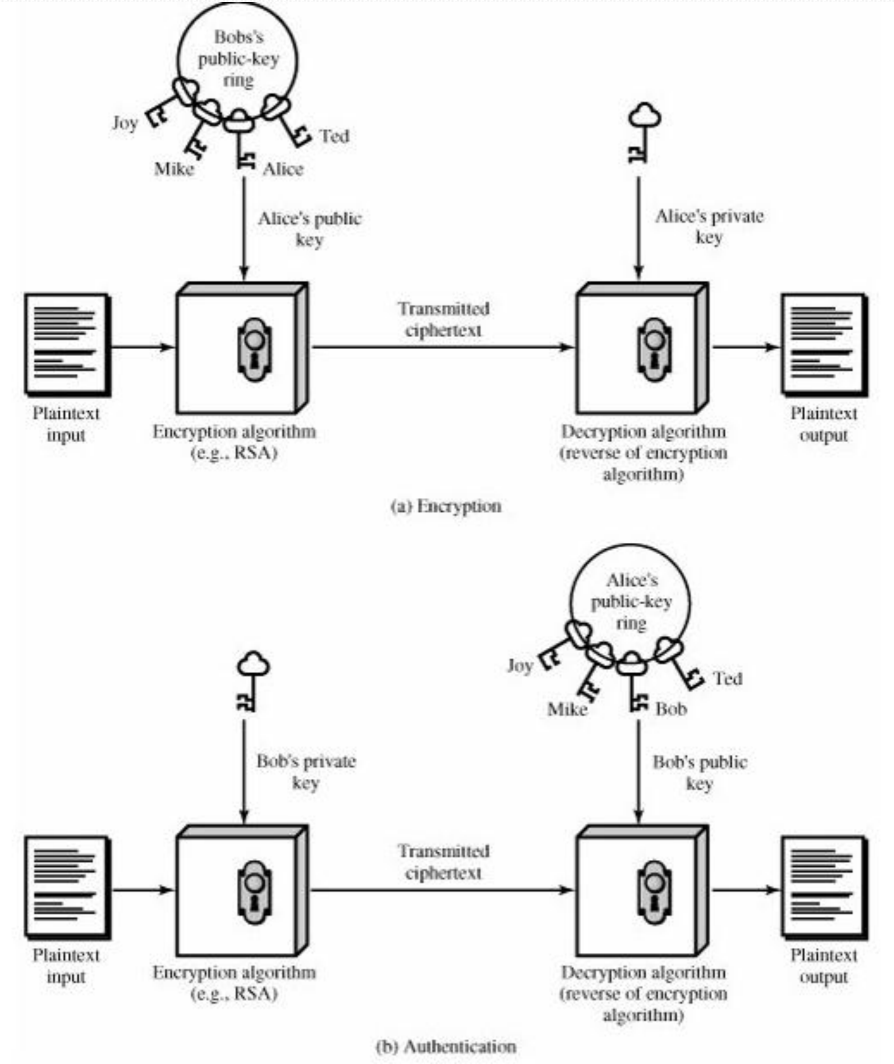


Key size (bits)	Number of alternative keys	Time required at 1 decryption/µs	Time required at 10^6 decryption/µs
32	2^{32} = 4.3 x 10^9	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	2^{56} = 7.2 x 10^{16}	2^{55} µs = 1142 years	10.01 hours
128	2^{128} = 3.4 x 10^{38}	2^{127} µs = 5.4 x 10^{24} years	5.4 x 10^{18} years
168	2^{168} = 3.7 x 10^{50}	2^{167} µs = 5.9 x 10^{36} years	5.9 x 10^{30} years
26 characters (permutation)	26! = 4 x 10^{26}	2 x 10^{26} µs = 6.4 x 10^{12} years	6.4 x 10^6 years

Shared Key Encryption


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Public Key Encryption



(a) Encryption

(b) Authentication

Classical Cryptosystems

Substitution Techniques

- Caesar Cipher
  - Example
    Plain : meet me after the toga party
    cipher: PHHW PH DIWHU WKH WRJD SDUWB

  - Subtitution Table:
    plain: abcdefghijklmnopqrstuvwxyz
    cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

  - Formula
    $C = E(3, p) = (p + 3) \bmod 26$
    $p = D(k, C) = (C - k) \bmod 26$

How to do cryptanalysis???