

# CRYPTOGRAPHY

Dr. Shubhangi Sapkal

# Cryptography-Introduction

- Cryptography is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.
- In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.
- These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

# Cryptography-Introduction

Modern cryptography concerns itself with the following four objectives:

- **Confidentiality:** the information cannot be understood by anyone for whom it was unintended
- **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
- **Non-repudiation:** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
- **Authentication:** the sender and receiver can confirm each other's identity and the origin/destination of the information
- Procedures and protocols that meet some or all of the above criteria are known as cryptosystems.

# Cryptography

Cryptographic systems are characterized along three independent dimensions:

- 1. The type of operations used for transforming plaintext to ciphertext.** All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.
- 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 *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

# Features Of Cryptography

- **Confidentiality:**  
Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:**  
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:**  
The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:**  
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

# Types Of Cryptography

In general there are three types Of cryptography:

- **Symmetric Key Cryptography:**

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

- **Hash Functions:**

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

- **Asymmetric Key Cryptography:**

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

# Cryptographic algorithms

- Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices such as smartphones, and applications.
- A cipher suite uses one algorithm for encryption, another algorithm for message authentication, and another for key exchange.
- This process, embedded in protocols and written in software that runs on operating systems and networked computer systems, involves public and private key generation for data encryption/decryption, digital signing and verification for message authentication, and key exchange.



# Types of cryptography

- **Single key or symmetric key encryption** algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it. Types of symmetric-key cryptography include the Advanced Encryption Standard (AES), a specification established in November 2001 by the National Institute of Standards and Technology as a Federal Information Processing Standard (FIPS 197), to protect sensitive information. The standard is mandated by the U.S. government and widely used in the private sector.
- In June 2003, AES was approved by the U.S. government for classified information. It is a royalty-free specification implemented in software and hardware worldwide. AES is the successor of the Data Encryption Standard (DES) and DES3. It uses longer key lengths (128-bit, 192-bit, 256-bit) to prevent brute force and other attacks.

# Types of cryptography

- **Public-key or Asymmetric-key encryption** algorithms use a pair of keys, a public key associated with the creator/sender for encrypting messages and a private key that only the originator knows (unless it is exposed or they decide to share it) for decrypting that information. The types of public-key cryptography include RSA, used widely on the internet; Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin; Digital Signature Algorithm (DSA) adopted as a Federal Information Processing Standard for digital signatures by NIST in FIPS 186-4; and Diffie-Hellman key exchange.
- To maintain data integrity in cryptography, **hash functions**, which return a deterministic output from an input value, are used to map data to a fixed data size. Types of cryptographic hash functions include SHA-1 (Secure Hash Algorithm 1), SHA-2 and SHA-3.

# symmetric Cipher Model

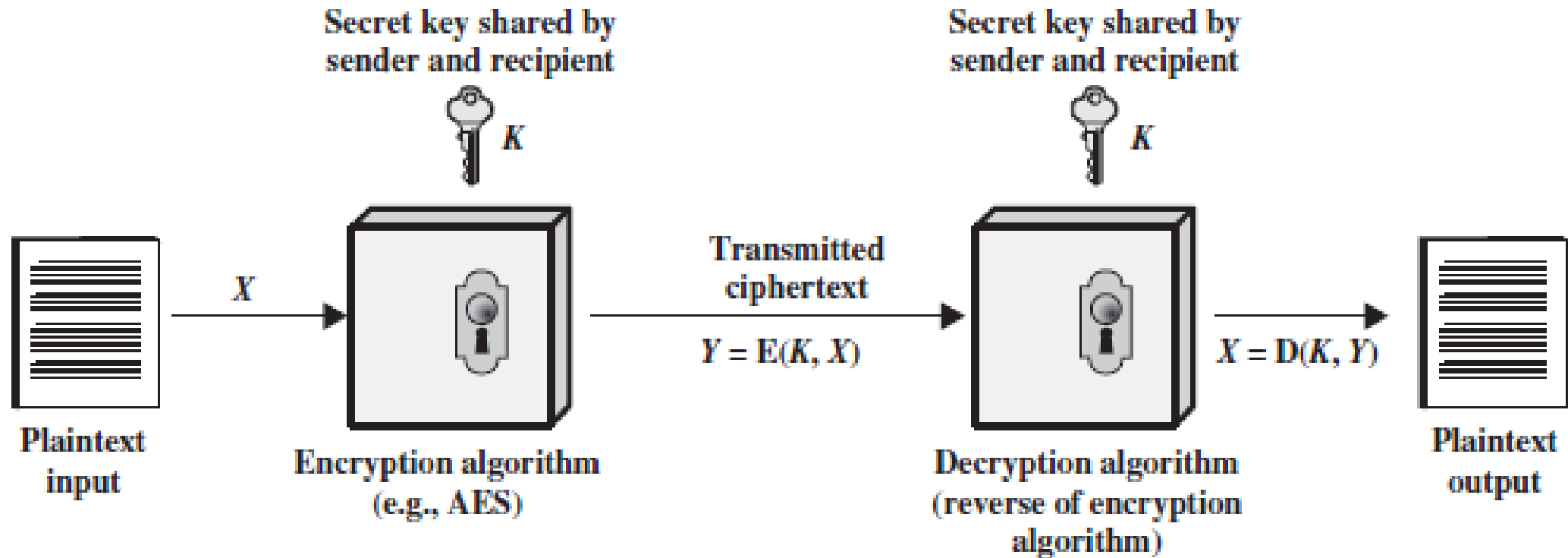


Figure 2.1 Simplified Model of Symmetric Encryption

# Symmetric Encryption

A symmetric encryption scheme has five ingredients

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

# Symmetric Encryption

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plain text and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

