# Classical Encryption Techniques

Prepared By
T. Sree Sharmila

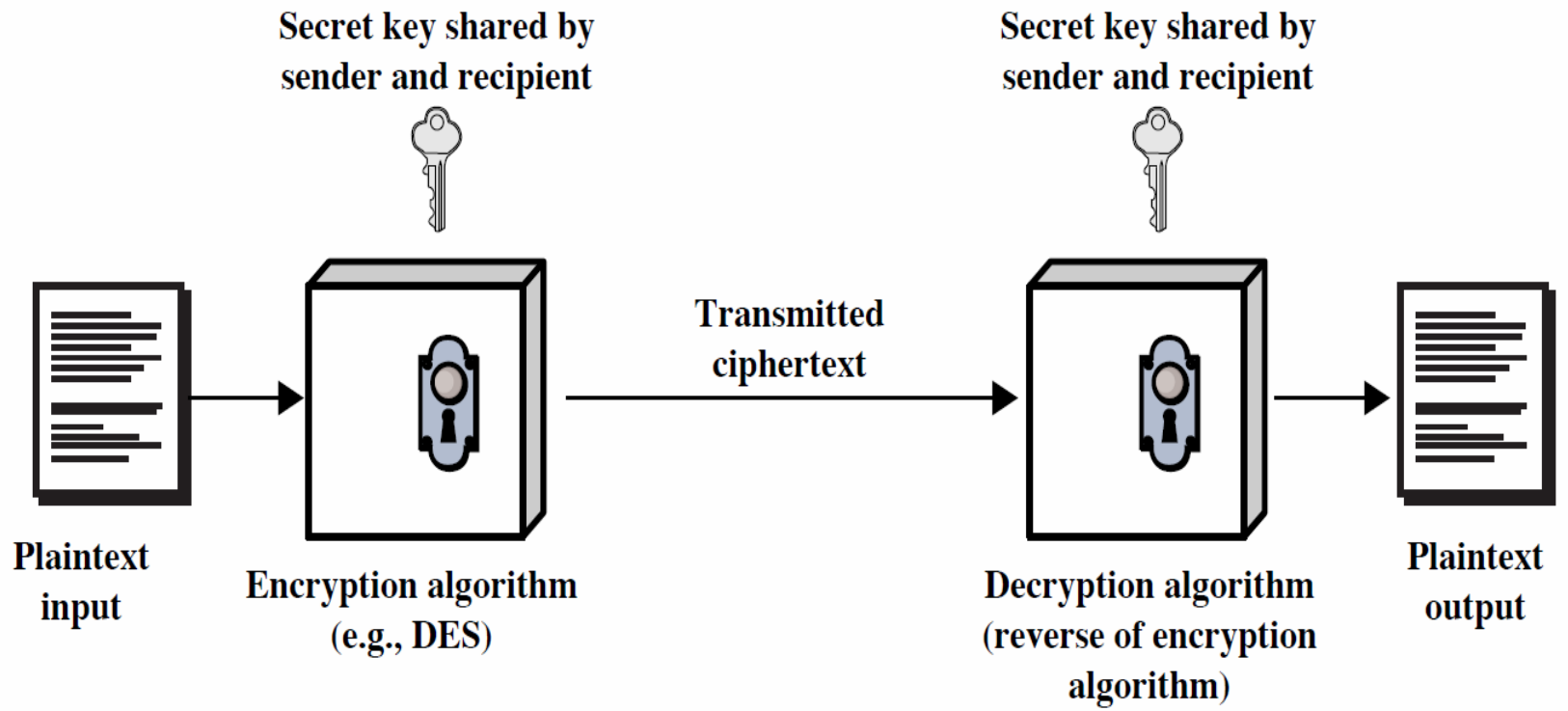
# Classical encryption techniques

- As opposed to modern cryptography
- Goals:
  - to introduce basic concepts & terminology of encryption
  - to prepare us for studying modern cryptography

