UNIT II

Introduction to 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 that 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.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to the ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows. The sender's message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of received, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively. Let's consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar's Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3. For example:

Plaintext : Geeksforgeeks

Ciphertext : Jhhnvirujhhnv

Note: *Even if the adversary knows that the cipher is based on Caesar's Cipher, it cannot predict the plaintext as it doesn't have the key in this case which is to shift the characters back by three places. Refer to Introduction to Crypto-terminologies.*

Types of Cryptography:

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

1. Symmetric-key cryptography: This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.
2. Asymmetric-key cryptography: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.
Hash functions: A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

Applications of Cryptography:

Cryptography has a wide range of applications in modern-day communication, including:

- **Secure online transactions:** Cryptography is used to secure online transactions, such as online banking and e-commerce, by encrypting sensitive data and protecting it from unauthorized access.
- **Digital signatures:** Digital signatures are used to verify the authenticity and integrity of digital documents and ensure that they have not been tampered with.
- **Password protection:** Passwords are often encrypted using cryptographic algorithms to protect them from being stolen or intercepted.

Military and intelligence applications: Cryptography is widely used in military and intelligence applications to protect classified information and communications.

Challenges of Cryptography:

While cryptography is a powerful tool for securing information, it also presents several challenges, including:

- **Key management**: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.
- **Quantum computing:** The development of quantum computing poses a potential threat to current cryptographic algorithms, which may become vulnerable to attacks.
- **Human error:** Cryptography is only as strong as its weakest link, and human error can easily compromise the security of a communication.

History of Cryptography

Humans have two basic needs when we take about communication. One is the need to communicate selectively, to communicate and share information. These two basic needs while

communicating gave rise to coding and encrypting the messages in such a way that only intended people could have access to the information.

The word ‘cryptography’ originated from two greek words ‘Krypto’ means hidden and ‘graphene’ means writing.

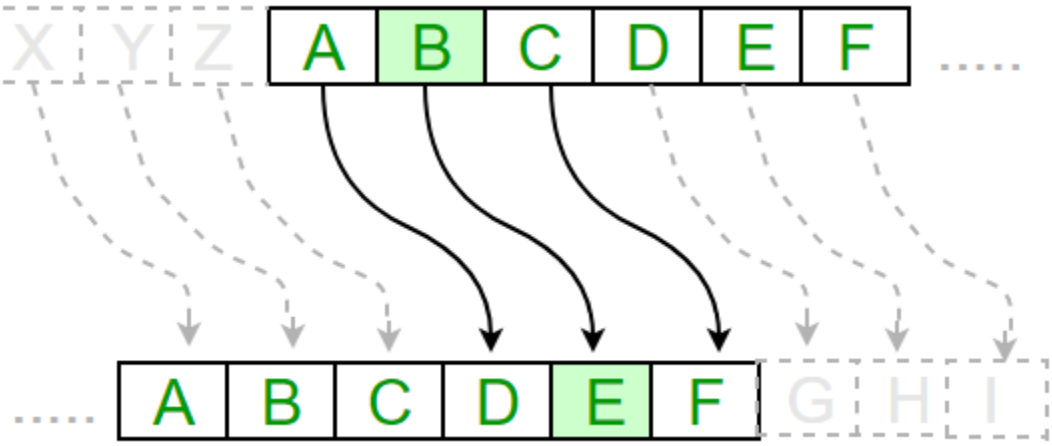
Classical Cryptography

The roots are cryptography are found in Roman and Egyptian civilizations. Below are some of the ancient types of cryptography:

1. Hieroglyphs Cryptography: The earliest known use of Cryptography can be dated back to 1900 BCE during the time of the Old Kingdom of Egypt in form of non-standard hieroglyphs.

- Hieroglyphs were a secret form of communication that the Egyptians used to communicate with one another.
- This secret text was known only to the scribes of the kings who used to transmit messages on their behalf.

2. Caesar Cipher: The ancient Greeks were well known for the use of Ciphers. The Caesar Cipher or Shift Cipher is one of the earliest and simplest well-known cryptographic techniques. It is a form of Substitution Cipher where each character in a word is replaced by a fixed number of positions. For example with a shift of 3, A is replaced by D, B by E, and so on.



3. Vigenere Cipher: During the 16th century, Vigenere designed a cipher in which the encryption key is repeated multiple times spanning the entire message, and then the cipher text is generated by adding the message character with key character modulo 26. This approach is also vulnerable to attacks, where the secrecy of the message depends on the secrecy of the encryption key.

4. Hebern rotating machine: At the start of the 19th century, Hebern designed a Hebern rotating machine. In this machine, a single rotor is used where the secret key is embedded in the rotating disc and the key has an embedded substitution table. Each key press from the keyboard resulted in the output of cipher text. This code is broken by using the letter frequencies.

5. Enigma machine: Cryptography played a vital in the victory of Allied forces during World War I and World War II. World War II prominently saw the use of electromechanical cipher

machines. The story of the Allied victory over the Germans by cracking the world-famous Enigma machine is well known. Like all rotor machines, Enigma is a combination of electro-mechanical subsystems. It consisted of somewhat three to five rotors. Whenever a key was pressed, one or more rotors rotated on the spindle, and accordingly, the key was scrambled to something else. The Enigma cipher was broken by Poland.

Data Encryption Standard (DES)

In the early 1970s, IBM realized that its customer base is requesting some type of encryption method to protect the data. They formed a crypto group headed by Horst-Feistel. This group designed a cipher called Lucifer. In 1973, the Nation Bureau of Standards (NBS) which is now known as the National Institute of Standards and Technology (NIST) put out a proposal for the block cipher. Lucifer was eventually accepted and called Data Encryption Standard (DES).

- It is a symmetric-key algorithm based on the Feistel cipher and is used for the encryption of electronic data.
- It has a relatively small key size of 56-bits and is encrypted 64 bits or 8 characters at a time.
- In 1997, DES was broken by an exhaustive search attack.
- But, it was later discontinued as it was found to be insecure, especially against brute force attacks cause of its relatively small key size.

Advance Encryption Standard (AES)

In 1997, NIST again put out a proposal for a new block cipher. The Rijndael cipher is eventually accepted and renamed as Advanced Encryption Standard (AES).

- DES was replaced by Advance Encryption Standard or AES in 2001.
- Unlike DES, AES is based on a substitution-permutation network.
- AES is a sub-set of Rijndael.
- It is a family of ciphers with different key and block sizes.
- In the case of AES, the block size is 128 bits or 16 characters which means 16 characters can be encrypted at a time.
- It comes with three different key size variants: 128 bits, 192 bits, and 256 bits.

