Unit 1

Introduction to Cryptography

Cryptography

Cryptography is 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 is known as cryptography. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

1. 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.
2. 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.
3. Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.
4. 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.
5. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.
6. Cryptography is the science to encrypt and decrypt data that enables the users to store sensitive information or transmit it across insecure networks so that it can be read only by the intended recipient.
7. Data which can be read and understood without any special measures is called **plaintext**, while the method of disguising (cover up) plaintext in order to hide its substance is called **encryption**.
8. Encrypted plaintext is known as cipher text and process of reverting the encrypted data back to plain text is known as **decryption**.
9. The science of analysing and breaking secure communication is known as cryptanalysis. The people who perform the same also known as attackers.
10. Cryptography can be either strong or weak and the strength is measured by the time and resources it would require to recover the actual plaintext.
11. Hence an appropriate decoding tool is required to decipher the strong encrypted messages.
12. As the computing power is increasing day by day, one has to make the encryption algorithms very strong in order to protect data and critical information from the attackers.

Computer security

Computer security is the protection that is set up for computer systems and keeps critical information from unauthorized access, theft, or misuse. *It is the process of preventing and detecting unauthorized use of our computer system.* **Computer security** can be defined as

controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. The components of a computer system that needs to be protected are:

- *Hardware,* the physical part of the computer, like the system memory and disk drive
- *Firmware,* permanent software that is etched into a hardware device's non-volatile memory and is mostly invisible to the user
- *Software,* the programming that offers services, like operating system, word processor, internet browser to the user

Computer Security Challenges :

1. Security is not simple it requires a lot of research and money
2. Potential attacks on the security features need to be considered.
3. Procedures used to provide particular services are often counter-intuitive.
4. It is necessary to decide where to use the various security mechanisms.
5. Requires constant monitoring.
6. Security mechanisms typically involve more than a particular algorithm or protocol.
7. Security is essentially a battle of wits (intelligence) between a perpetrator (person who carries out a harmful, illegal, or immoral act.) and the designer.
8. Little benefit from security investment is perceived until a security failure occurs.
9. Strong security is often viewed as obstacle to efficient and user-friendly operation

Information Security

It is not only about securing information from unauthorized access. It is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like our details or we can say our profile on social media, our data in mobile phone, our biometrics etc. Thus, Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

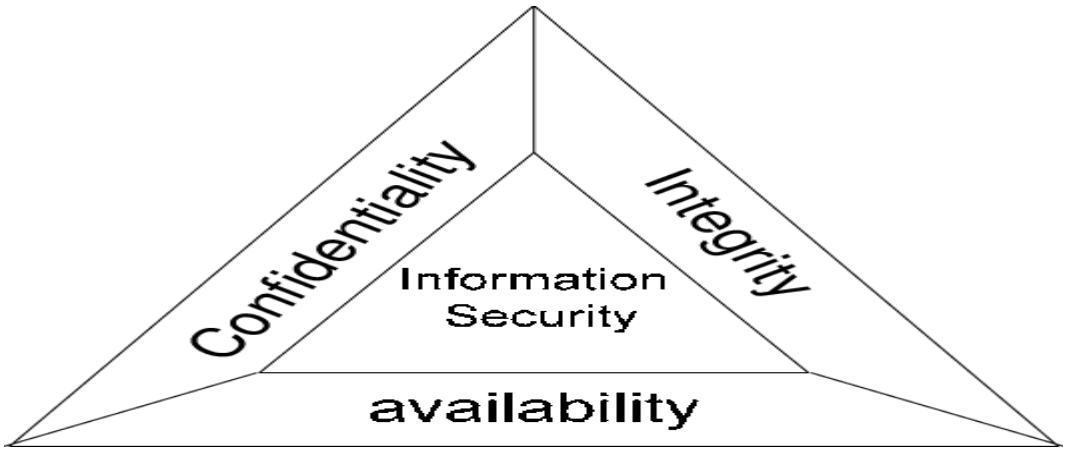
Network security

It is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.

CIA Triad

The CIA Triad is a well-known, venerable (respected) model for the development of security policies used in identifying problem areas, along with necessary solutions in the arena of information security.



In the information security (InfoSec) community, “CIA” has nothing to do with a certain well-recognized US intelligence agency. These three letters stand for confidentiality, integrity, and availability, otherwise known as the CIA triad.

Confidentiality

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached (break).

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and UNIX file permissions.

