Information Security Systems
EC-615-F

Lecture No 7

Topics To be Covered

- Symmetric encryption
- Secret key encryption
- Shared key encryption

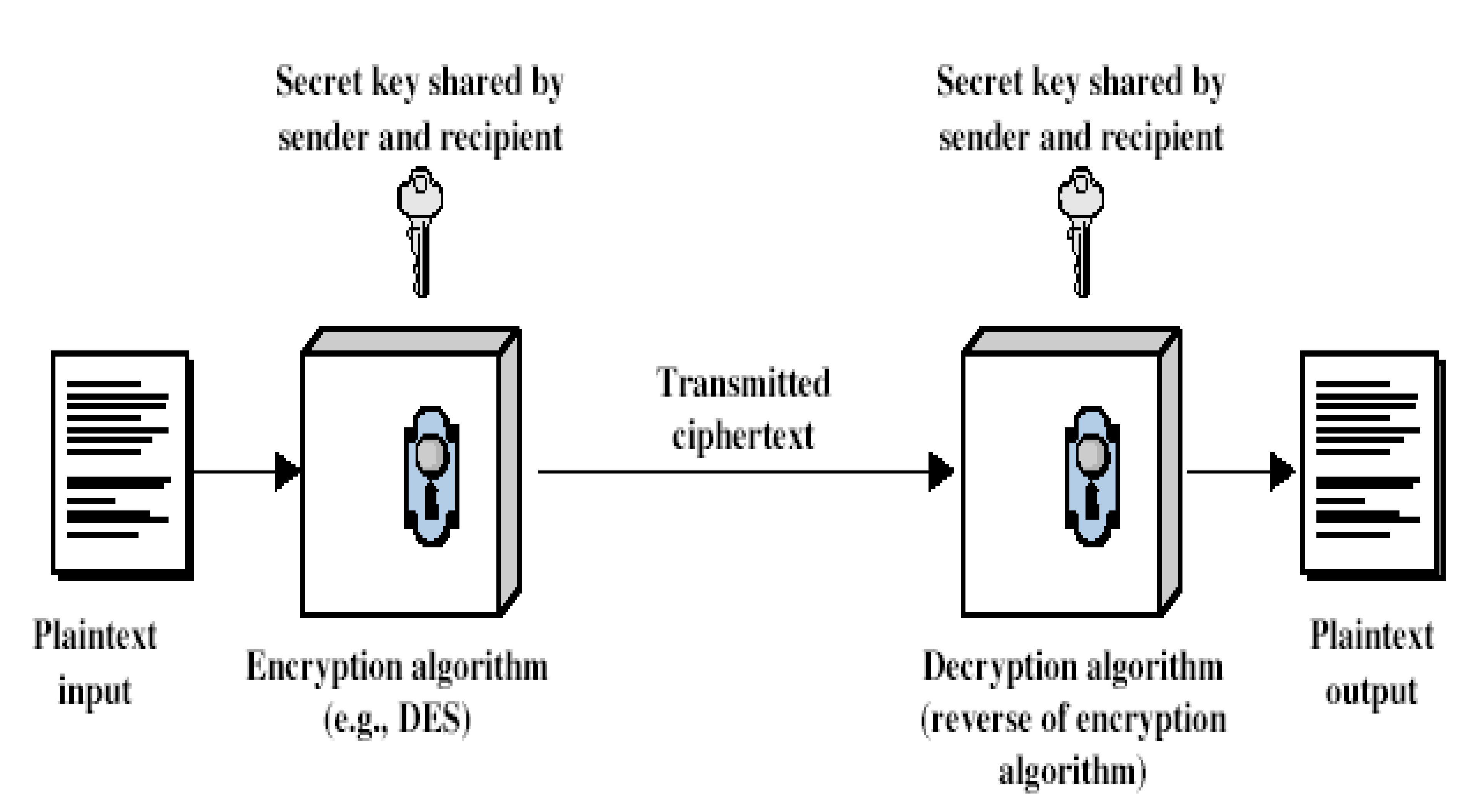
Symmetric Encryption

- or conventional / secret-key / single-key
- sender and recipient share a common key
- was the only type of cryptography, prior to invention of public-key in 1970's