Cryptography and Network Security Principles

In present day scenario security of the system is the sole priority of any organisation. The main aim of any organisation is to protect their data from attackers. In cryptography, attacks are of two types such as Passive attacks and Active attacks.
Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.

Figure : 1.1

In figure 1.1 it made the text secure by forming it into cipher text using encryption algorithm and further decryption to use it.
The Principles of Security can be classified as follows:

1. **Confidentiality:**
   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.
   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication:**
   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

3. **Integrity:**
   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

- **System Integrity:** System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Data Integrity:** Data Integrity assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

4. **Non-Repudiation:**

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5.Access control:

The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6.Availability:

The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

7. **Issues of ethics and law**

The following categories are used to categorize ethical dilemmas in the security system.Individuals' right to access personal information is referred to as privacy.

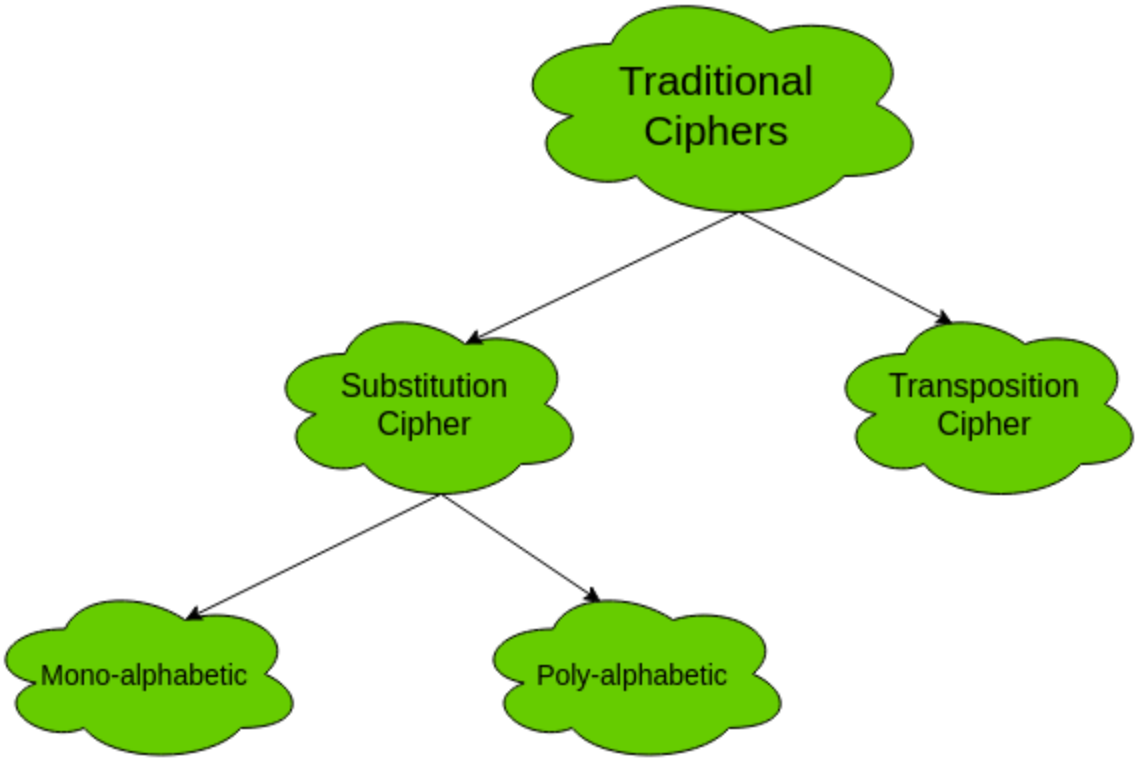
Property: It is concerned with the information's owner.

Accessibility is concerned with an organization's right to collect information.

Accuracy: It is concerned with the obligation of information authenticity, fidelity, and accuracy.

Traditional Symmetric – Key Cipher

The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**. The following flowchart categories the traditional ciphers:

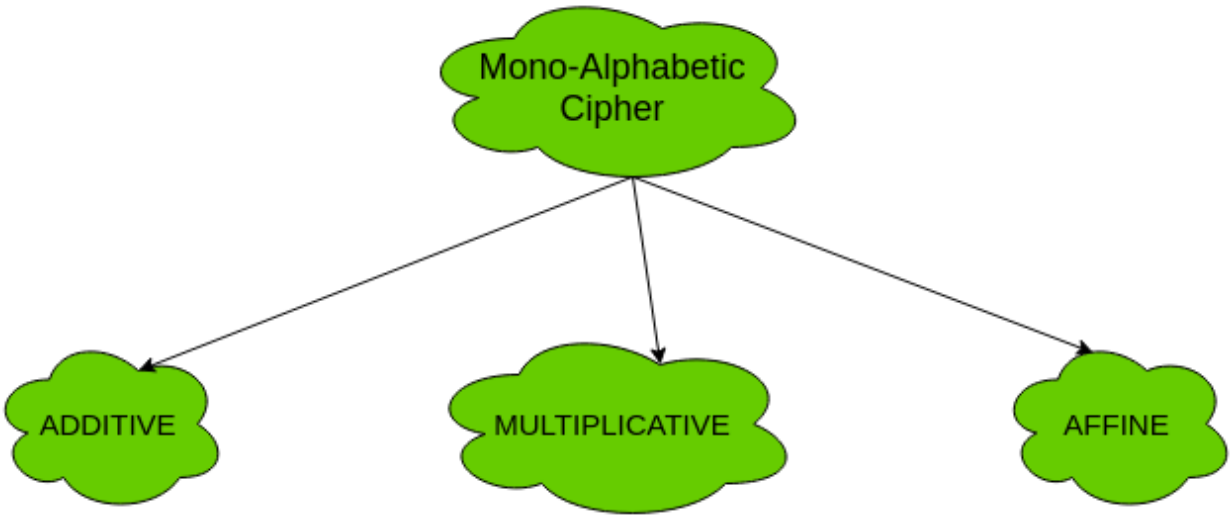


1. Substitution Cipher:
Substitution Ciphers are further divided into **Mono-alphabetic Cipher** and **Poly-alphabetic Cipher**.
First, let's study about mono-alphabetic cipher.

1. **Mono-alphabetic Cipher** –
   In mono-alphabetic ciphers, each symbol in plain-text (eg; 'o' in 'follow') is mapped to one cipher-text symbol. No matter how many times a symbol occurs in the plain-text, it will correspond to the same cipher-text symbol. For example, if the plain-text is 'follow' and the mapping is :
   - f -> g
   - o -> p
   - l -> m
   - w -> x

   The cipher-text is 'gpmmpx'.

