Cryptography (BCA 615)
BCA 6th Sem

Lecture Notes By:
Dr. Neha Kishore
Associate Professor,
CSE Department, MAIT, MAU

Basics of Cryptography

Introduction to Cryptography

- Cryptography is a science of disguising messages so that only the intended recipient can decipher the received message.
- It also provide Message integrity, authentication and digital signatures.
- Combination of Cryptology and Cryptanalysis.

Definitions

- **Cryptosystem**
  - **Transforms *plaintext* into *ciphertext* using a *key***
  - **ciphertext unintelligible without knowledge of key**

Definitions

- **Cryptology**

  is the practice and study of encryption techniques for secure communication

- **Cryptanalysis**

  is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so.

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm

Introduction to Cryptography

- **Original message to be encrypted is called – *Plain Text*.**
- **Disguised Version – *Cipher Text*.**
- **Process of disguising a message – *Encryption*.**
- **The process of recovering the original message – *Decryption*.**

Conventional Encryption Principles

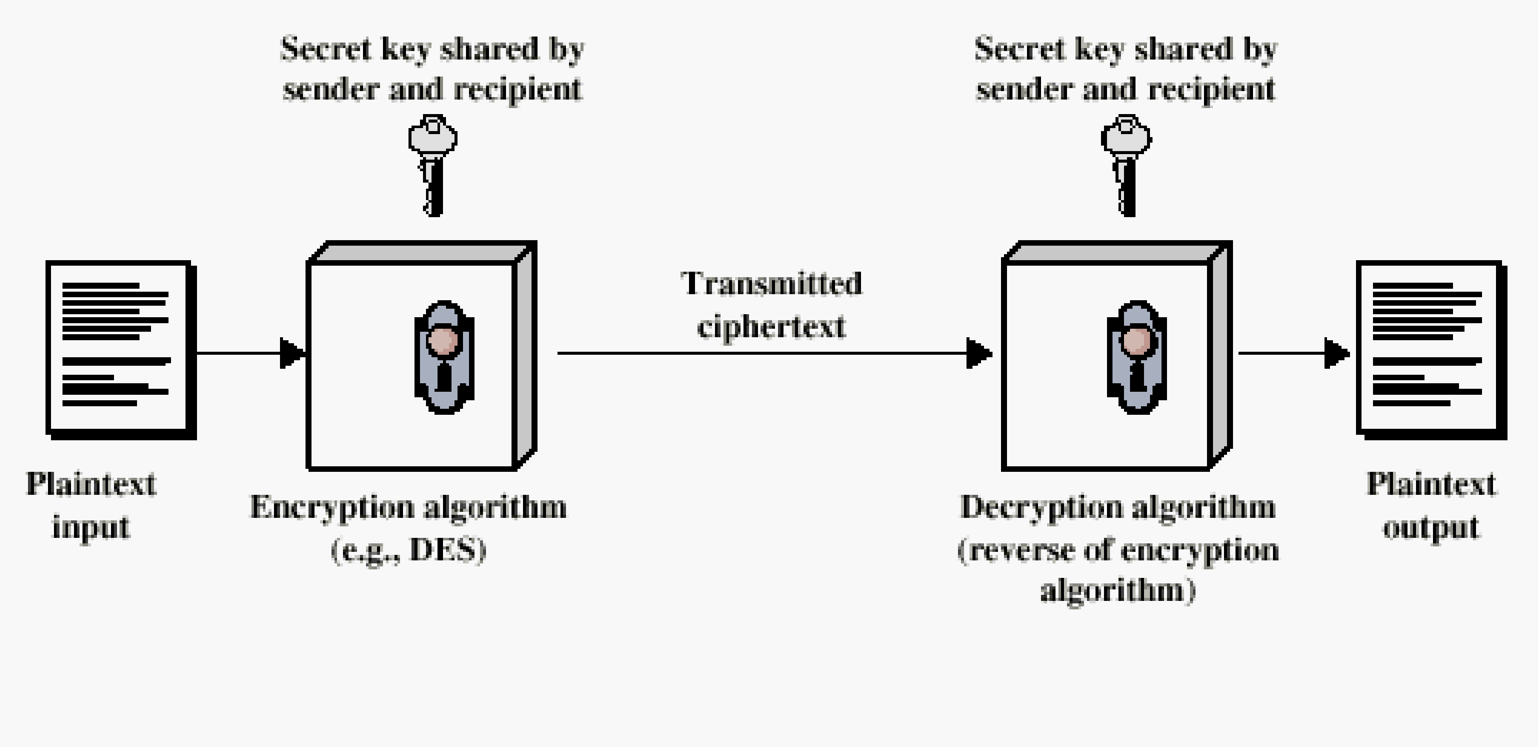

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Conventional Encryption

Introduction to Cryptography

- Encryption involves the use of encrytion function or algorithm, denoted by E, and encryption key, e.
- Similarly, decryption involves the use of decryption function or algorithm, denoted by D, and decryption key, d.

$$c = E_e\ (p)$$

$$p = D_d\ (c)$$

Types of Cryptography

- Symmetric or
  Secret key Cryptography

- Asymmetric or
  Public key Cryptography

Secret key Cryptography

- Both sender and receiver share a common secret
- The same secret is used for encryption and decryption
- So, e = d, in the equation.
- Hence this is also called symmetric key cryptography.

Secret key Cryptography

- If Bob and Alice share a common secret key, k, then Bob encrypts a message using the key, k and Alice also decrypts the message using the same key, k.
- Operation performed by Bob –
  - $c = E_k (p)$
- Operation performed by Alice –

  p = Dk (c)

Public key Cryptography

- Two distinct key pair are used.
- The encryption key or public key and the decryption key or private key
- The public key is used for encryption and is revealed to the world.
- The private key is used for decryption by the receiver.
- Because both keys are distinct, hence this is also called asymmetric key cryptography.