# Basic terminology

- Plaintext: original message to be encrypted
- Ciphertext: the encrypted message
- Enciphering or encryption: the process of converting plaintext into ciphertext
- Encryption algorithm: performs encryption
  - Two inputs: a plaintext and a secret key

# Symmetric Cipher Model



- Deciphering or decryption: recovering plaintext from ciphertext
- Decryption algorithm: performs decryption
  - Two inputs: ciphertext and secret key
- Secret key: same key used for encryption and decryption
  - Also referred to as a symmetric key

- Cipher or cryptographic system : a scheme for encryption and decryption
- Cryptography: science of studying ciphers
- Cryptanalysis: science of studying attacks against cryptographic systems
- Cryptology: cryptography + cryptanalysis

# Ciphers

- Symmetric cipher: same key used for encryption and decryption
  - Block cipher: encrypts a block of plaintext at a time (typically 64 or 128 bits)
  - Stream cipher: encrypts data one bit or one byte at a time
- Asymmetric cipher: different keys used for encryption and decryption

# Symmetric Encryption

- or conventional / secret-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are symmetric
- The only type of ciphers prior to the invention of asymmetric-key ciphers in 1970’s
- by far most widely used

# Symmetric Encryption

- Mathematically:

  $Y = E_K(X)$ or $Y = E(K, X)$

  $X = D_K(Y)$ or $X = D(K, Y)$
- $X$ = plaintext
- $Y$ = ciphertext
- $K$ = secret key
- E = encryption algorithm
- D = decryption algorithm
- Both E and D are known to public

# Cryptanalysis

- Objective: to recover the plaintext of a ciphertext or, more typically, to recover the secret key.
- Kerkhoff's principle: the adversary knows all details about a cryptosystem except the secret key.
- Two general approaches:
  - brute-force attack
  - non-brute-force attack (cryptanalytic attack)

# Brute-Force Attack

- Try every key to decipher the ciphertext.
- On average, need to try half of all possible keys
- Time needed proportional to size of key space

| Key Size (bits) | Number of Alternative Keys | Time required at 1 decryption/μs | Time required at $10^6$ decryptions/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 = $5.4 \times 10^{24}$ years | $5.4 \times 10^{18}$ years |
| 168 | $2^{168} = 3.7 \times 10^{50}$ | $2^{167}$ μs = $5.9 \times 10^{36}$ years | $5.9 \times 10^{30}$ years |
| 26 characters (permutation) | $26! = 4 \times 10^{26}$ | $2 \times 10^{26}$ μs = $6.4 \times 10^{12}$ years | $6.4 \times 10^6$ years |

# Cryptanalytic Attacks

- May be classified by how much information needed by the attacker:
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Chosen-ciphertext attack

# Ciphertext-only attack

- Given: a ciphertext c
- Q: what is the plaintext m?
- An encryption scheme is completely insecure if it cannot resist ciphertext-only attacks.

# Known-plaintext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, …, $(m_k,c_k)$ and a new ciphertext c.

- Q: what is the plaintext of c?
- Q: what is the secret key in use?

# Chosen-plaintext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, …, $(m_k,c_k)$, where $m_1, m_2, \ldots, m_k$ are chosen by the adversary; and a new ciphertext c.

- Q: what is the plaintext of c, or what is the secret key?

# Example: chosen-plaintext attack

- In 1942, US Navy cryptanalysts discovered that Japan was planning an attack on “AF”.
- They believed that “AF” means Midway island.
- Pentagon didn’t think so.
- US forces in Midway sent a plain message that their freshwater supplies were low.
- Shortly, US intercepted a Japanese ciphertext saying that “AF” was low on water.
- This proved that “AF” is Midway.

# Chosen-ciphertext attack

- Given: $(m_1,c_1)$, $(m_2,c_2)$, …, $(m_k,c_k)$, where $c_1, c_2, \ldots, c_k$ are chosen by the adversary; and a new ciphertext c.

- Q: what is the plaintext of c, or what is the secret key?