   Types of mono-alphabetic ciphers are:



(a). Additive Cipher (Shift Cipher / Caesar Cipher) – The simplest mono-alphabetic cipher is additive cipher. It is also referred to as 'Shift Cipher' or 'Caesar Cipher'. As the name suggests, 'addition modulus 2' operation is performed on the plain-text to obtain a cipher-text.

$C = (M + k) \bmod n$

$M = (C - k) \bmod n$

where,

C -> cipher-text

M -> message/plain-text

k -> key

The key space is 26. Thus, it is not very secure. It can be broken by brute-force attack. For more information and implementation see Caesar Cipher

(b). Multiplicative Cipher – The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

$C = (M * k) \bmod n$

$M = (C * k^{-1}) \bmod n$

where,

k^{-1} -> multiplicative inverse of k (key)

The key space of multiplicative cipher is 12. Thus, it is also not very secure.

(c). Affine Cipher – The affine cipher is a combination of additive cipher and multiplicative cipher. The key space is 26 * 12 (key space of additive * key space of multiplicative) i.e. 312. It is relatively secure than the above two as the key space is larger. Here two keys k_1 and k_2 are used.

$C = [(M * k_1) + k_2] \bmod n$

$M = [(C - k_2) * k_1^{-1}] \bmod n$

For more information and implementation, see Affine Cipher

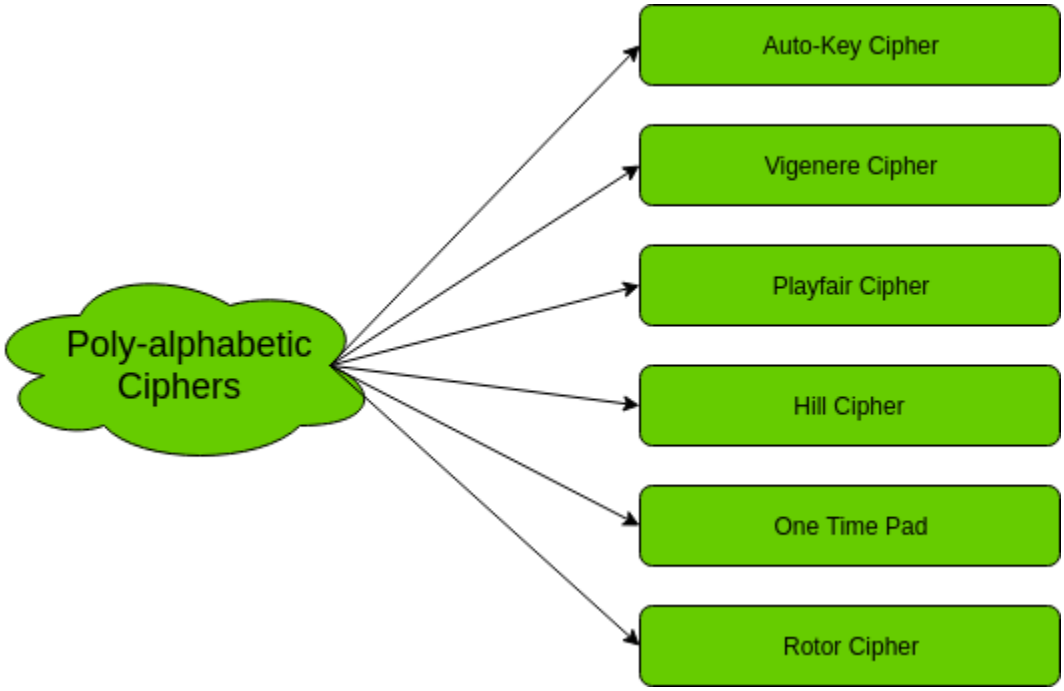
Now, let's study about poly-alphabetic cipher.

2. **Poly-alphabetic Cipher** – In poly-alphabetic ciphers, every symbol in plain-text is mapped to a different cipher-text symbol regardless of its occurrence. Every different occurrence of a symbol has different mapping to a cipher-text. For example, in the plain-text 'follow', the mapping is :

f -> q
o -> w
l -> e
l -> r
o -> t
w -> y

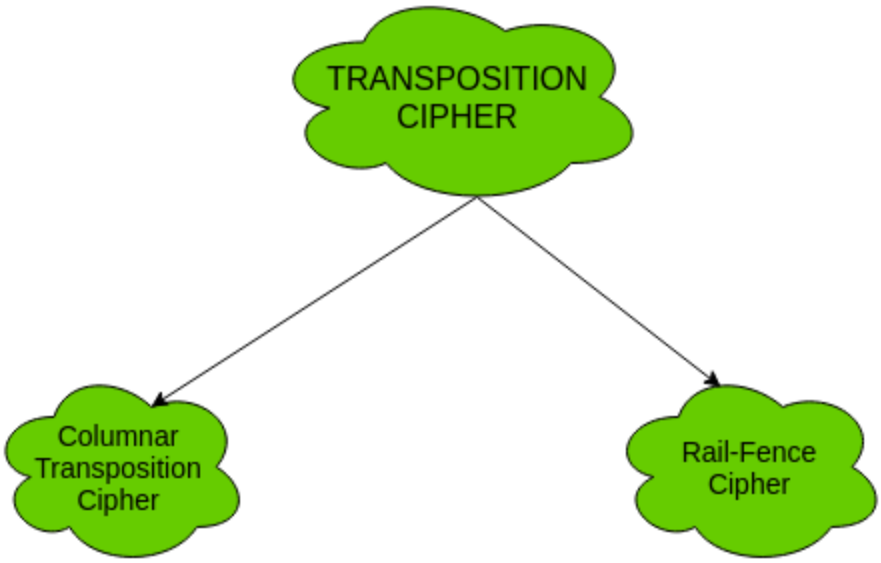
Thus, the cipher text is 'qwerty'.

Types of poly-alphabetic ciphers are:



2. Transposition Cipher:

The transposition cipher does not deal with substitution of one symbol with another. It focuses on changing the position of the symbol in the plain-text. A symbol in the first position in plain-text may occur in fifth position in cipher-text.
Two of the transposition ciphers are:



Asymmetric – Key Cryptography (Public key cryptotgraphy):

Public Key Encryption

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as **ciphertext**.

Encryption:
The process of changing the plaintext into the ciphertext is referred to as **encryption.** The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

The security of conventional encryption depends on the major two factors:

1. The Encryption algorithm
2. Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.
Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Decryption:
The process of changing the ciphertext to the plaintext that process is known as **decryption**.