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Symmetric Cipher Model


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

Requirements

- Two requirements for secure use of symmetric encryption:
    - a strong encryption algorithm
    - a secret key known only to sender / receiver

    $Y = \mathrm{E}_K(X)$

    $X = \mathrm{D}_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

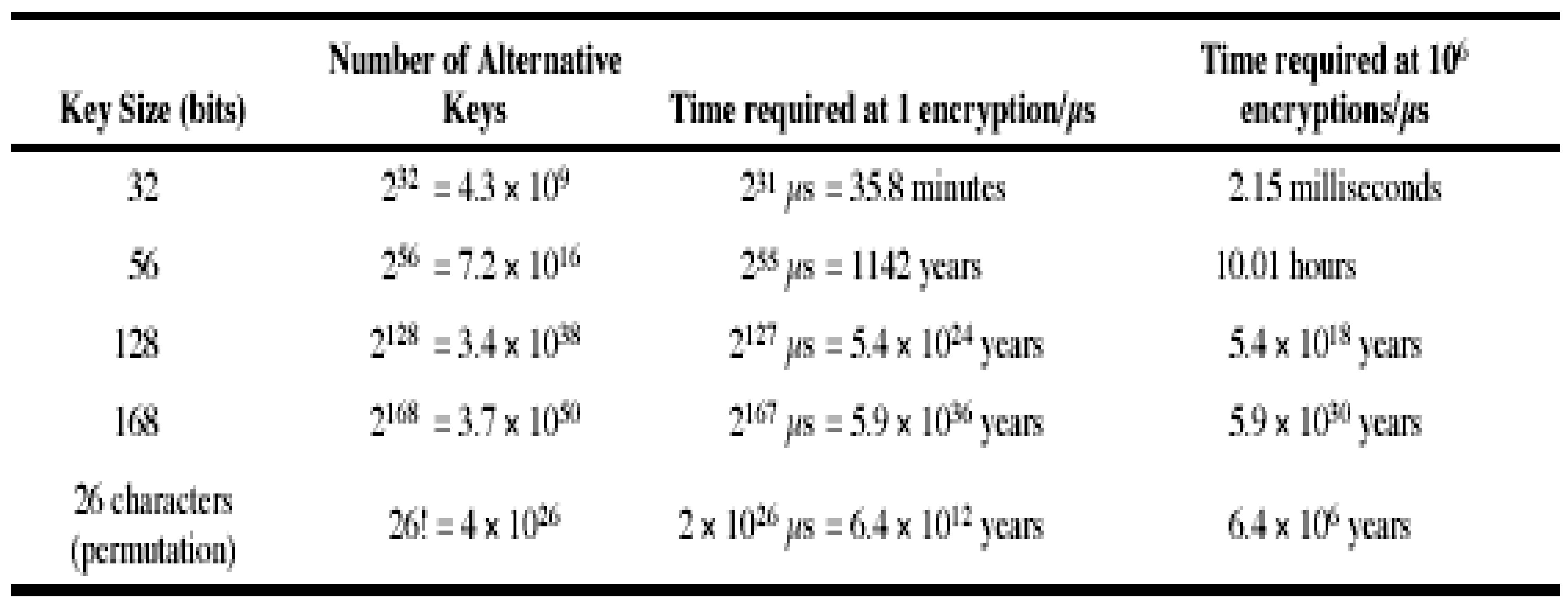
- can be characterized by:
  - type of encryption operations used
    - substitution / transposition / product
  - number of keys used
    - single-key or secret-key vs two-key or public-key
  - way in which plaintext is processed
    - block / stream

Types of Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm / ciphertext, statistical, can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext to attack cipher
- **chosen plaintext**
  - select plaintext and obtain ciphertext to attack cipher
- **chosen ciphertext**
  - select ciphertext and obtain plaintext to attack cipher
- **chosen text**
  - select either plaintext or ciphertext to en/decrypt to attack cipher

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext



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

More Definitions

- **unconditional security**
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **computational security**
  - given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken

Types of Ciphers

- *Substitution* ciphers
- *Permutation* (or *transposition*) ciphers
- Product ciphers

Classical Substitution Ciphers

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar (?)
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

- What’s the key?