**VISION INSTITUTE OF MANAGEMENT**

**COMPUTER NETWORK SECURITY**

**BCA 3rd YEAR(6th SEM)**

**UNIT-1(Introduction & Cryptography)**

**Computer Network Security-**

Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

## Aspects of Network Security:

Following are the desirable properties to achieve secure communication:



* **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
* **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
* **End-point authentication:** Authentication means that the receiver is sure of the sender?s identity, i.e., no imposter has sent the message.
* **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

**Security Attacks:**

**Active attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

1. **Masquerade –**
Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other forms of active attacks.

****

1. **Modification of messages –**
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.



1. **Repudiation –**
This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.
2. **Replay –**
It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



1. **Denial of Service –**
It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruptions of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



**Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content –**

Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



1. **Traffic analysis –**

Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



**Computer Network Security Services:**



## Message confidentiality-

• It means that the content of a message when transmitted across a network must remain confidential, *i.e.*only the intended receiver and no one else should be able to read the message.

• The users; therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

## Message Integrity-

• It means the data must reach the destination without any adulteration *i.e.*exactly as it was sent.

• There must be no changes during transmission neither accidentally nor maliciously.

• Integrity of a message is ensured by attaching a checksum to the message.

• The algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

## Message Authentication-

## **In**message authentication the receiver needs to be .sure of the sender's identity *i.e.*the receiver has to make sure that the actual sender is the same as claimed to be.

## There are different methods to check the genuineness of the sender:

1. The two parties share a common secret code word. A party is required to show the secret code word to the other for authentication.
2. Authentication can be done by sending digital signature.
3. A trusted third party verifies the authenticity. One such way is to use digital certificates issued by a recognized certification authority.

## 4. Message non-reproduction-

• Non-repudiation means that a sender must not be able to deny sending a message that it actually sent.

• The burden of proof falls on the receiver.

• Non-reproduction is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent.

• Non-repudiation is achieved by authentication and integrity mechanisms.

## 5. Entity Authentication-

• In entity authentication (or user identification) the entity or user is verified prior to access to the system resources.

**Computer Network Security Mechanisms:**

****

## ****Relation between security services and mechanisms:****

****

**A Model For Internetwork Security:**

****

* A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
* Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
* A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.



Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application pro-grams as well as utility programs, such as editors and compilers. Programs can pre-sent two kinds of threats:

1. **Information access threats:**Intercept or modify data on behalf of users whoshould not have access to that data.
2. **Service threats:**Exploit service flaws in computers to inhibit use by legitimateusers.

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.5). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

**Cryptography:**

**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

**Cryptography** is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it



Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

 2. Hash functions.

3. Public-key cryptography

**Symmetric-key Cryptography:** Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

**Public-Key Cryptography:** This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

**Hash Functions:**No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

**Notion of Plain text:**

* *Plaintext* is a term used in cryptography that refers to a [message](http://www.linfo.org/message.html) before *encryption* or after *decryption*. That is, it is a message in a form that is easily readable by humans.
* Encryption is the process of obscuring messages to make them unreadable in the absence special knowledge. It is usually done for secrecy, and typically for confidential communications. It can also be used for [*authentication*](http://www.linfo.org/authentication.html) (i.e., the process of confirming the identity of an individual or a transmission). Decryption is the opposite, i.e., the conversion of encrypted data into plaintext. *Ciphertext* is a message after encryption or before decryption.
* Plaintext should not be confused with [*plain text*](http://www.linfo.org/plain_text.html). The latter refers to text consisting entirely of [*characters*](http://www.linfo.org/character.html) (e.g., those of an [alphabet](http://www.linfo.org/alphabet.html)) that are used in some written human language, as contrasted with sequences of [bits](http://www.linfo.org/bit.html) that do not represent human readable characters. Plaintext is written in plain text.
* Plain text can consist of plaintext and/or ciphertext. Plaintext, because it consists of human-readable characters, is a type of plain text. Ciphertext can be written as plain text or in any other form.
* Plaintext is encrypted into ciphertext using a cipher [*algorithm*](http://www.linfo.org/algorithm.html). An algorithm is a set of precise and unambiguous rules that specify how to solve some problem or perform some task. Examples of plaintext [information](http://www.linfo.org/information.html) that is usually encrypted prior to transmission over a [network](http://www.linfo.org/network.html) are financial transactions and diplomatic messages.