Public Key Encryption: Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

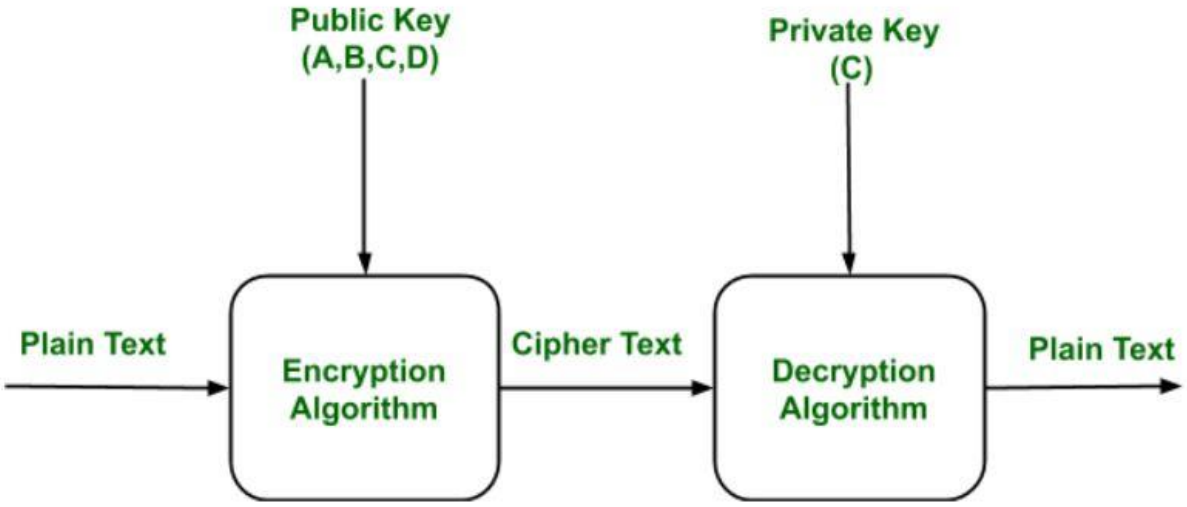
Difference between Encryption and Public-key Encryption:

basis	Encryption	Public-Key Encryption
Required for Work:	• Same algorithm with the same key is used for encryption and decryption. • The sender and receiver must share the algorithm and key.	• One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for encryption and other for decryption. • Receiver and Sender must each have one of the matched pair of keys (not identical).
Required for Security:	• Key must be kept secret. • If the key is secret, it is very impossible to decipher message. • Knowledge of the algorithm plus samples of ciphertext must be impractical to determine the key.	• One of the two keys must be kept secret. • If one of the keys is kept secret, it is very impossible to decipher message. • Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be impractical to determine the other key.

Characteristics of Public Encryption key:

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two keys (Public and Private key) can be used for encryption with another key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Example:
Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.



Components of Public Key Encryption:

- **Plain Text:**
  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:**
  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:**
  The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:**
  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:**
  One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption.

Weakness of the Public Key Encryption:

- Public key Encryption is vulnerable to Brute-force attack.
- This algorithm also fails when the user lost his private key, then the public key Encryption becomes the most vulnerable algorithm.
- Public Key Encryption also is weak towards man in the middle attack. In this attack a third party can disrupt the public key communication and then modify the public keys.

- If user private key used for certificate creation higher in the PKI(Public Key Infrastructure) server hierarchy is compromised, or accidentally disclosed, then a “man-in-the-middle attack” is also possible, making any subordinate certificate wholly insecure. This is also the weakness of public key Encryption.

Applications of the Public Key Encryption:

- **Encryption/Decryption:**
  Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensure that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:**
  Digital signature is for sender’s authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders public key only.
- **Key exchange:**
  This algorithm can use in both Key-management and securely transmission of data.

Security Goals:

The security goals in cryptography and network security revolve around preserving data's confidentiality, integrity, and availability. These goals are achieved through encryption, access control, and IP security architecture in cryptography and network security to ensure data safety while it is in motion and stored.

The Main Goals of cryptography

- Data Privacy(confidentiality)
- Data Authenticity(it came from from where it claims)
- Data integrity(it has not been modified on the way) in the digital world

Confidentiality

- Confidentiality is most commonly addressed goal
- The meaning of a message is concealed by encoding it
- The sender encrypts the message using a cryptographic key
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender

Data Integrity

- Integrity Ensures that the message received is the same as the message that was sent
- Uses hashing to create a unique message digest from the message that is sent along with the message

- Recipient uses the same technique to create a second digest from the message to compare to the original one
- This technique only protects against unintentional alteration of the message
- A variation is used to create digital signatures to protect against malicious alteration

Authentication

- A user or system can prove their identity to another who does not have personal knowledge of their identity
- Accomplished using digital certificates
- Kerberos is a common cryptographic authentication system

Cryptographic attacks:

Cryptography attacks are malicious attempts to compromise the security of cryptographic systems, aiming to exploit vulnerabilities and gain unauthorized access to sensitive information. These attacks pose a significant threat to the confidentiality, integrity, and availability of encrypted data.

What are Cryptography Attacks?

Cryptography attacks are malicious attempts to compromise the security of cryptographic systems, aiming to exploit vulnerabilities and gain unauthorised access to sensitive information.

These attacks pose a significant threat to the confidentiality, integrity, and availability of encrypted data.

Attackers employ various strategies to breach cryptographic defences, targeting weaknesses in algorithms, keys, or implementation processes.

Understanding the different types of cryptography attacks is crucial for developing robust security measures.

To safeguard against cryptography attacks, it is essential to adopt strong encryption algorithms, regularly update systems to patch vulnerabilities, implement secure key management practices, and be vigilant against evolving threats in the dynamic landscape of digital security.

8 Types of Attack in Cryptography

When talking about about cryptography attacks there are 8 main ways it happens:

Brute Force

Brute force cryptography attacks represent a relentless assault on encrypted information, employing a systematic method of trying every possible key until the correct one is found.

This method involves an exhaustive trial-and-error approach, making it time-consuming but effective if encryption keys are weak or easily guessable.

Brute force attacks can target various cryptographic systems, including passwords, encryption keys, and digital signatures.

To mitigate the risk of brute force attacks, employing strong and complex encryption keys is imperative.

Longer and more intricate keys exponentially increase the time and computational resources required for attackers to succeed.

The effectiveness of cryptographic defences relies on the resilience against brute force attempts, emphasising the importance of robust key management practices in the digital security landscape.