# Requirements of Encryption

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. This requirement is usually stated in a stronger form:

The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

**2. Sender and receiver must have obtained copies of the **secret key** in a secure fashion and must keep the key secure.** If someone can discover the key and knows the algorithm, all communication using this key is readable.

# Symmetric Encryption

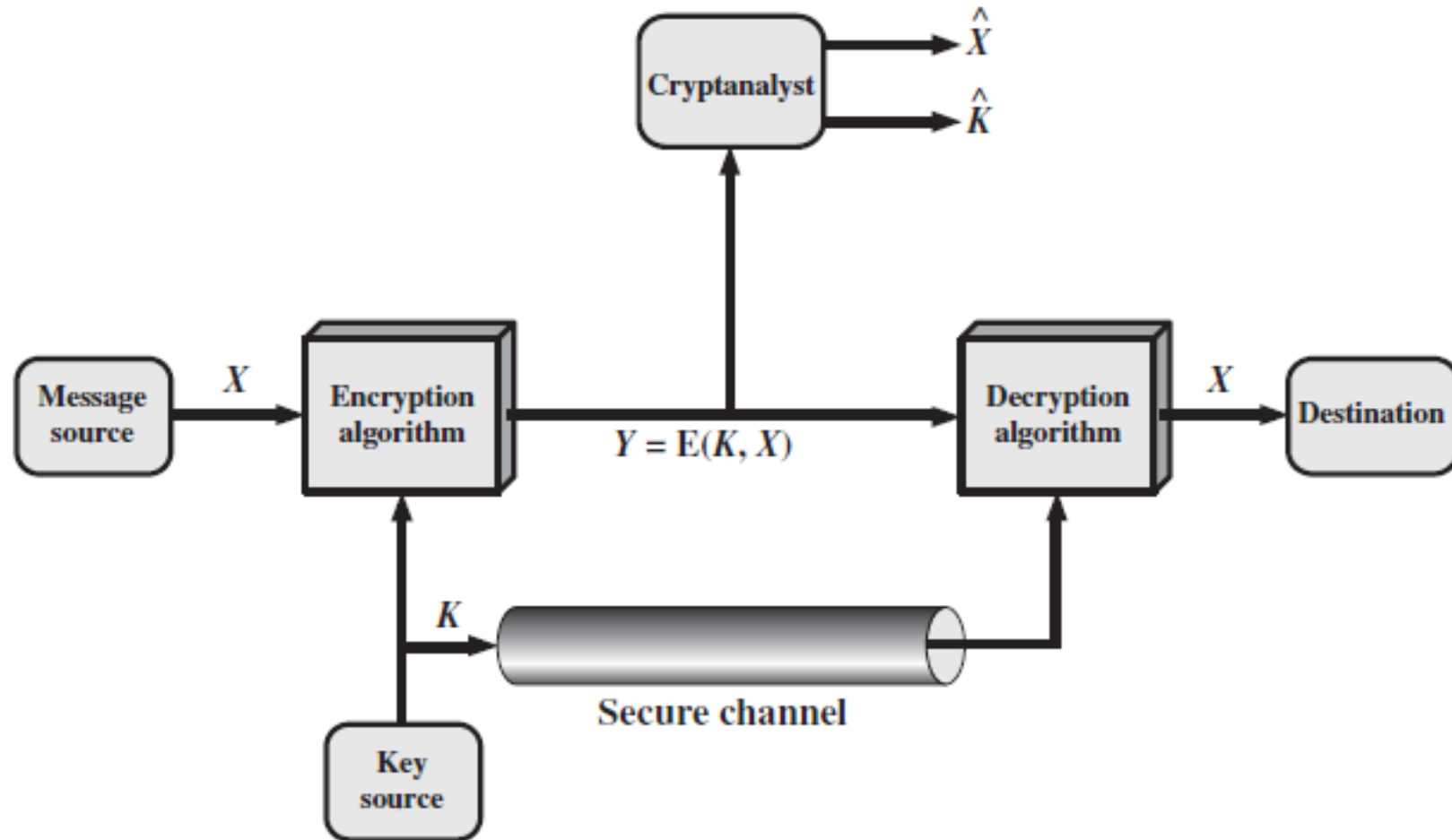


Figure 2.2 Model of Symmetric Cryptosystem

# Cryptanalysis and Brute-Force Attack

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.



# Cryptanalysis and Brute-Force Attack

An encryption scheme is said to be **computationally secure** if either of the two criteria are met.

1. The cost of breaking the cipher exceeds the value of the encrypted information.
2. The time required to break the cipher exceeds the useful lifetime of the information.