Integrity

Data integrity is what the "I" in CIA Triad stands for. This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability

This is the final component of the CIA Triad and refers to the actual availability of our data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it is available when it is needed.

High availability systems are the computing resources that have architectures that are specifically designed to improve availability. Based on the specific system design, this may target hardware failures, upgrades or power outages to help improve availability, or it may manage several network connections to route around various network outages.

Security Goals

A security goal is a statement of the following form:

The system shall prevent/detect *action* on/to/with *asset*.

For example, "the system shall prevent theft of money" and "the system shall prevent erasure of account balances." Each goal should relate to confidentiality, integrity, or availability, hence security goals are a kind of security property.

Note that security goals specify **what** the system should prevent, not **how** it should accomplish that prevention. Statements like "the system shall use encryption to prevent reading of messages" and "the system shall use authentication to verify user identities" are not good security goals. These are implementation details that should not appear until later in the software engineering process. Similarly, "the system shall resist attacks" is not a good security goal, because it fails to specify what in particular needs prevention.

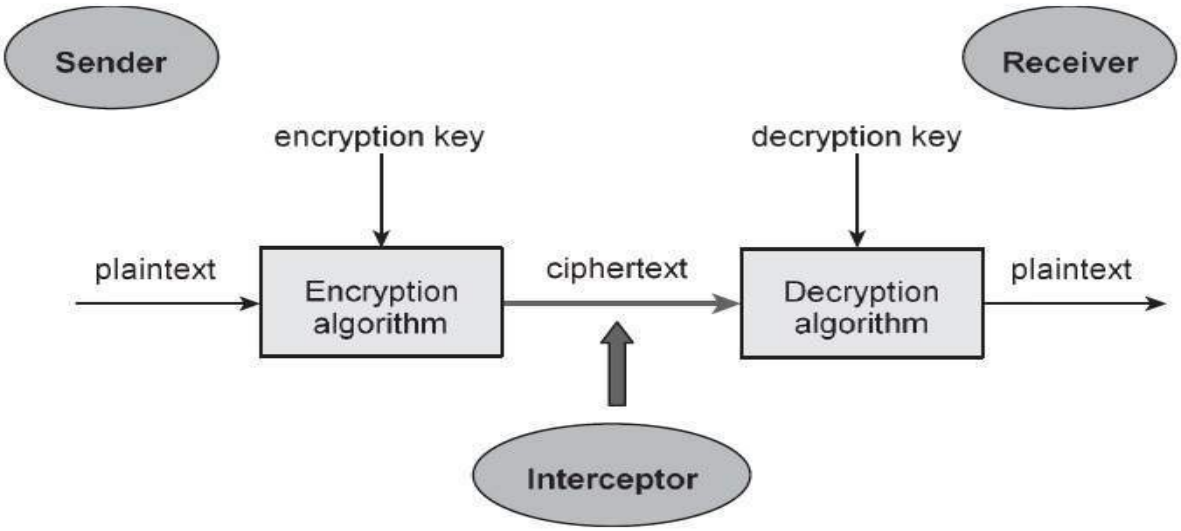
In reality, not all security goals are feasible to achieve. When designing a vault, we might want to prevent theft of money. But, no system can actually do that against a sufficiently motivated, resourceful, and capable threat. So we need to perform a *feasibility analysis* of security goals in light of the threats to the system.

Cryptosystems

1. A cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext to encode or decode messages securely.
2. The term “cryptosystem” is shorthand for “cryptographic system” and refers to a computer system that employs cryptography, a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.
3. To help keep data secure, cryptosystems incorporate the algorithms for key generation, encryption and decryption techniques.

4. At the heart of cryptographic operations is a cryptographic key, a string of bits used by a cryptographic algorithm to transform plain text into ciphertext or the reverse.
5. The key is part of the variable data provided as input to a cryptographic algorithm to execute this sort of operation.
6. The cryptographic scheme's security depends on the security of the keys used.
7. Cryptosystems are used for sending messages in a secure manner over the internet, such as credit card information and other private data.
8. In another application of cryptography, a system for secure electronic mail might include methods for digital signatures, cryptographic hash functions and key management techniques.
9. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.
10. A cryptosystem is also referred to as a **cipher system**.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted.



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows −

- **Plaintext :-** It is the data to be protected during transmission.