Cipher Only Attack

Cipher-only attacks are a category of cryptography attacks where the adversary possesses only the ciphertext without knowledge of the corresponding plaintext or the encryption key.

In these attacks, the attacker aims to deduce meaningful information from the ciphertext alone, assuming the cryptographic algorithm is known.

Unlike more complex attacks, cipher-only attacks leverage only the intercepted encrypted information to uncover potential vulnerabilities in the encryption process.

The effectiveness of cipher-only attacks relies heavily on the strength of the encryption algorithm employed.
Robust cryptographic systems are designed to withstand such attacks, ensuring that even with knowledge of the algorithm, deciphering the original information without the key remains a formidable challenge.

These attacks underscore the importance of selecting secure encryption algorithms that can withstand scrutiny even when the ciphertext is in the hands of potential adversaries.

Known Plaintext Attack

Known plaintext attacks target cryptographic systems by exploiting the knowledge of both the plaintext and its corresponding ciphertext.

In these attacks, adversaries aim to deduce the encryption key based on the known relationship between certain plaintext and ciphertext pairs.

The challenge for cryptographic systems is to resist compromise even when portions of the plaintext and corresponding encrypted data are known to the attacker.

The vulnerability lies in the potential exposure of specific data pairs, allowing attackers to analyse patterns and deduce elements of the encryption key.

Robust encryption algorithms are designed to withstand known plaintext attacks by introducing complexity and unpredictability, making it challenging for adversaries to extrapolate the encryption key from limited information.

This type of attack emphasises the importance of developing and implementing encryption methods that can effectively secure information even when portions of the data are known to potential attackers.

Chosen Plaintext Attack

Chosen plaintext attacks represent a sophisticated cryptographic threat where intruders have the ability to select specific plaintexts and observe their corresponding ciphertexts.

This type of attack aims to deduce information about the encryption key by analysing the outcomes of deliberately chosen input and output pairs.

In chosen plaintext attacks, attackers exploit their ability to manipulate the encryption process, revealing patterns that may lead to the compromise of the cryptographic system.

The challenge for cryptographic defences lies in constructing algorithms that remain secure even when subjected to intentional manipulation by adversaries.

Robust encryption methods employ intricate mathematical structures and mechanisms to resist chosen plaintext attacks, ensuring that the system's integrity and confidentiality are upheld.

As cybersecurity evolves, the continuous development of encryption techniques that can withstand such advanced attacks becomes pivotal in maintaining the security of sensitive information.

Chosen Ciphertext Attack

Chosen ciphertext attacks pose a formidable threat to cryptographic systems, as adversaries possess the ability to choose specific ciphertexts and obtain their corresponding plaintexts.

In these attacks, attackers manipulate the decryption process, aiming to deduce sensitive information or the encryption key itself.

Chosen ciphertext attacks exploit vulnerabilities in cryptographic systems by allowing intruders to actively influence the decryption of specific data.

To counter chosen ciphertext attacks, robust cryptographic algorithms must be designed to withstand manipulation attempts on encrypted data.

The challenge lies in creating encryption methods that maintain security even when attackers have a level of control over the ciphertexts they choose to decrypt.

Effective cryptographic defences focus on introducing complexities and safeguards that thwart the adversary's ability to extract meaningful information from intentionally chosen ciphertexts, ensuring the confidentiality and integrity of encrypted data.

Key and Algorithm Attack

Key and algorithm attacks in cryptography target the vulnerability of the encryption key or the underlying algorithm itself.

Criminals aim to exploit weaknesses in either the cryptographic key or the algorithm, seeking unauthorised access to encrypted information.

In key attacks, the adversary focuses on compromising the encryption key, while algorithm attacks aim to exploit flaws in the mathematical processes governing encryption.

To counteract key and algorithm attacks, robust key management practices and secure algorithms are crucial.

The strength of cryptographic systems lies in the complexity and unpredictability introduced into both the encryption key and algorithm.

By continually enhancing key and algorithm security, cryptographic defences ensure resilience against sophisticated attacks, safeguarding sensitive information from unauthorised access and manipulation.

Regular updates and advancements in cryptographic practices are essential to stay ahead of evolving threats in the dynamic landscape of digital security.

Side Channel Attacks

Side channel attacks target cryptographic systems by exploiting information unintentionally leaked during the encryption or decryption process.

These attacks do not directly target the algorithm or key but focus on exploiting auxiliary information, such as power consumption, timing, or electromagnetic radiation.

By analysing these side channels, adversaries attempt to deduce sensitive information or gain insights into the cryptographic operations.

Protecting against side channel attacks requires additional measures beyond traditional cryptographic methods.

Cryptographic implementations must address potential vulnerabilities in physical or implementation aspects, ensuring that unintentional information leaks do not compromise the confidentiality or integrity of the encrypted data.
Robust countermeasures involve introducing noise, randomising operations, or employing secure hardware to minimise the information leaked through side channels, bolstering the overall resilience of cryptographic systems against sophisticated attacks.

Replay Attacks

Replay attacks in cryptography involve the malicious retransmission of captured data to gain unauthorised access or manipulate system behaviour.

Attackers intercept and duplicate previously recorded data transmissions, aiming to deceive the system into accepting replicated information as legitimate.

These attacks exploit the lack of mechanisms to distinguish between original and duplicated data.

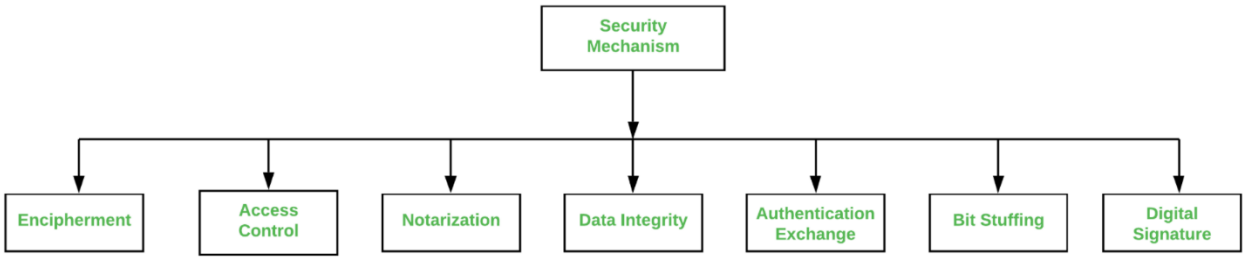
Preventing replay attacks necessitates the implementation of measures that can detect and discard repeated or out-of-sequence data transmissions.