Public key Cryptography

- If Bob has a public – private key pair, Alice would encrypt her message using Bob's public key. Bob then decrypts the message using his private key assuming that he keeps it securely and only he can use that key.
- Operation performed by Bob –
  - $c = E_{B.pub}(p)$
- Operation performed by Alice –

  $p = D_{B.pri}(c)$

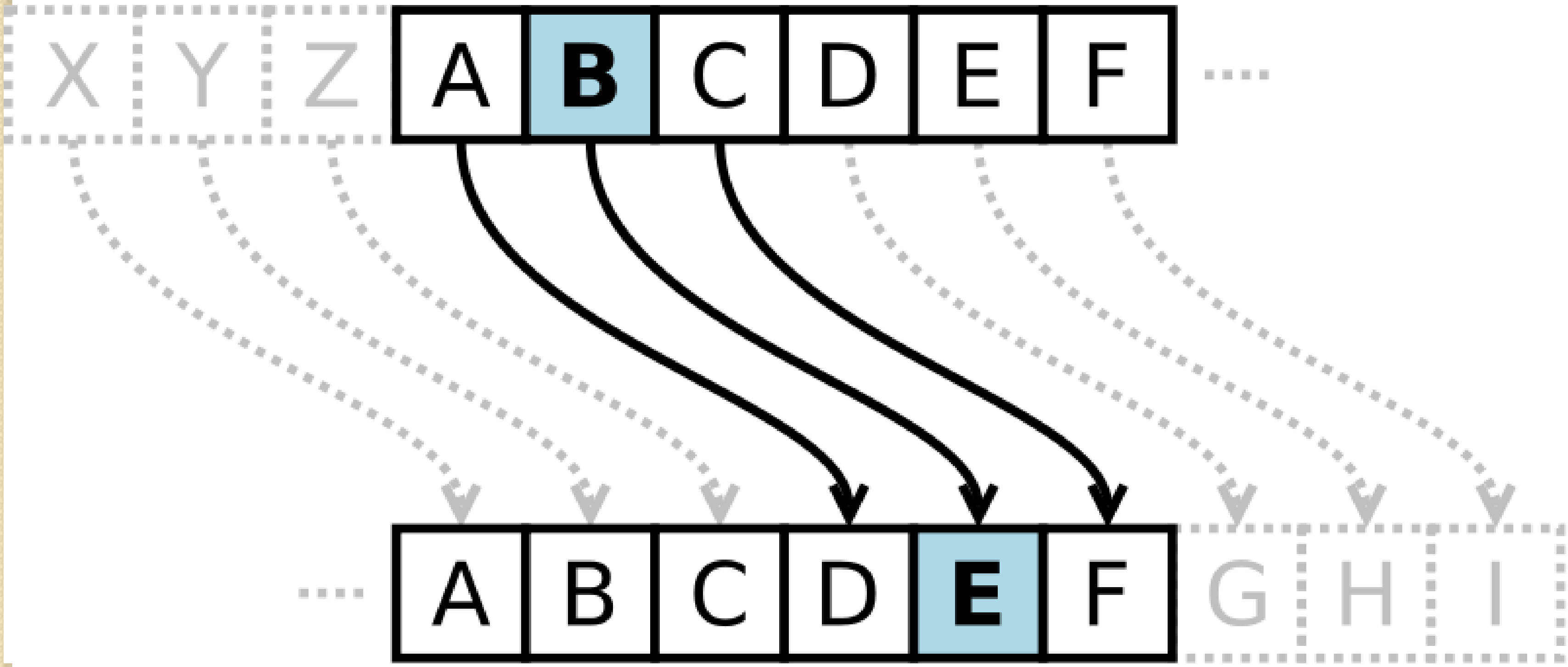
Historical Ciphers

- **Also called Substitution Techniques**

- **Monoalphabetic Cipher**
  - **Caesar Cipher**
- **Polyalphabetic Cipher**
  - **Vigenere Cipher**
  - **Hill Cipher**

Monoalphabetic Ciphers

- **Caesar cipher**



Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- More formally:
  - Encrypt(Letter, Key) = (Letter + Key) (mod 26)
  - Decrypt(Letter, Key) = (Letter - Key) (mod 26)
- Encrypt("NIKITA", 3) = "QLNLWD"
- Decrypt("QLNLWD", 3) = "NIKITA"

Example --

- D for A, E for B, …… A for X, B for Y, etc.

- Plaintext –
- WHAT IS THE POPULATION OF MARS

- Ciphertext ?

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Polyalphabetic Ciphers

- In this type, the cipher text corresponding to a particular character is not fixed. It may depend upon, for example, its position in the block.
- Vigenere Cipher
- Hill Cipher

Vigenere Cipher

- Uses multi digit key, k_1, k_2, k_3, …, k_m which are integers.
- Plaintext is split into non overlapping blocks, each contains m consecutive characters.
- The first letter of each block is replaced by the letter k_1 position to its right, the second letter by the k_2 position its right and so on.

Vigenere Cipher

- **Plain text**
- W I S H I N G Y O U S U C C E S S
- 04 19 03 22 07 12 05 11 04 19 03 22 07 12 05 11 04
- **Cipher text**
- A B V D P Y L J S N X F G V H O Z
- The first letter in plain text is W. The corresponding key is 04, means the cipher text is the letter 4 positions ahead.
- The key length is 8, means it repeats after every 8 characters.
- There are 4 occurrences of "s" letter.
- Each "s" is encrypted as different.