- **Encryption Algorithm:-** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. A cryptographic algorithm takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext:-** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm:-** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. A cryptographic algorithm takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key:-** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key:-** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He/she, however, must never know the decryption key.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

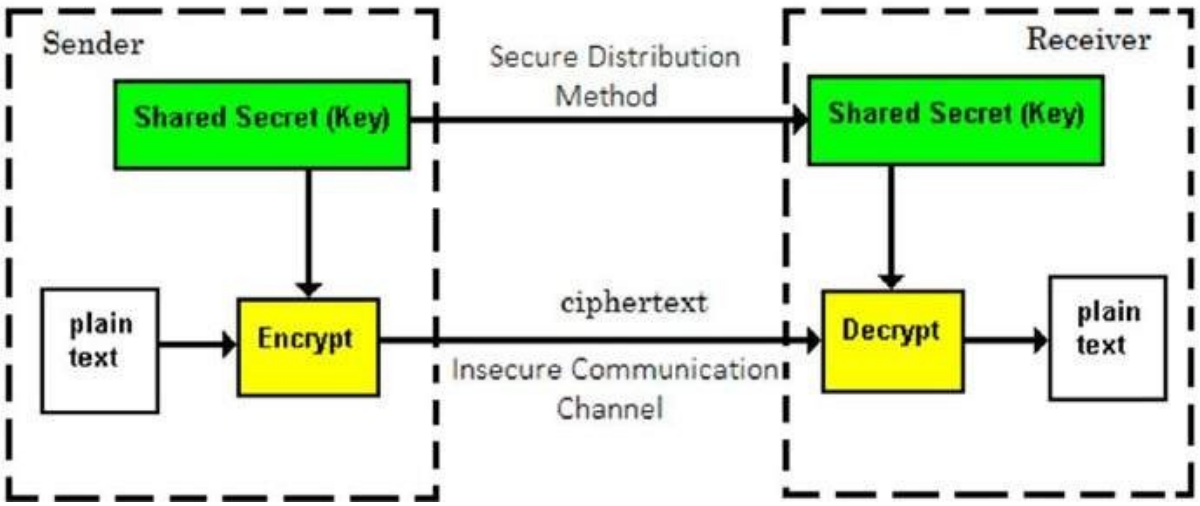
The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

A few well-known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The major features of cryptosystem based on symmetric key encryption are −

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust (strong) mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and unmanageable.
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

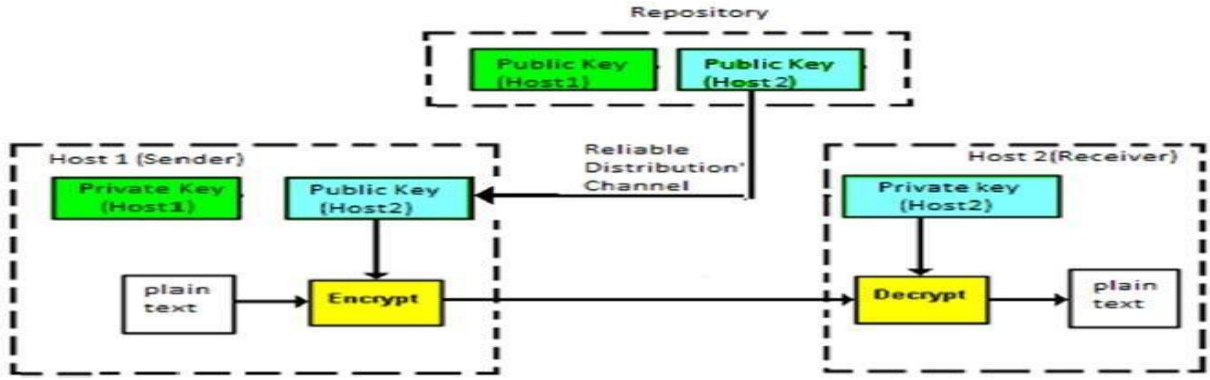
There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** − Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** − Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration −



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows −

- Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When *Host1* needs to send data to *Host2,* he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
- *Host2* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

Private Key: In the Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.
Public Key: In a Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message. Now, we see the difference between them:

S.NO	Private Key	Public Key
1.	The private key is faster than the public key.	It is slower than a private key.

S.NO	Private Key	Public Key
2.	In this, the same key (secret key) and algorithm are used to encrypt and decrypt the message.	In public-key cryptography, two keys are used, one key is used for encryption, and the other is used for decryption.
3.	In private key cryptography, the key is kept a secret.	In public-key cryptography, one of the two keys is kept a secret.
4.	The private key is **Symmetrical** because there is only one key that is called a secret key.	The public key is **Asymmetrical** because there are two types of keys: private and public keys.
5.	In this cryptography, the sender and receiver need to share the same key.	In this cryptography, the sender and receiver do not need to share the same key.
6.	In this cryptography, the key is private.	In this cryptography, the public key can be public and a private key is private.
7.	It is an efficient technology.	It is an inefficient technology.
8.	It is used for large amounts of text.	It is used for only short messages.
9.	There is the possibility of losing the key that renders the systems void.	There is less possibility of key loss, as the key is held publicly.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge − the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

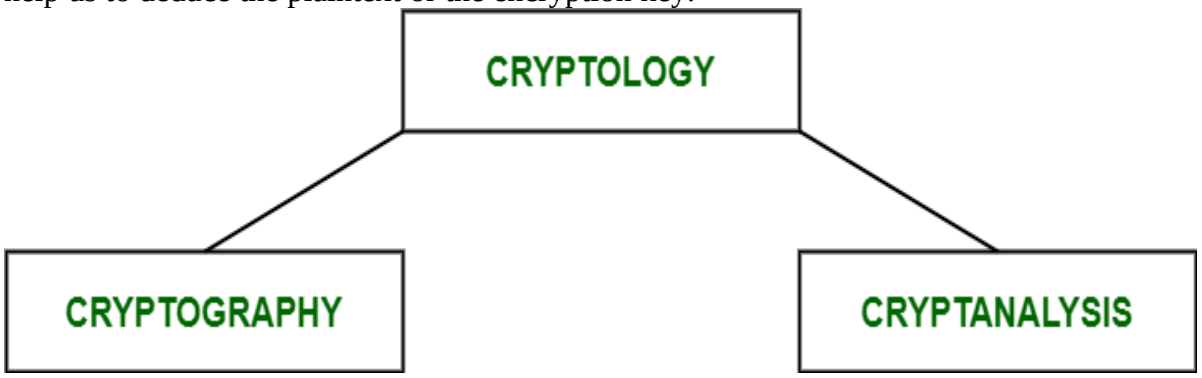
This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process − that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

Cryptanalysis

Cryptology has two parts namely, **Cryptography** which focuses on creating secret codes and **Cryptanalysis** which is the study of the cryptographic algorithm and the breaking of

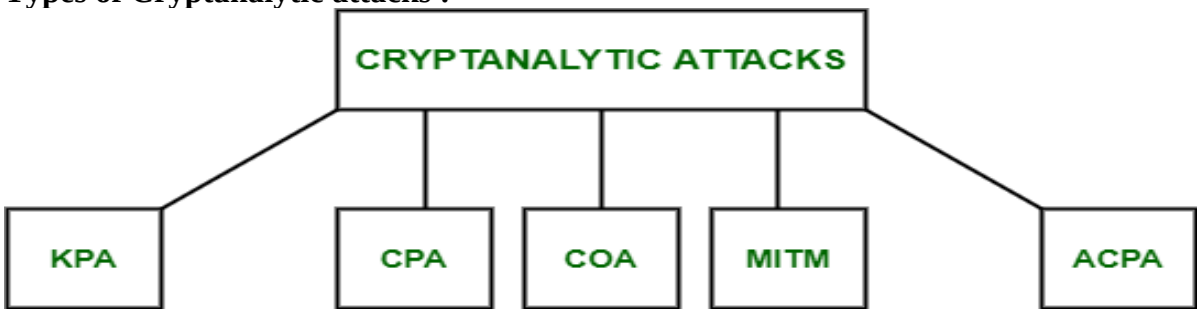
those secret codes. The person practicing Cryptanalysis is called a **Cryptanalyst**. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For example, a Cryptanalyst might try to decipher a ciphertext to derive the plaintext. It can help us to deduce the plaintext or the encryption key.



Parts Of Cryptology

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called **Cryptanalytic attacks.** The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.

Types of Cryptanalytic attacks :



The Five Types of Cryptanalytic Attacks

- **Known-Plaintext Analysis (KPA):**

  In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

- **Chosen-Plaintext Analysis (CPA) :**

  In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. Its very simple to implement like KPA but the success rate is quite low.
- **Ciphertext-Only Analysis (COA) :**

  In this type of attack, only some cipher-text is known and the attacker tries to find the

corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required.

- **Man-In-The-Middle (MITM) attack :**

  In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel.

- **Adaptive Chosen-Plaintext Analysis (ACPA) :**

  This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.

Security Threats

The terms threat, **vulnerability** and **weakness** are often used in cyber security. Understanding the difference between these terms is important. It allows organizations to correctly implement, document and assess their cyber security activities and controls. Here, we take a closer look at security threats.

A threat is a potential violation of security and causes harm. A threat can be a malicious program, a natural disaster or a thief. Vulnerability is a weakness of system that is left unprotected. Systems that are vulnerable are exposed to threats. Threat is a possible danger that might exploit vulnerability; the actions that cause it to occur are the security attacks.

Security Attack

Attack is a deliberate unauthorized action on a system or asset. An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. These are the unauthorized or illegal actions that are taken against the government, corporate, or private IT assets in order to destroy, modify, or steal the sensitive data.

Attacks can be classified as active and passive attacks. An attack will have a motive and will follow a method when the opportunity arises.

Active attacks

In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for integrity and availability of the message. Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. The system resources can be changed due to active attacks. So, the damage done with active attacks can be harmful to the system and its resources.

Replay − Replay contains the passive capture of an information unit and its consecutive retransmission to create an unauthorized development.

Masquerade − A masquerade creates place when one entity impersonate to be a various entity. A masquerade attack generally involves one of the multiple forms of active attack.

For instance, authentication array can be captured and replayed after a true authentication array has taken place, therefore allowing an authorized entity with some privileges to acquire more privileges by imitate an entity that has those privileges.

Modification of messages − Modification of message simply defines that some portion of a legitimate message is transformed, or that messages are held up or reordered, to make an unauthorized effect.

Denial of Service − The denial of service avoids or prevent the general use or administration of communications facilities. This attack can have a definite focus. For instance, an entity can suppress some messages supervised to a specific destination.

Another type of service denial is the division of an entire network, either by damaging the network or by overloading it with messages so as to corrupt performance.

In the below image, we can see the process of active attacks.

In active attacks, the victim gets notified about the attack. The implication of an active attack is typically difficult and requires more effort. Active attacks can be prevented by using some techniques. We can try the below-listed measures to prevent these attacks -

- Use of one-time password help in the authentication of the transactions between two parties.
- There could be a generation of the random session key that will be valid for a single transaction. It should prevent the malicious user from retransmitting the actual information once the session ends.

Passive attacks

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.

There are two method of passive attacks are release of message contents and traffic analysis.

The release of message contents is simply learn. A telephone chat, an electronic mail message, and a transferred file can include sensitive or confidential data. It is like to avoid an opponent from understanding the contents of these transmissions.

A second method of passive attack are traffic analysis. Assume that it is an approach of hiding the contents of messages or some information traffic so that opponents, even if they acquired the message, could not extract the data from the message.

The general approach for masking contents is encryption. If it can have an encryption security in area, an opponent can be able to find the duplicate of these messages.

The opponent can decide the location and identity of broadcasting hosts and can detect the frequency and magnitude of messages being exchanged. This data can be beneficial in guessing the feature of the communication that was creating place.

In the below image, we can see the process of passive attacks.

Unlike active attacks, in passive attacks, victims do not get informed about the attack. It is difficult to detect as there is no alteration in the message. Passive attacks can be prevented by using some encryption techniques. We can try the below-listed measures to prevent these attacks -

- We should avoid posting sensitive information or personal information online. Attackers can use this information to hack your network.
- We should use the encryption method for the messages and make the messages unreadable for any unintended intruder.

Cryptographic Attacks

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as *broken* or *compromised*.

Based on the methodology used, attacks on cryptosystems are categorized as follows −

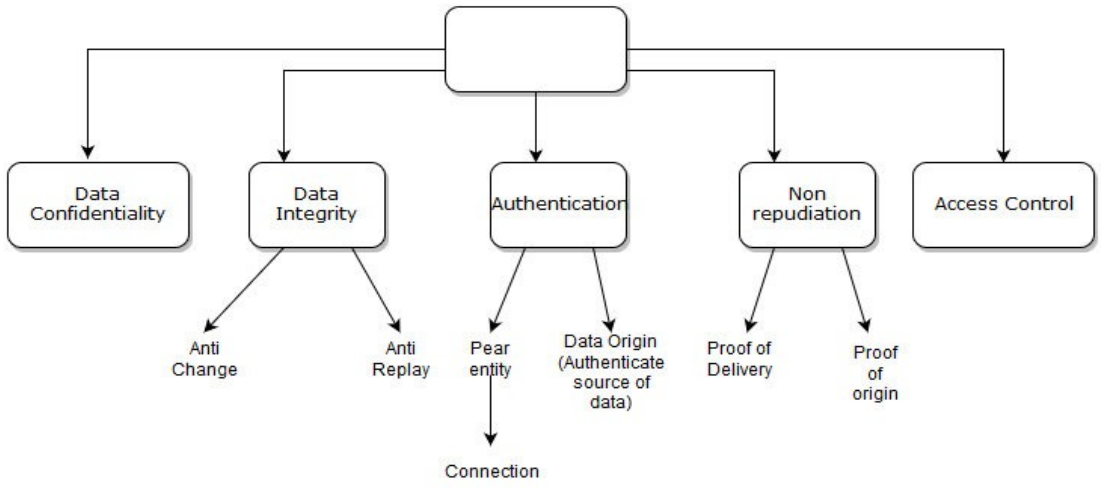
- **Ciphertext Only Attacks (COA)** − In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.
- **Known Plaintext Attack (KPA)** − In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.
- **Chosen Plaintext Attack (CPA)** − In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.
- **Dictionary Attack** − This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.
- **Brute Force Attack (BFA)** − In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.
- **Birthday Attack** − This attack is a variant of brute-force technique. It is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates. Let us assume the first student's birthdate is 3rd Aug. Then to find the next student whose birthdate is 3rd Aug, we need to enquire $1.25^* \quad \sqrt{365} \approx 25$ students.
  Similarly, if the hash function produces 64 bit hash values, the possible hash values are 1.8×10^{19}. By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about 5.1×10^9 random inputs.
  If the attacker is able to find two different inputs that give the same hash value, it is a **collision** and that hash function is said to be broken.
- **Man in Middle Attack (MIM)** − The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
  - Host *A* wants to communicate to host *B*, hence requests public key of *B*.
  - An attacker intercepts this request and sends his public key instead.
  - Thus, whatever host *A* sends to host *B*, the attacker is able to read.

- In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to *B*.
- The attacker sends his public key as *A*'s public key so that *B* takes it as if it is taking it from *A*.

- **Side Channel Attack (SCA)** − This type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.
- **Timing Attacks** − They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.
- **Power Analysis Attacks** − These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.
- **Fault analysis Attacks** − In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

Security Services:

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. Following are the five categories of these services:



Auth entication: The assurance that the communicating entity is the one that it claims to be.

- **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
- **Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.

Data Confidentiality: Protects data from unauthorized disclosure.

Access Control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Data Integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Non-repudiation: Protects against denial by one of the entities involved in a communication of having participated in all or part of the communication.

- **Proof of Origin:** Proof that the message was sent by the specified party.
- **Proof of Delivery:** Proof that the message was received by the specified party.

Security Policies

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Security Mechanism

A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol.

1. **Encipherment:** Encipherment is hiding or covering data and can provide confidentiality. It makes use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. Cryptography and Steganography techniques are used for enciphering.

2. **Data integrity:** The data integrity mechanism appends a short check value to the data which is created by a specific process from the data itself. The receiver receives the data and the check value. The receiver then creates a new check value from the received data and compares the newly created check value with the one received. If the two check values match, the integrity of data is being preserved.
3. **Digital Signature:** A digital signature is a way by which the sender can electronically sign the data and the receiver can electronically verify it. The sender uses a process in which the sender owns a private key related to the public key that he or she has announced publicly. The receiver uses the sender's public key to prove the message is indeed signed by the sender who claims to have sent the message.
4. **Authentication exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange. The two entities exchange some messages to prove their identity to each other. For example the three-way handshake in TCP.
5. **Traffic padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
6. **Routing control:** Enables selection of particular physically secure routes for certain data and allows routing changes which means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from traffic analysis on a particular route.
7. **Notarization:** The use of a trusted third party to control the communication between the two parties. It prevents repudiation. The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request.
8. **Access Control:** A variety of mechanisms are used to enforce access rights to resources/data owned by a system, for example, PINS, and passwords.

Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present. In cryptography there are two processes i.e. encryption and decryption performed at sender and receiver end respectively. Encryption is the processes where a simple multimedia data is combined with some additional data (known as key) and converted into unreadable encoded format known as Cipher. Decryption is the reverse method as that of encryption where the same or different additional data (key) is used to decode the cipher and it is converted in to the real multimedia data.
Cryptography techniques can be categorized according to their basic principles or protocols they follow. But here we are going to concentrate on the two types of cryptography technique: **Classical Cryptography** and **Quantum Cryptography**.