Time-stamping and sequence numbers are common techniques employed to mitigate the risk of replay attacks.

By incorporating these safeguards, cryptographic systems can verify the freshness and authenticity of incoming data, thwarting attempts to exploit repeated transmissions for unauthorised access or manipulation.

Cryptography Services and Mechanisms:

Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



Types of Security Mechanism are :

1. **Encipherment :**
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
2. **Access Control :**
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

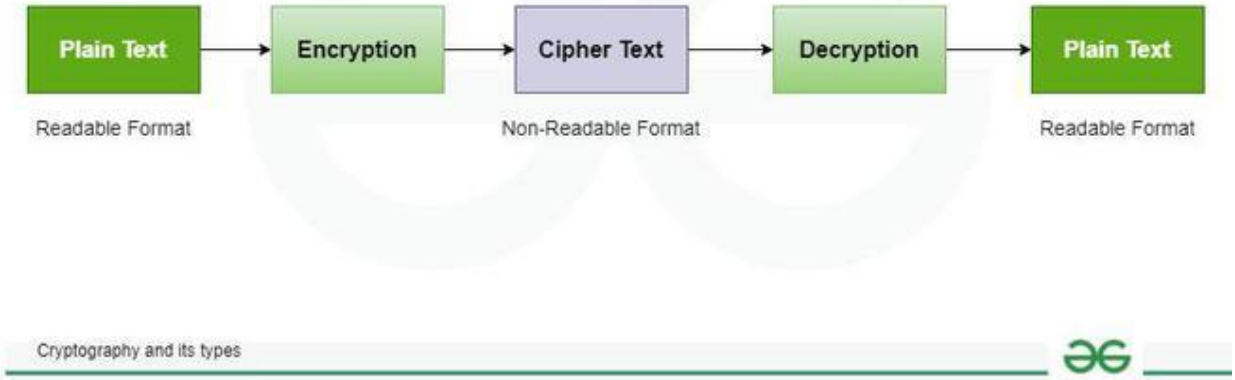
3. **Notarization :**
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
4. **Data Integrity :**
   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
5. **Authentication exchange :**
   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
6. **Bit stuffing :**
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
7. **Digital Signature :**
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Cryptography and its Types

Cryptography **i**s a technique of securing communication by converting plain text into ciphertext. It involves various algorithms and protocols to ensure data confidentiality, integrity, authentication, and non-repudiation. In this article, we will discuss cryptography and its types.

What is Cryptography?

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and the suffix "graphy" means "writing". In Cryptography, the techniques that 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 them. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.



Cryptography and its types

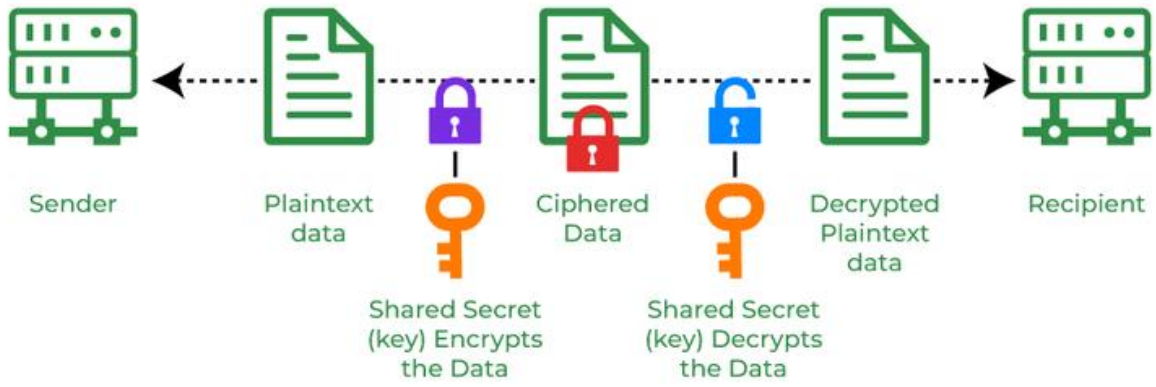
Features Of Cryptography

- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at a later stage.
- **Authentication:** The identities of the sender and receiver are confirmed. As well destination/origin of the information is confirmed.
- **Interoperability:** Cryptography allows for secure communication between different systems and platforms.
- **Adaptability:** Cryptography continuously evolves to stay ahead of security threats and technological advancements.

Types Of Cryptography

1. Symmetric Key Cryptography

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



Symmetric Key Cryptography

2. Hash Functions

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

3. Asymmetric Key Cryptography

In Asymmetric Key Cryptography, a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.

Asymmetric Key Cryptography

Applications of Cryptography

- **Computer passwords:** Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.
- **Digital Currencies:** To protect transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
- **Secure web browsing:** Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.
- **Electronic signatures:** Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.
- **Authentication:** Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.
- **Cryptocurrencies:** Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to protect transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
- **End-to-end Internet Encryption:** End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

Advantages of Cryptography

- **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
- **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the Internet.
- **Protection against attacks:** Cryptography aids in the defense against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
- **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.

Cryptography Techniques:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is also used to set up a secure connection between two systems. Cryptography uses mathematics (primarily arithmetic and number theory) to provide confidentiality, integrity, and authenticity for messages under certain conditions. It includes confidentiality by ensuring that information cannot be read or tampered with in transit, where unauthorized parties could intercept and read.

The first thing to know about cryptography is that there is no single universal method for encrypting your message. There are many ways to do it, each with its advantages and disadvantages. Today's most common encryption methods are public and symmetric key cryptography.

Many cryptographic algorithms arise naturally out of their use in other contexts, such as digital signature schemes or encryption techniques for secure electronic commerce over insecure networks such as the Internet. For example, RSA cryptosystems were initially developed to solve integer factorization.

Cryptography is sometimes used by criminals to avoid detection and allow illicit messages to be passed along without interception. It is also used by public-key cryptosystems such as RSA, which are widely used in security protocols.

Encryption Algorithms

A cryptography algorithm is a method of encryption and decryption that uses a mathematical formula to convert plain text into cipher text and back again. The cryptography encryption algorithm is a type of cipher used for data confidentiality and integrity in a computer system. It uses an encryption key to convert plaintext into ciphertext, which is then sent over a network, such as the Internet, to a destination where the receiver will decrypt it.

Cryptography encryption algorithms are commonly used in commercial electronic commerce, online banking, and other applications where confidentiality is essential. These encryption algorithms include Data Encryption Standard (DES), Triple DES, Blowfish, and CAST-256.

There are several types of encryption algorithms; these include block ciphers and stream ciphers.

