# CRYPTOGRAPHY AND NETWORK SECURITY

## UNIT-I

## Introduction

To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).

Until a few decades ago, the information collected by an organization was stored on physical files. The confidentiality of the files was achieved by restricting the access to a few authorized and trusted people in the organization.

In the same way, only a few authorized people were allowed to change the contents of the files. Availability was achieved by designating at least one person who would have access to the files at all times.

With the advent of computers, information storage became electronic. Instead of being stored on physical media, it was stored in computers. The three security requirements, however, did not change. The files stored in computers require confidentiality, integrity, and availability. The implementation of these requirements, however, is different and more challenging.

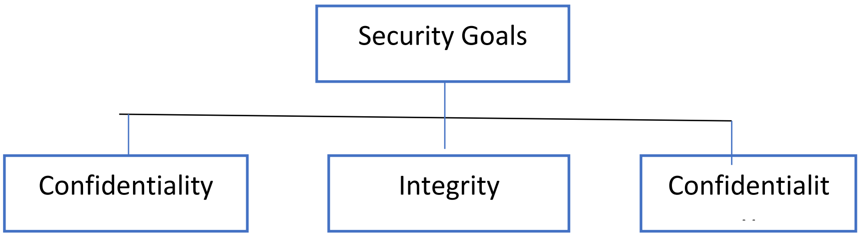
During the last two decades, computer networks created a revolution in the use of information. Information is now distributed. Authorized people can send and retrieve information from a distance using computer networks.

Although the three above-mentioned requirements confidentiality, integrity, and availability have not changed, they now have some new dimensions. Not only should information be confidential when it is stored in a computer; there should also be a way to maintain its confidentiality when it is transmitted from one computer to another.

we first discuss the three major goals of information security. We then see how attacks can threaten these three goals. We then discuss the security services in relation to these security goals. Finally, we define mechanisms to provide security services and introduce techniques that can be used to implement these mechanisms.

## 1.1. SECURITY GOALS

Let us first discuss three security goals: confidentiality, integrity, and availability



### Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information. In the military, concealment of sensitive information is the major concern. In industry, hiding some information from competitors is crucial to the operation of the organization. In banking, customers' accounts need to be kept secret. Confidentiality not only applies to the storage of the information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.

### Integrity

Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information.

### Availability

The third component of information security is availability. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.

## 1.2. ATTACKS

Our three goals of security, confidentiality, integrity, and availability can be threatened by security attacks. Although the literature uses different approaches to categorizing the attacks, we will first divide them into three groups related to the security goals. Later, we will divide them into two broad categories based on their effects on the system.

### Attacks Threatening Confidentiality

In general, two types of attacks threaten the confidentiality of information: snooping and traffic analysis.

**Snooping**

Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit. To prevent snooping, the data can be made non intelligible to the interceptor by using encipherment techniques.

**Traffic Analysis**

Although encipherment of data may make it non intelligible for the interceptor, she can obtain some other type information by monitoring online traffic. For example, she can find the electronic address (such as the e-mail address) of the sender or the receiver. She can collect pairs of requests and responses to help her guess the nature of transaction.

Attacks Threatening Integrity

The integrity of data can be threatened by several kinds of attacks: modification, masquerading, replaying, and repudiation.

**Modification**

After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself. For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit herself. Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

### Masquerading

Masquerading, or spoofing, happens when the attacker impersonates somebody else. For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer. Sometimes the attacker pretends instead to be the receiver entity. For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

### Replaying

Replaying is another attack. The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

### Repudiation

This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request. An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

## Attacks Threatening Availability

We mention only one attack threatening availability: denial of service.

### Denial of Service

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and delete a server’s response to a client, making the client to believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

Passive Versus Active Attacks, let us now categorize the attacks into two groups: passive and active.

**Passive Attacks**

In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system. The system continues with its normal operation. However, the attack may harm the sender or the receiver of the message. Attacks that threaten confidentiality snooping and traffic analysis are passive attacks. The revealing of the information may harm the sender or receiver of the message, but the system is not affected. For this reason, it is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential information. Passive attacks, however, can be prevented by encipherment of the data.

**Active Attacks**

An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

## 1.3. SECURITY SERVICES AND MECHANISMS

**International Telecommunication Union-Telecommunication Standardisation Sector (ITU-T)** is a standards organisation. It deals with the creation of standards for data telecommunication with additional focus on voice as well as data communications. The standards set by this organisation are named X.800. Under X800, we have **security services** (related to security goals and attacks) and **security mechanisms** to achieve these services. One security service may be served by one or more security mechanisms. Similarly, one mechanism may provide one or more security services.

### 1.3.1 Security services

ITU-T (X.800) has identified five security service categories, classified into 14 security services. Let us summarise the X.800 security services as follows:

- **Authentication**: This provides an assurance that the communicating party is really who it claims to be. This is divided into two types:
    - Peer entity authentication: In a logical connection, this provides a guarantee regarding the identity of the connected entities

    - Data origin authentication: This takes the form of authenticating the source of data in a connectionless data transfer.
- **Access control**: Here, the aim is to prevent an unauthorised access of a resource.
- **Data confidentiality**: This feature stops unauthorised disclosure of information. It is classified into four services:
    - Connection confidentiality: Here, the aim is to protect all the users on a connection.
    - Connectionless confidentiality: When we want to protect all the data in a single data block, we use this service.
    - Selective field confidentiality: Here, we wish to protect certain blocks of user data in a connection
    - Traffic flow confidentiality: This involves observation of the traffic flows to protect user data.
- **Data integrity**: Here, the aim is to ensure that data was received at the receiver exactly as it was sent by the sender, without any alterations. Five services are provided under this, as follows:
    - Connection integrity with recovery: Takes care of the integrity for all the users on a single connection. If there is a loss of integrity, recovery is attempted.
    - Connection integrity without recovery: Takes care of the integrity for all the users on a single connection. If there is a loss of integrity, recovery is not attempted
    - Selective field connection recovery: Here, the integrity of all the data in a user data block is ensured. If there is a loss of integrity, recovery is attempted.
    - Connectionless integrity. Useful for data integrity of a single connectionless data block.
    - Selective field connectionless integrity: Unlike a whole connection, data in a certain data block is checked for integrity.
- Non repudiation: Prevents the denial of one of the participants in communication. This is divided into two services:
    - Non repudiation, Origin: This is a proof that a particular message was indeed sent by a particular sender and not anyone else.

  - Non repudiation, Destination: This is a proof that a particular message was indeed received
    by a particular receiver.

**1.5.2 Security mechanisms**

ITU-T (X,800) specifies security mechanisms. Let us briefly describe these security mechanisms:

- **Encipherment: Encipherment** means hiding data. Hence, this takes care of *confidentiality*. The techniques of cryptography and steganography can be used to achieve encipherment.
- **Data integrity:** To achieve **data integrity**, a short extract of the original data is computed by using a specific mechanism and this extract is appended to the original data. Any change in the original data or extract invalidates the other, and therefore, signals loss of data integrity.
- Digital signature: In a digital signature mechanism, the sender of a message electronically signs the message in such a way that no one else can duplicate this signature, but can validate it.
- Authentication exchanges: When two parties need to prove their identity to each other, they perform an authentication exchange. Here, some secrets only known to these parties are exchanged to establish this proof.
- Traffic padding: A technique known as traffic analysis is performed by attackers to guess the secret data being exchanged between two parties. To defeat this attack, some junk data called as traffic padding is deliberately introduced in the original data by the sender.
- Routing control: Sometimes, attackers attack the connection/line/route of the messages being exchanged. To prevent such attacks, the communicating parties can select and continuously change the route. This mechanism is called as routing control.
- Notarisation: A trusted third party is involved to ensure trust between the communicating parties, so that they feel secure about their communication. This process is called as notarisation.

- Access control: The mechanism of access control ensures that the authorised users are permitted to carry out appropriate transactions or have access to the designated resource. Unauthorised users are not permitted to do so.

## 1.4. MATHEMATICS OF CRYPTOGRAPHY

Cryptography is based on some specific areas of mathematics, including number theory, linear algebra, and algebraic structures.

### 1.4.1. PRIME NUMBERS

**Factoring**

Prime numbers are very important in cryptography. A prime number is a positive integer, greater than 1. whose only factors are 1 and itself. That is, a prime number cannot be divided by any number other than 1 and itself. It should be obvious that 2, 3, 5.7. 11.... are prime numbers and 4, 6, 8, 10, 12... are not. There are an infinite number of prime numbers. Cryptography uses prime numbers heavily. Especially public key cryptography has its roots in prime number theory.

Two numbers are relatively prime when they have no factors in common other than 1. If the Greatest Common Divisor (GCD) of *a* and *n* is 1, it is written as *gcd (a, n) = 1*. As we will note, the numbers 21 and 44 are relatively prime (because they have no factors in common), but the numbers 21 and 45 are not (because they have a factor 3 in common).

### 1.4.2 Modular Arithmetic and Discrete Logarithms

**Modular arithmetic** is based on simple principles: Module is the remainder left after an integer division. For example, 23 mod 11= 12, because 12 is the remainder of the division 23/11. Modular arithmetic then says that 23 and 11 are equivalent. That is, 23 = 11 (mod 12). In general, a o b (mod n) if a = b + kn for some integer k.

If a > 0 and 0<b<n, then b is the remainder of the division a / n. Other names for these are: **residue** for b and **congruent** for a. The triple equal to sign (º) denotes **congruence**. Cryptography uses computation mod n very frequently.

Modular exponentiation is a one-way function used in cryptography. Solving it is easy. For example. Consider

$a^x$ (mod n), given the values of a, x and n. It is quite simple to solve. However, the inverse problem of mod exponentiation is that of finding the discrete logarithm of a number. This is quite tough. For instance, find x where $a^x$ = b (mod n). As an example, if $3^{x\,o}$ 15 (mod 17), then x=6. For large numbers, solving this equation is quite difficult.

**1.4.3 Square Roots Modulo a Prime**

If n is the result of the multiplication of two prime numbers, then the ability to find out the square root mod n is equivalent to the ability of factoring n. That is, if we know the prime factors of n. then we can easily calculate the square roots of a number mod n.