**Encryption and Decryption:**

**Encryption** is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

The major distinction between secret writing associated secret writing is that secret writing is that the conversion of a message into an unintelligible kind that’s undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.

****

**Key:**

## A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. ... A key is a part of the variable data that is provided as input to a cryptographic algorithm to execute this sort of operation.

* **Symmetric Key Encryption:**
[Encryption](https://www.geeksforgeeks.org/encryption-its-algorithms-and-its-future/) is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.
* **Asymmetric Key Encryption:**
Asymmetric Key Encryption is based on public and private key encryption technique. It uses two different key to encrypt and decrypt the message. It is more secure than symmetric key encryption technique but is much slower.

**Cipher Text:**

In cryptography, cipher text (ciphertext) is data that has been [encrypted](https://www.webopedia.com/TERM/E/encryption.html). Cipher text is unreadable until it has been converted into [plain text](https://www.webopedia.com/TERM/P/plain_text.html) (decrypted) with a [key](https://www.webopedia.com/TERM/K/key.html).

**OR**

**Ciphertext** is **encrypted** text. Plaintext is what you have before **encryption**, and **ciphertext** is the **encrypted** result. The term **cipher** is sometimes used as a synonym for **ciphertext**, but it more properly means the method of **encryption** rather than the result.

**Cryptanalysis:**

**Cryptanalysis** is the investigation of systems, ciphertext, and ciphers in order to reveal the hidden meaning or details of the system itself. The goal of this type of study is to discover the hidden aspects even if the key or main algorithm is unable to be deciphered.

**OR**

**Cryptanalysis** is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

**Cryptanalysis attack types include:**

1. **Known-Plaintext Analysis (KPA):** Attacker decrypts ciphertext with known partial plaintext.
2. **Chosen-Plaintext Analysis (CPA):** Attacker uses ciphertext that matches arbitrarily selected plaintext via the same algorithm technique.
3. **Ciphertext-Only Analysis (COA):** Attacker uses known ciphertext collections.
4. Man-in-the-Middle (MITM) Attack: Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actually compromised. Attacker employs this attack for the interception of messages that pass through the communications channel. Hash functions prevent MITM attacks.
5. **Adaptive Chosen-Plaintext Attack (ACPA):** Similar to a CPA, this attack uses chosen plaintext and ciphertext based on data learned from past encryptions.

**Public Key encryption:**

**Public**-**key encryption** is a cryptographic system that uses two **keys** -- a **public key** known to everyone and a **private** or secret **key** known only to the recipient of the message. Example: When John wants to send a **secure** message to Jane, he uses Jane's **public key** to **encrypt** the message.



# Digital Signature:

The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

## Signing the Whole Document-

* In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
* In Digital Signature, the private key is used for encryption while the public key is used for decryption.
* Digital Signature cannot be achieved by using secret key encryption.



### Digital Signature is used to achieve the following three aspects:

* **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
* **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.
* **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.

## Signing the Digest:

* Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
* The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
* The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
* The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.
* A hash function must have two properties to ensure the success:
	+ First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
	+ Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

### Following are the steps taken to ensure security:

* The miniature version (digest) of the message is created by using a hash function.
* The digest is encrypted by using the sender's private key.
* After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
* The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.



****

## Public Key Cryptography:

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

**The most important properties of public key encryption scheme are −**

* Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
* Each receiver possesses a unique decryption key, generally referred to as his private key.
* Receiver needs to publish an encryption key, referred to as his public key.
* Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
* Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
* Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

The process of encryption and decryption is depicted in the following illustration –



**RSA Algorithm-**

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

## Algorithm

**The RSA algorithm holds the following features** −

* RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
* The integers used by this method are sufficiently large making it difficult to solve.
* There are two sets of keys in this algorithm: private key and public key.

**You will have to go through the following steps to work on RSA algorithm –**

### Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown –

N=p\*q

Here, let N be the specified large number.

### Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1.

### Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

### Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows –

 ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

## Encryption Formula:

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

 C = Pe mod n

## Decryption Formula:

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver**C** has the private key **d**, the result modulus will be calculated as −

 Plaintext = Cd mod n