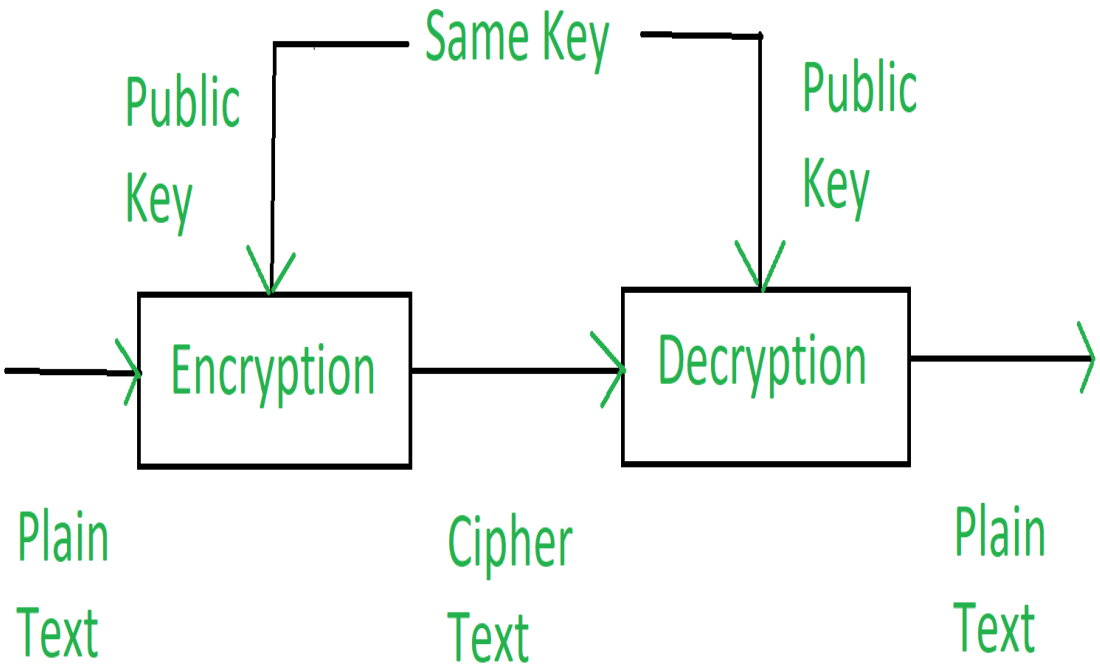
Classical Cryptography:
Classical cryptography is based on the mathematics and it relies on the computational difficulty of factorizing large number. The security of classical cryptography is based on the high complexity of the mathematical problem for the instance factorization of large number.
In the classical cryptography the original data i.e., the plain text is transformed into the encoded format i.e. cipher text so that we can transmit this data through insecure communication channels. A data string which known as key is used to control the transformation of the data from plain text to cipher text. This arrangement helps to keep

data safe as it required the key for extracting the original information from the cipher text. Without the key no one can read the data. In this technique it is assumed that the only authorized receiver has the key.

Classical Cryptography has two types of techniques:

1. **Symmetric Cryptography:**

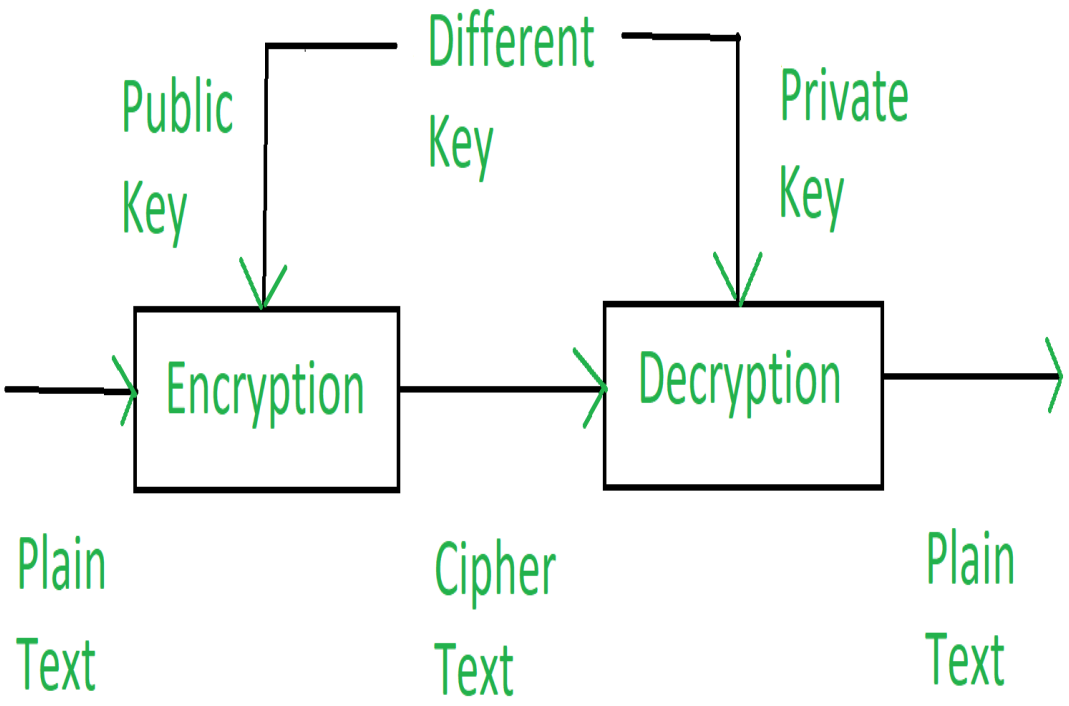
   In the symmetric cryptography a single key is used for encrypting and decryption the data. This encryption key is private key. This is the limitation of this encryption technique that this private key must be distributed only among the authorized sender and receiver.



Symmetric Cryptography

2. **Asymmetric Cryptography:**

   In the asymmetric cryptography a pair of key, i.e., public key and private key is used for encryption and decryption. A sender can use its public key to encrypt the data and on receiver end receiver can decrypt the data by using its private key. This technique overcomes the problem of key distribution.



Asymmetric Cryptography

Advantages of Classical Cryptography:

- While employing the one-time pad, it is unbreakable.
- It is easy to do manually, no computer required.
- It protects the plain text from casual snooping.

Disadvantages of Classical Cryptography:

- While employing the one-time pad, it is cumbersome and requires a personal meetup to exchange the pads.
- If not employing the OTP, anyone who is even remotely interested in knowing what you wrote and knows about cryptography will be able to break the encryption.

3. **Quantum Cryptography:**

   Quantum Cryptography is based on physics and it relies on the laws of quantum mechanics. It is arising technology which emphasizes the phenomena of quantum physics in which two parties can have secure communication based on the invariabilities of the laws of the quantum mechanics. Quantum mechanics is the mathematical framework or set of rules for the construction of physical theories.

There are two important elements of quantum mechanics on which quantum cryptography depends: **Heisenberg Uncertainty Principle** and **Photon Polarization Principle**. These are:

1. **Heisenberg Uncertainty Principle:**

   This principle says that if we measure one thing, we cannot measure another thing

accurately. For example, if we apply this principle to human, we could measure a person's height, but we can't measure his weight. The only odd thing about this principle is that it becomes true only for the instant at which we try to measure something. This principle is applied to the photons. Photons have wave like structure and are polarized or tilted in certain direction. While measuring photon polarization, all subsequent measurements are get affected by the choice of measures that we made for polarization. This principle plays the vital role to prevent the efforts of attacker in quantum cryptography.

2. **Photon Polarization Principle:**

   This principle refers that; an eavesdropper cannot copy the unique quantum bits, i.e., unknown quantum state, due to the no-cloning principle. If an attempt is made for measuring any properties, it will disturb the other information.

Advantages of Quantum Cryptography:

- It establishes secure communication by providing security based on fundamental laws of physics instead of mathematical algorithms or computing technologies used today.
- It is virtually un-hack able.
- It is simple to use.
- Less resources are needed in order to maintain it.
- It is used to detect eavesdropping in QKD (Quantum Key Distribution). This is due to the fact that it is not possible to copy the data encoded in quantum state.
- The performance of such cryptography systems is continuously improved.

Disadvantages of Quantum Cryptography:

- The worldwide implementation of this can take up lots of jobs and hence unemployment will increase.
- While traveling through the channel polarization of photon may change due to various causes.
- Quantum cryptography lacks many vital features such as digital signature, certified mail etc.
- The largest distance supported by QKD is about 250 KM at a speed of 16 bps through guided medium.