- A block cipher encrypts blocks of plaintext and decrypts them one at a time.
- A stream cipher encodes multiple characters or characters from a file in a single operation.

How do Various Cryptographic Algorithms Work?

Cryptographic algorithms have a basic algorithm that produces a key, and then they each use this key to encrypt and decrypt information. But there are many ways to go about it.

- One way is to use a block cipher, which takes several bytes and converts them into a more extended sequence of bytes. This process is called encryption.
- The other way is to take a block cipher, convert it into something smaller, and then convert it back into the original block size. This process is called decryption (or deciphering).

These algorithms can be symmetric or asymmetric, depending on the algorithm used.

- Symmetric algorithms use the same key to encrypt and decrypt the data, while asymmetric algorithms use two separate keys, one to encrypt and one to interpret the data.
- The algorithms also use a message authentication code (MAC) to ensure the message's integrity.

Substitution Cipher:

Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

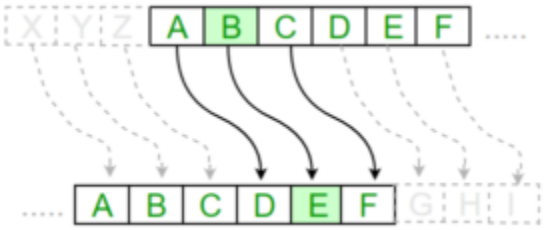
Note: Special case of Substitution cipher is known as Caesar cipher where the key is taken as 3.

Mathematical representation

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

(Encryption Phase with shift n)

(Decryption Phase with shift n)



Examples:

Plain Text: I am studying Data Encryption
Key: 4
Output: M eq wxyhCmrk Hexe IrgvCtxmsr

Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key: 4
Output: EFGHIJKLMNOPQRSTUVWXYZabcd

Algorithm for Substitution Cipher:

Input:

- A String of both lower and upper case letters, called PlainText.
- An Integer denoting the required key.

Procedure:

- Create a list of all the characters.
- Create a dictionary to store the substitution for all characters.
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Print the new string generated.

Transposition Cipher:

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Example

A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as **: holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Stream Ciphers:

In stream cipher, one byte is encrypted at a time while in block cipher ~128 bits are encrypted at a time. Initially, a key(k) will be supplied as input to pseudorandom bit generator and then it produces a random 8-bit output which is treated as keystream. The resulted keystream will be of size 1 byte, i.e., 8 bits. Stream ciphers are fast because they encrypt data bit by bit or byte by byte, which makes them efficient for encrypting large amounts of data quickly.Stream ciphers work well for real-time communication, such as video streaming or online gaming, because they can encrypt and decrypt data as it's being transmitted.

Key Points of Stream Cipher

1. Stream Cipher follows the sequence of pseudorandom number stream.
2. One of the benefits of following stream cipher is to make cryptanalysis more difficult, so the number of bits chosen in the Keystream must be long in order to make cryptanalysis more difficult.
3. By making the key more longer it is also safe against brute force attacks.
4. The longer the key the stronger security is achieved, preventing any attack.

5. Keystream can be designed more efficiently by including more number of 1s and 0s, for making cryptanalysis more difficult.
6. Considerable benefit of a stream cipher is, it requires few lines of code compared to block cipher.

Encryption

For Encryption,

- Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
- The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

Example:

Plain Text : 10011001
Keystream : 11000011
Cipher Text : 01011010

What is Asymmetric Encryption:

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key. Asymmetric encryption has several advantages over symmetric encryption, which uses the same key for both encryption and decryption. One of the main advantages is that it eliminates the need to exchange secret keys, which can be a challenging process, especially when communicating with multiple parties. Additionally, asymmetric encryption allows for the creation of digital signatures, which can be used to verify the authenticity of data. Asymmetric encryption is commonly used in various applications, including secure online communication, digital signatures, and secure data transfer. Examples of asymmetric encryption algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). Asymmetric encryption, commonly known as public-key cryptography, employs two distinct keys for encryption and decoding. The private key is a separate key from the public key that is kept private by the owner of the public key while the public key is made available to everyone. Anyone can encrypt a message using the public key, but only the holder of the private key can unlock it. With no chance of the communication being intercepted and read by a third party, anyone can send a secure message to the public key's owner. Asymmetric encryption is frequently used for secure internet communication, including email encryption, e-commerce, and online banking. Digital signatures, which are used to confirm the legitimacy of digital documents and messages, are another application for it.

Advantages of Asymmetric Encryption

Asymmetric encryption also known as public key cryptography is a method of cryptography that uses two different keys to encrypt and decrypt data, here are some advantages of asymmetric encryption: –

- **Enhanced Security:** Asymmetric encryption provides a higher level of security compared to symmetric encryption where only one key is used for both encryption and decryption with asymmetric encryption a different key is used for each process and the private key used for decryption is kept secret by the receiver making, it harder for an attacker to intercept and decrypt the data.
- **Authentication:** Asymmetric encryption can be used for authentication purposes which means that the receiver can verify the sender s identity. This is achieved by the sender encrypting a message with their private key which can only be decrypted with their public key if the receiver can successfully decrypt the message, it proves that it was sent by the sender who has the corresponding private key.
- **Non-repudiation:** Asymmetric encryption also provides non-repudiation which means that the sender cannot deny sending a message or altering its contents this is because the message is encrypted with the sender s private key and only their public key can decrypt it . Therefore, the receiver can be sure that the message was sent by the sender and has not been tampered with.
- **Key distribution:** Asymmetric encryption eliminates the need for a secure key distribution system that is required in symmetric encryption with symmetric encryption, the same key is used for both encryption and decryption and the key needs to be securely shared between the sender and the receiver asymmetric encryption, on the other hand, allows the public key to be shared openly and the private key is kept secret by the receiver.
- **Versatility:** Asymmetric encryption can be used for a wide range of applications including secure email communication online banking transactions and e-commerce it is also used to secure SSL/TSL connections which are commonly used to secure internet traffic.

Overall, the use of asymmetric encryption offers enhanced security authentication non-repudiation key distribution, and versatility these advantages make it a widely used and effective method for protecting sensitive data in various applications.

Example of Asymmetric Encryption

Email communication is one way to show asymmetric encryption in action. Let’s say Alice and Bob have a public-private key pair and Alice wishes to send Bob an encrypted message. Using Bob’s public key, Alice encrypts her message before sending it to him. Bob uses his private key to decrypt the message after receiving it encrypted.

