INFORMATION SECURITY

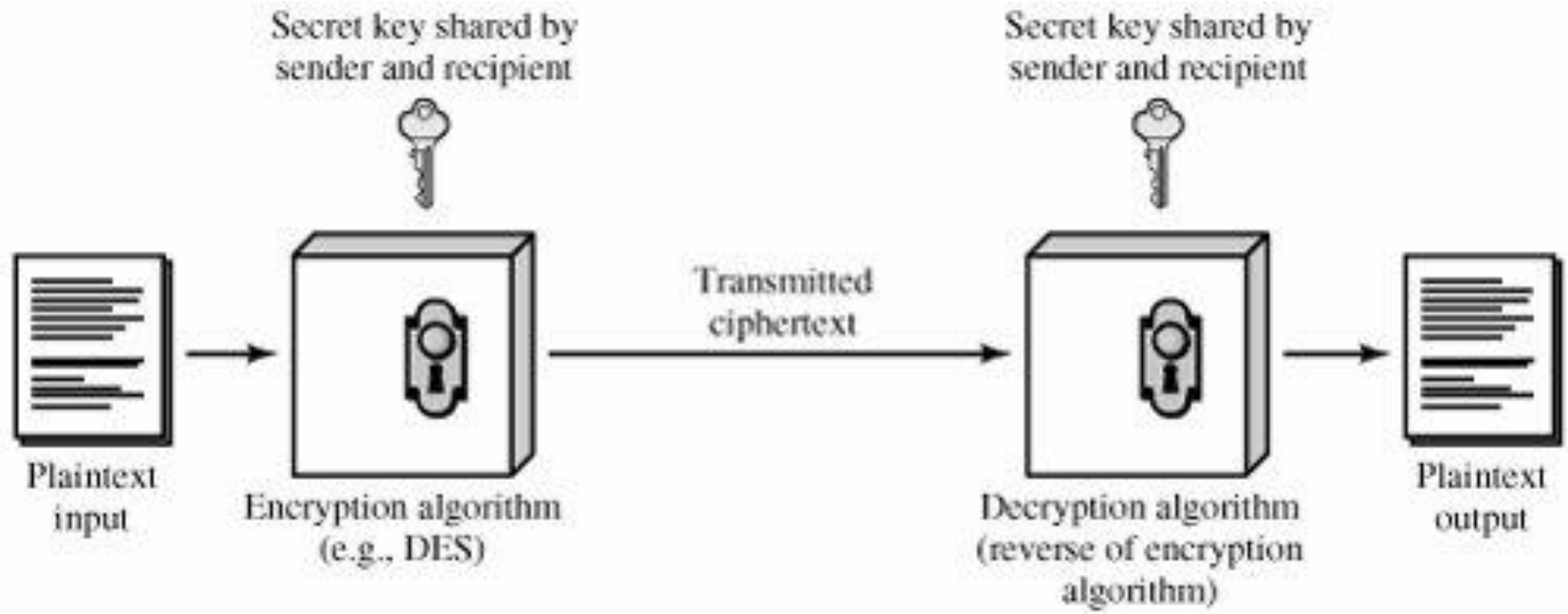
CRYPTOGRAPHY

-2-

By : Eman Talib Jasim

Department of Information Technology 2018-2019

Simple Symmetric Cryptography 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

- Terms
  - **Plain Text**
    - The original intelligible message or data that is fed to algorithm
  - **Encryption Algorithm**
    - Performs various substitution or transformation on the plain text

- **Secret key**
  - Input to encryption algorithm
  - Key value is independent of text & algorithm.
  - Algorithm will produce transformed/substitution output based on key.

- **Cipher text**
  - Is the scrambled message produced as output.
  - Depend on plain text and secret key
  - It seems to be a random stream of data and stands as unintelligible.

- There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

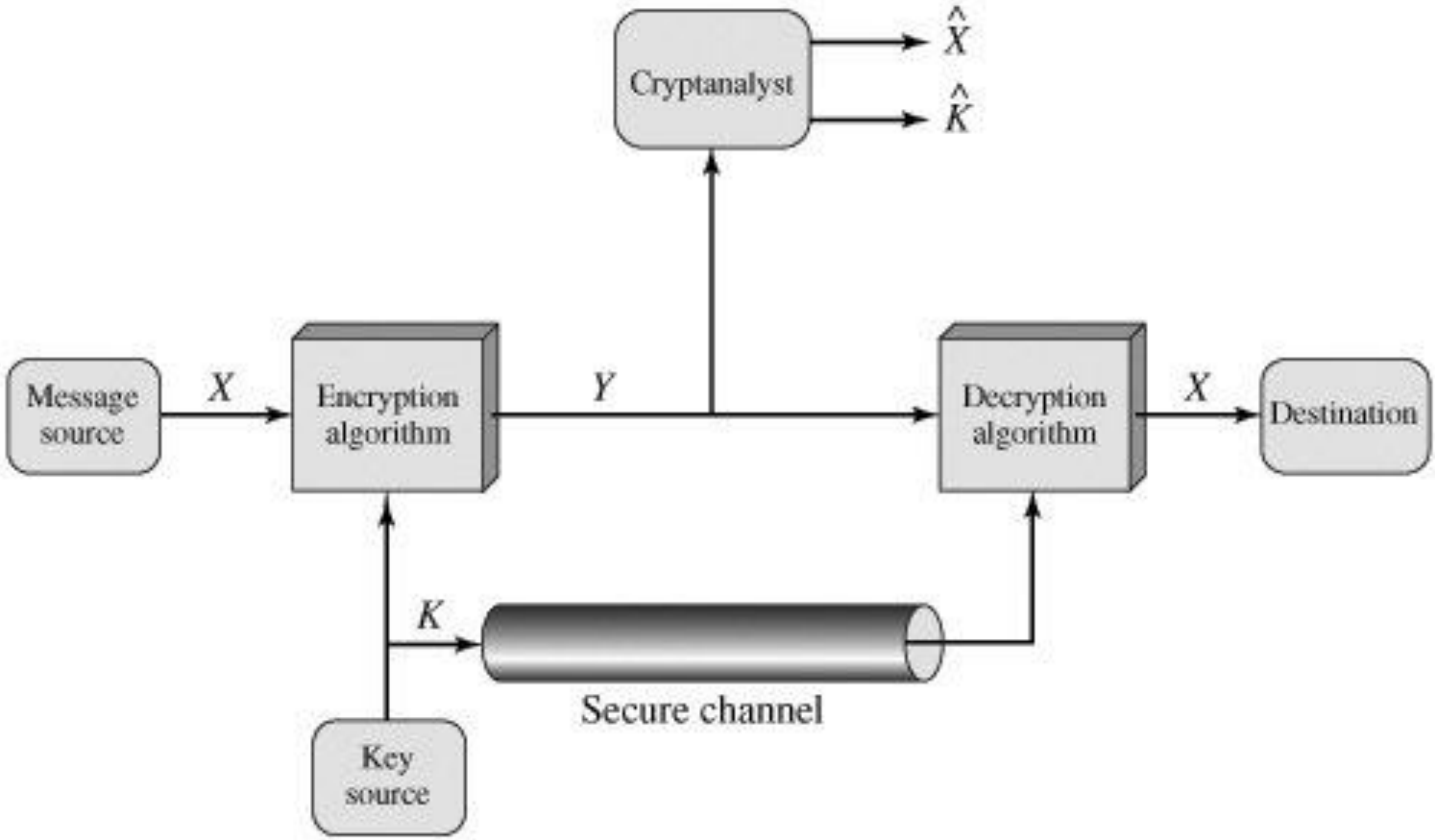
- Example:
  - Let ‘A’ be the source, produces a message in a plain text $X=[X_1,X_2,X_3....X_M]$, where M elements of X, are letter in some finite alphabets.
  - For Encryption a Key of the form $K=[K_1,K_2,K_3.....K_J]$ is generated.
  - With message X and encryption key K as input, the encryption algorithm forms the cipher text

$$Y=[Y_1,Y_{2,}Y_3...Y_N]$$

We can write as

$Y=E(K,X)$ → Encryption & $X=D(K,Y)$ → Decryption

Conventional Cryptosystem



- Cryptology
  - Is the area of cryptography and cryptanalysis used together.
- Cryptography
  - is the science of using mathematics to encrypt and decrypt data enables us to transmit message across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.**

a. Substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element.

b. Transposition, in which elements in the plaintext are rearranged.

2. **The number of keys used**. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. **The way in which the plaintext is processed**.

a. A block cipher processes the input one block of elements at a time, producing an output block for each input block.

- Cryptanalysis
  - Technique used for deciphering a message without any knowledge of enciphering text is called cryptanalysis

    “Breaking the Code”
  - To attack on encryption system to recover the key or recover plain text of cipher text.
  - Two Approaches
    - **Cryptanalysis**
      - This attack exploits the characteristics of algorithm to attempt to figure out a specific plain text or figure out the key .
    - **Brute-Force Attack**
      - The Attacker tries very possible on a piece of cipher text until an intelligible translation into plain text is obtained

Average Time required for exhaustive key search

Key size (bits)	Number of alternative keys		Time required at 1 decryption/ *m* s	
32	2^{32}	= 4.3 x 10^{9}	2^{31} *m* s	= 35.8 minutes
56	2^{56}	= 7.2 x 10^{16}	2^{55} *m* s	= 1142 years
128	2^{128}	= 3.4 x 10^{38}	2^{127} *m* s	= 5.4 x 10^{24}years
168	2^{168}	= 3.7 x 10^{50}	2^{167} *m* s	= 5.9 x 10^{36}years
	26!	= 4 x 10^{26}	2 x 10^{26} *ms*	= 6.4 x 10^{12}years

Secret key or Symmetric key cryptography

1- conventional system (classical)

A- substitution ciphers: A substitution cipher replaces one symbol with another.

- monoalphabetic ciphers :-

  1-Direct stander(caesar cipher)

  2- mono-alphabetic cipher

  3-Standared reverse cipher

  4-keyword mixed cipher

  5-multiplicative cipher

  6-Affine cipher

Secret key or Symmetric key cryptography

Polyalphabetic Cipher :

Each alphabetic character of a plaintext can be mapped onto m alphabetic characters of a ciphertext. Usually m is related to the encryption key.

1-Vigenere

2-Beaufort

Polygraphic ciphers:

a cipher that operates on larger groups of letters .

1-playfair

2-Hill cipher