SECURITY

INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

SECURITY ATTACKS, SERVICES AND MECHANISMS

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- Security attack – Any action that compromises the security of information owned by an organization.
- Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.
- Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

SECURITY SERVICES

The classification of security services are as follows:

- **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
  Eg., printing, displaying and other forms of disclosure.
- **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

- **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- **Non repudiation**: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- **Access control**: Requires that access to information resources may be controlled by or the target system.
- **Availability**: Requires that computer system assets be available to authorized parties when needed.

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security.

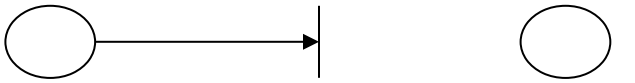
SECURITY ATTACKS

There are four general categories of attack which are listed below.

- **Interruption**

  An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.

  e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.

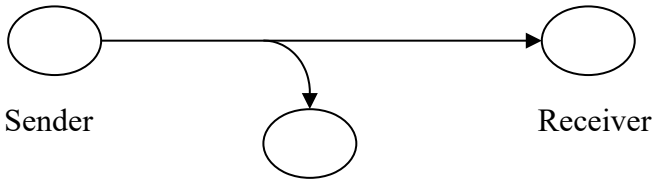


Sender Receiver

- **Interception**

  An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.

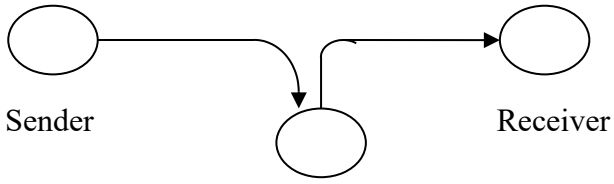
e.g., wire tapping to capture data in the network, illicit copying of files or programs.



- **Modification**

  An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.

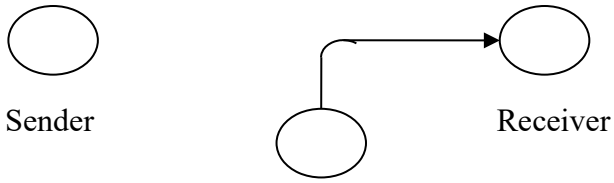
  e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



- **Fabrication**

  An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.

  e.g., insertion of spurious message in a network or addition of records to a file.



A useful categorization of these attacks is in terms of

- Passive attacks
- Active attacks

Passive attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

- Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.
- Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Active attacks

These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

- Masquerade – One entity pretends to be a different entity.

- Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
- Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Symmetric and public key algorithms

Encryption/Decryption methods fall into two categories.

- Symmetric key
- Public key

In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

CONVENTIONAL ENCRYPTION MODEL

Conventional encryption also referred to as symmetric encryption or single key encryption was the only type of encryption in use prior to the development of public key encryption.

Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be

transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

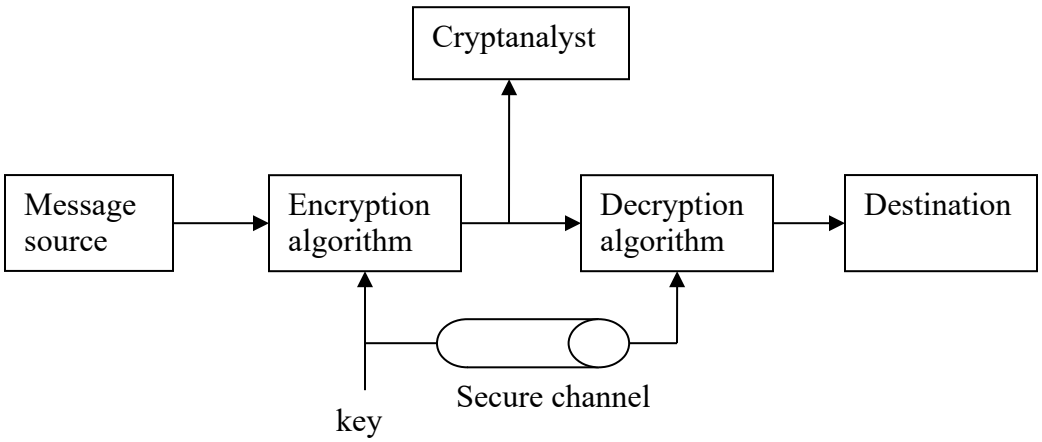


Figure: conventional cryptosystem

A source produces a message in plaintext, X = [X1, X2, … , XM] where M are the number of letters in the message. A key of the form K = [K1, K2, …, KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, …, YN]. This can be expressed as

$$Y = E_K(X)$$

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D_K(Y)$$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms. If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if the

opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate.

PRINCIPLES OF PUBLIC KEY CRYPTOGRAPHY

The concept of public key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption.

- Key distribution under symmetric key encryption requires either (1) that two communicants already share a key, which someone has been distributed to them or (2) the use of a key distribution center.
- Digital signatures.

Public key cryptosystems

Public key algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristics:

- It is computationally infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and the encryption key.

In addition, some algorithms, such as RSA, also exhibit the following characteristic:

- Either of the two related keys can be used for encryption, with the other used for decryption.

The essential steps are the following:

- Each user generates a pair of keys to be used for encryption and decryption of messages.
- Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private.
- If A wishes to send a confidential message to B, A encrypts the message using B's public key.
- When B receives the message, it decrypts using its private key. No other recipient can decrypt the message because only B knows B's private key.

With this approach, all participants have access to public keys and private keys are generated locally by each participant and therefore, need not be distributed. As long as a system controls its private key, its incoming communication is secure.

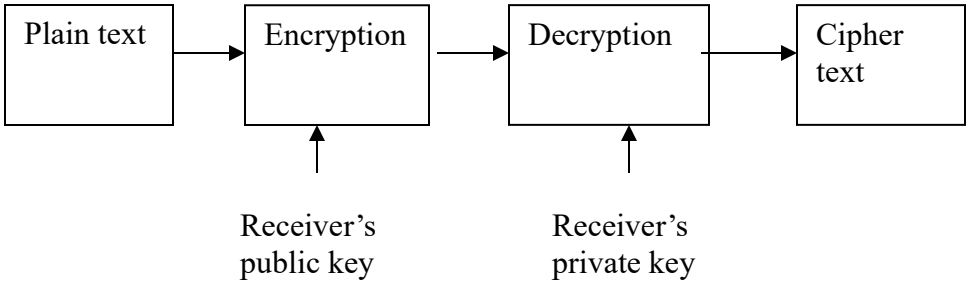


Fig: encryption

Let the plaintext be X=[X1, X2, X3, …,Xm] where m is the number of letters in some finite alphabets. Suppose A wishes to send a message to B. B generates a pair of keys: a public key KU_b and a private key KR_b. KR_b is known only to B, whereas KU_b is publicly available and therefore accessible by A.

With the message X and encryption key KU_b as input, A forms the cipher text Y=[Y1, Y2, Y3, … Yn].

$$\text{i.e., } Y = E\ KU_b(X)$$

The receiver can decrypt it using the private key KR_b.

$$\text{i.e., } X = D\ KR_b()$$

The other approach (using sender's private key for encryption and sender's public key for decryption) will provide authentication which is illustrated in the following diagram.

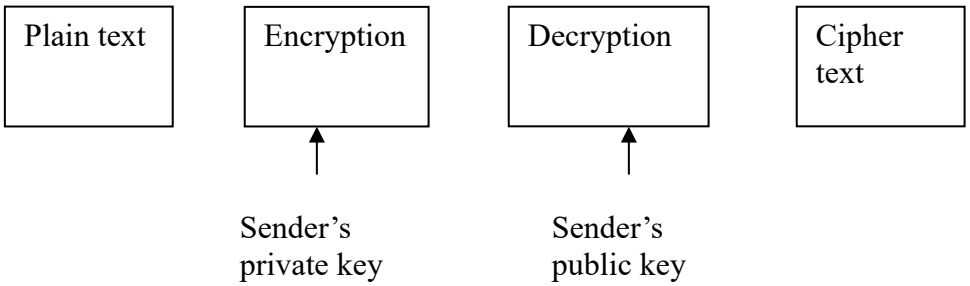


Fig: authentication

The encrypted message serves as a **digital signature.**

It is important to emphasize that the encryption process just described does not provide confidentiality. There is no protection of confidentiality because any observer can decrypt the message by using the sender's public key.

It is however, possible to provide both the authentication and confidentiality by a double use of the public scheme.

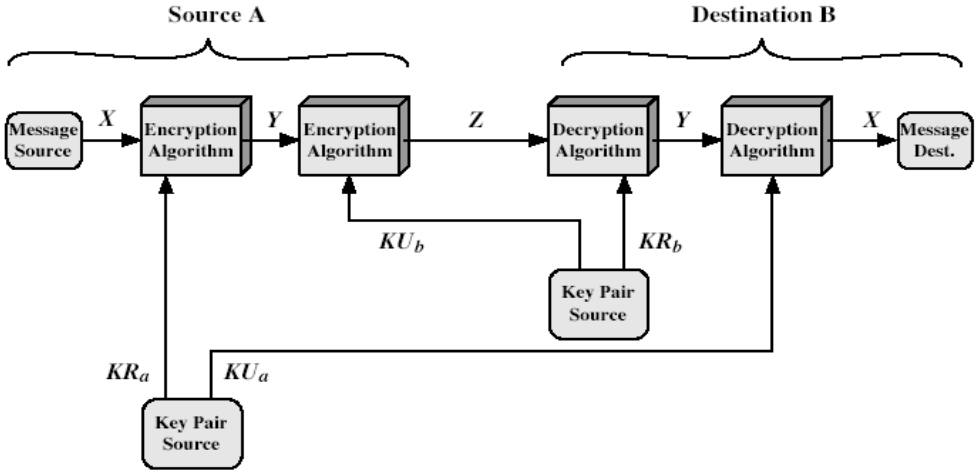


Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

Ciphertext $Z = EKU_b [EKR_a (X)]$

Plaintext $X = EKU_a [EKR_b (Y)]$

Initially, the message is encrypted using the sender's private key. This provides the digital signature. Next, we encrypt again, using the receiver's public key. The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus confidentiality is provided.