For instance, Alice composes and encrypts an email for Bob using Bob’s public key. She follows up by sending Bob the encrypted email. After receiving the email, Bob uses his private key to decrypt it so that it may be read. As a result, Alice can communicate Bob securely without being concerned that the message’s content will be viewed by someone else.

With the use of the matching private key, only the intended recipient may decode and read the email, guaranteeing the confidentiality of its contents. To provide secure and private

communication over the internet, asymmetric encryption is commonly employed in a variety of communication methods, including messaging apps, digital signatures, and file encryption.

The main features of asymmetric encryption (also known as public-key cryptography) are:

1. **Dual keys:** Asymmetric encryption uses a pair of keys, including a public key and a private key. The public key can be freely shared with anyone, while the private key is kept secret and known only to the key owner.
2. **Encryption and decryption:** Asymmetric encryption uses the public key to encrypt data and the private key to decrypt data. This allows secure communication between two parties without the need to exchange secret keys.
3. **Digital signatures:** Asymmetric encryption enables the creation of digital signatures, which can be used to verify the authenticity of data. A digital signature is created by encrypting a hash of the data with the sender's private key.
4. **Secure key exchange:** Asymmetric encryption allows for secure key exchange, which is a critical feature in secure communication. For example, the Diffie-Hellman key exchange algorithm uses asymmetric encryption to establish a shared secret key between two parties without exchanging the key itself.
5. **Security:** Asymmetric encryption is considered more secure than symmetric encryption because it eliminates the need to exchange secret keys, which can be a security risk. Additionally, the private key is kept secret, which makes it harder for attackers to intercept or tamper with the data.
6. **Slow processing:** Asymmetric encryption is slower than symmetric encryption because it involves more complex mathematical operations. This can make it less suitable for applications that require fast data processing.

RSA Algorithm in Cryptography:

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client's public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases

exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Let us learn the mechanism behind the RSA algorithm : >> Generating Public Key:

Select two prime no's. Suppose **P = 53 and Q = 59.**
Now First part of the Public key : n = P*Q = 3127.
We also need a small exponent say **e :**
But e Must be
An integer.
Not be a factor of Φ(n).
1 < e < Φ(n) [Φ(n) is discussed below],
Let us now consider it to be equal to 3.
Our Public Key is made of n and e

>> Generating Private Key:

We need to calculate Φ(n) :
Such that **Φ(n) = (P-1)(Q-1)**
so, Φ(n) = 3016
Now calculate Private Key, **d :**
d = (k*Φ(n) + 1) / e for some integer k
For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011) Now we will encrypt **"HI"**:

Convert letters to numbers : H = 8 and I = 9
Thus **Encrypted Data c = (89e)mod n**
Thus our Encrypted Data comes out to be 1394
Now we will decrypt **1394** :
Decrypted Data = (cd)mod n
Thus our Encrypted Data comes out to be 89
8 = H and I = 9 i.e. "HI".

ElGamal Encryption Algorithm

ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message. This cryptosystem is based on the difficulty of finding **discrete logarithm** in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}.

Idea of ElGamal cryptosystem:

Suppose Alice wants to communicate with Bob.

1. Bob generates public and private keys:
    - Bob chooses a very large number **q** and a cyclic group $\mathbf{F}_q$.

- From the cyclic group $\mathbf{F}_q$, he choose any element **g** and an element **a** such that gcd(a, q) = 1.
- Then he computes $h = g^a$.
- Bob publishes **F**, $\mathbf{h = g^a}$, **q**, and **g** as his public key and retains **a** as private key.

2. Alice encrypts data using Bob's public key :
    - Alice selects an element **k** from cyclic group **F** such that gcd(k, q) = 1.
    - Then she computes $p = g^k$ and $s = h^k = g^{ak.}$
    - She multiples s with M.
    - Then she sends $(p, M*s) = (g^k, M*s)$.
3. Bob decrypts the message :
    - Bob calculates $s' = p^a = g^{ak}$.
    - He divides M*s by s' to obtain M as $s = s'$.

Elliptic Curve Cryptography:

Cryptography is the study of techniques for secure communication in the presence of adversarial behavior. Encryption uses an algorithm to encrypt data and a secret key to decrypt it. There are 2 types of encryption:

1. **Symmetric-key Encryption (secret key encryption):** Symmetric-key algorithms are cryptographic algorithms that employ the same cryptographic keys both for plaintext encryption and ciphertext decoding. The keys could be identical, or there could be a simple transition between them.
2. **Asymmetric-key encryption (public key encryption):** Asymmetric-key algorithms encrypt and decrypt a message using a pair of related keys (one public key and one private key) and safeguard it from unauthorized access or usage.

The following topics of Elliptic Curve Cryptography will be discussed here:

1. **Introduction to Elliptic Curve Cryptography**
2. **History of Elliptic Curve Cryptography**
3. **Components of Elliptic Curve Cryptography**
4. **Elliptic Curve Cryptography Algorithms**
5. **Application of Elliptic Curve Cryptography**
6. **ECC vs RSA**
7. **Elliptic Curve Diffie-Hellman Protocol Implementation**
8. **Types of Security Attacks**
9. **Benefits of Elliptic Curve Cryptography**
10. **Limitations of Elliptic Curve Cryptography**
11. **Conclusion**

Introduction to Elliptic Curve Cryptography

ECC, as the name implies, is an asymmetric encryption algorithm that employs the algebraic architecture of elliptic curves with finite fields.

- Elliptic Curve Cryptography (ECC) is an encryption technology comparable to RSA that enables public-key encryption.
- While RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys.
- Victor Miller and Neal Koblitz separately proposed elliptic curve ciphers in the mid-1980s. On a high level, they are analogs of actual public cryptosystems in which modular arithmetic is substituted by elliptic curve operations.

History of Elliptic Curve Cryptography

- Neal Koblitz and Victor S. Miller independently proposed the use of elliptic curves in encryption in 1985.
- Elliptic curve cryptography algorithms entered wide use from 2004 to 2005.
- In the mid-1980s, researchers found that examining elliptic curves could lead to the discovery of new sources of difficult problems. Elliptic Curve Cryptography (ECC) introduced a new degree of security to public key cryptosystems, that provide combined encryption and digital signature services.
- The security of elliptic curve cryptosystems, like that of all public-key cryptosystems, is based on tough mathematical issues at the core. Given two elliptic curve points G and Y, where $Y = kG$.
- The term "elliptic curve" is derived from the ellipse. Elliptic curves were discovered in the form of the Diophantine equation for c, after the 17th century. Furthermore, while calculating the surface of the ellipse is simple, calculating the circumference of the ellipse is difficult. The equation can be simplified to an integral: