What is Encryption?

Data can be secured with encryption by being changed into an unintelligible format that can only be interpreted by a person with the proper decryption key. Sensitive data, including financial and personal information as well as communications over the internet, is frequently protected with it.

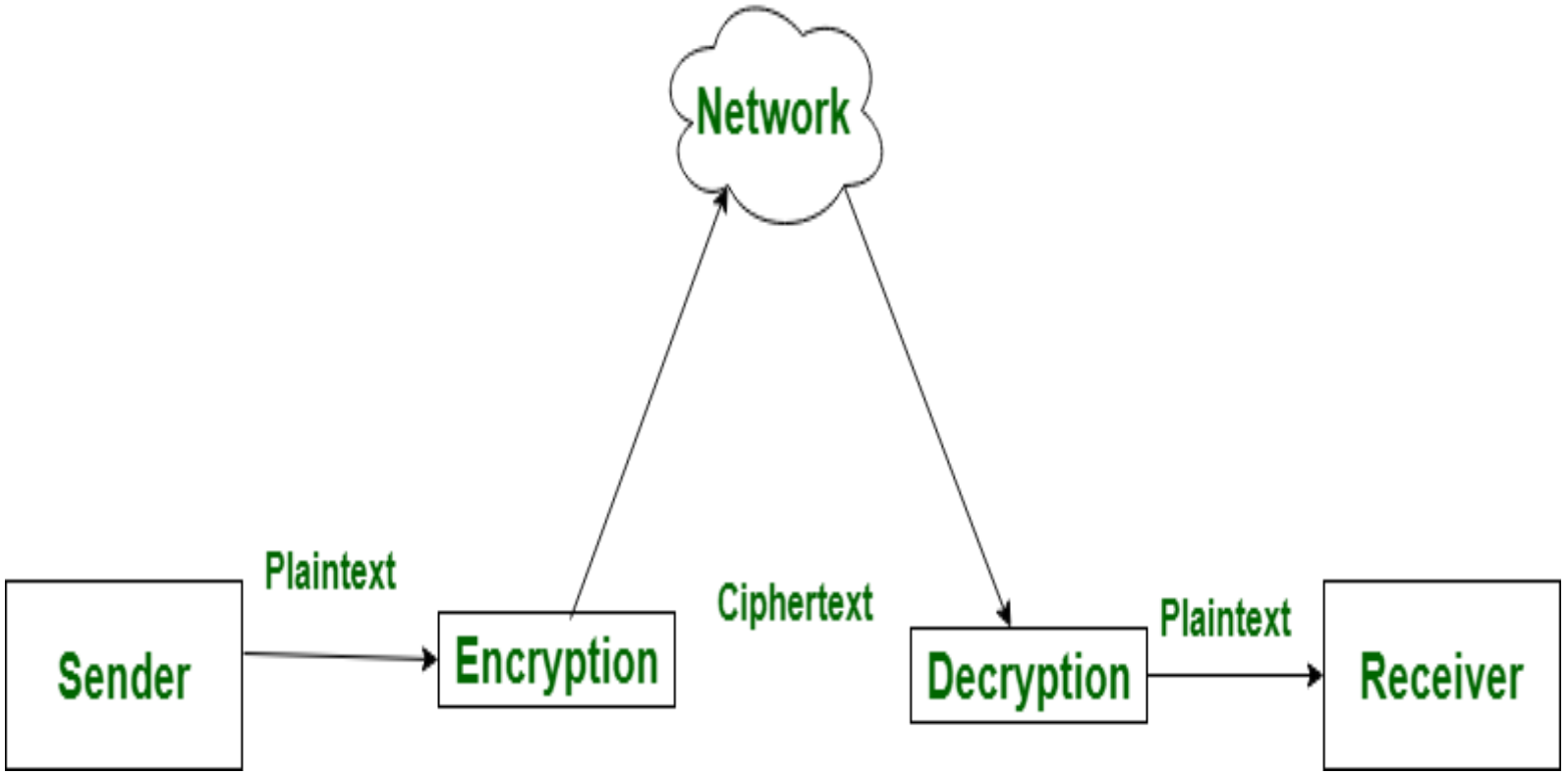
Application of Encryption :

1. **Online Banking:** To secure transactions, use online banking.
2. **Email security:** To safeguard the contents of emails.
3. **Secure Messaging:** To protect the privacy of discussions.
4. **Data Storage:** To prevent unwanted access to data that has been stored.

What is Decryption?

- To make encrypted data comprehensible again, it must first be decrypted and then put back into its original format. To access and utilize the protected information, authorized parties must follow this procedure.
- **Real-Life Examples of Encryption and Decryption.**
- **WhatsApp Messaging: It encrypts** It encrypts communications from beginning to end so that only the sender and recipient can read them.
- **HTTPS websites:** Encrypt user data to prevent third parties from intercepting it.
- **Encrypted Email Services:** Email services that use encryption, like Proton Mail, protect email contents.

Figure :


Network
Plaintext
Sender
Encryption
Ciphertext
Decryption
Plaintext
Receiver

Plain Text:

- **It is Simply a Message, Text or Information in Human readable form.**
- Plaintext is readable information that can be understood by humans or machines without the need for decryption tools or keys.

- For Example: “ Hello World “ , “ Online “

Cipher Text :

- **It is the Output of Input Plain Text which Converts after a encryption process.**
- **Cipher Text it unreadable form of a Plain Text.**
- **For ex: “ w h e l r l d o l o “**
- This Process of Converting plaintext to Cipher text is called encryption.
- And the Process of Converting cipher text back to plaintext is called decryption.

- Plain text: HOW ARE YOU
- Key : NCBTZQARX
- H O W A R E Y O U
- 7 14 22 0 17 4 24 14 20

  +
- N C B T Z Q A R X
- 13 2 1 19 25 16 0 17 23

  ---

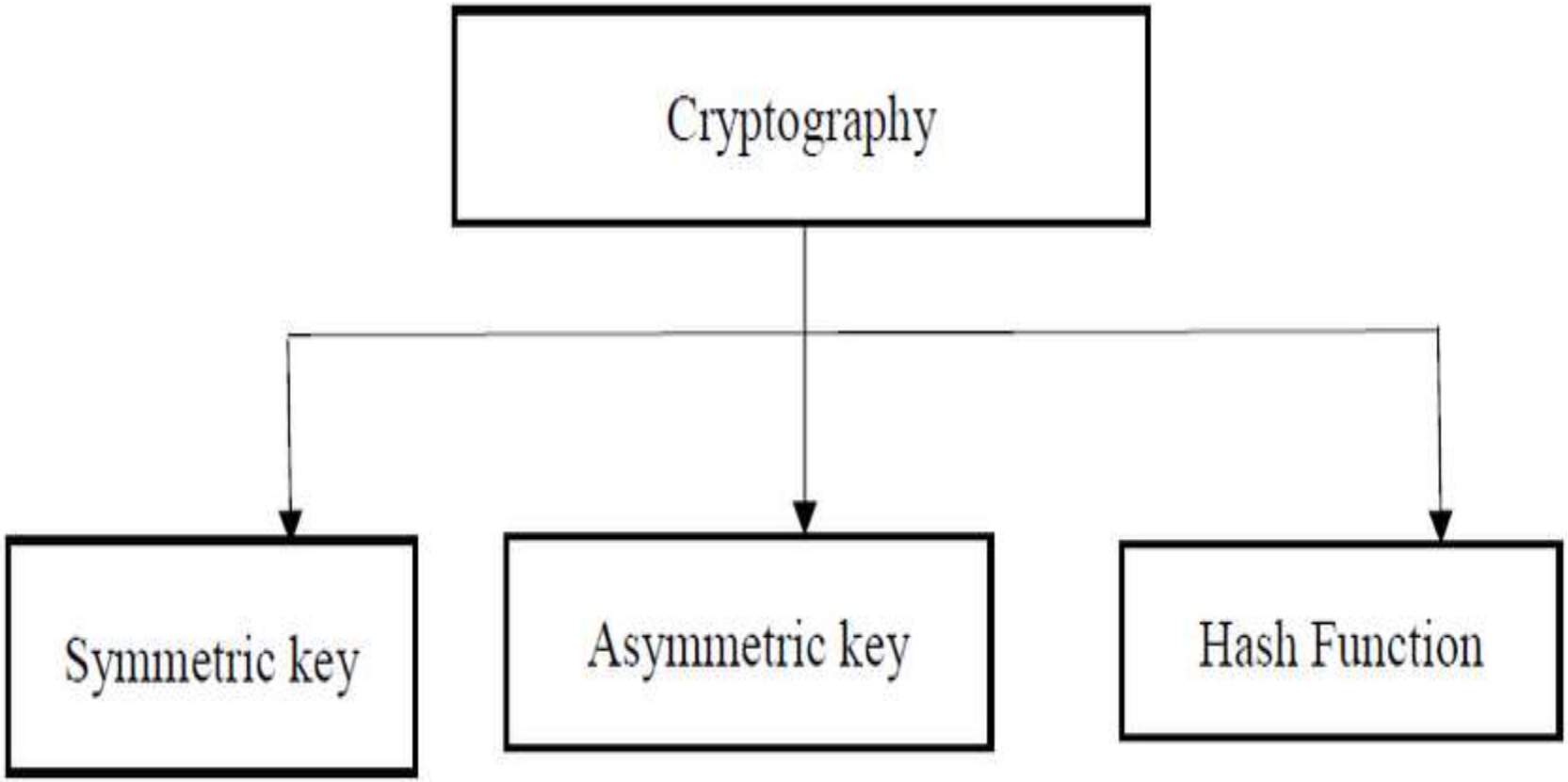
  20 16 23 19 42 20 24 31 43
- Subtract 26 if > 26: 20 16 23 19 16 20 24 5 17
- Cipher text : U Q X T Q U Y F R
- Cipher text : UQXTQUYFR
- **The formula of encryption is:**
- $E_n(x) = (x + n) \bmod 26$
- **The formula of decryption is:**
- $D_n(x) = (xi - n) \bmod 26$

- # code

```
def caesar_cipher(plain_text, shift):
    cipher_text = " "
    for char in plain_text:
        if char.isalpha():
            # Determine the offset based on the shift value
            offset = ord('a') if char.islower() else ord('A')
            # Apply the shift to the character and wrap around if
    necessary
            cipher_char = chr((ord(char) - offset + shift) % 26 + offset)
            cipher_text += cipher_char
        else:
            # Leave non-alphabetic characters unchanged
            cipher_text += char
    return cipher_text
```

Types of cryptography :

* **There are mainly three types of cryptography.**



1. Symmetric Key Cryptography

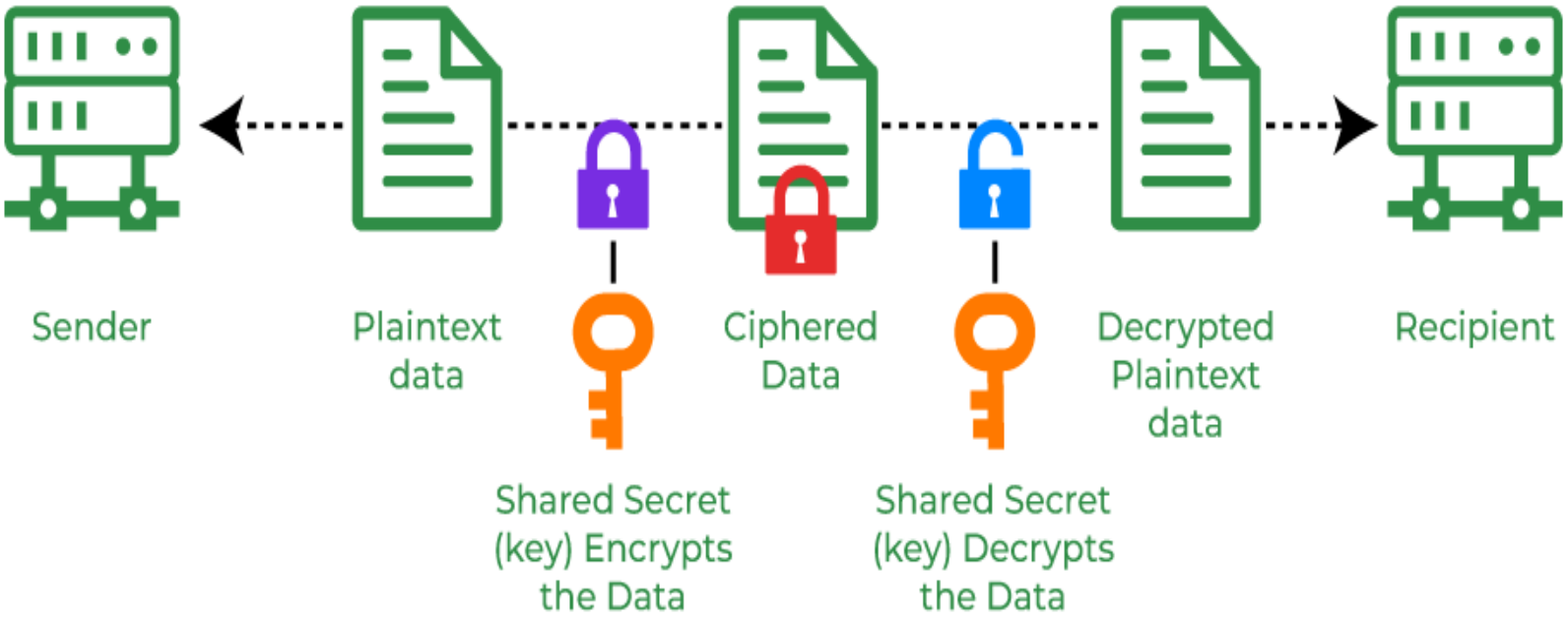
* It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages.

* **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 use systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES).

* So we can use the same key to lock and unlock messages. It is like having a secret code that you and your friend both know. It is very simple and fast. The two parties share the key in a secure way.

Symmetric Key cryptography



2 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.

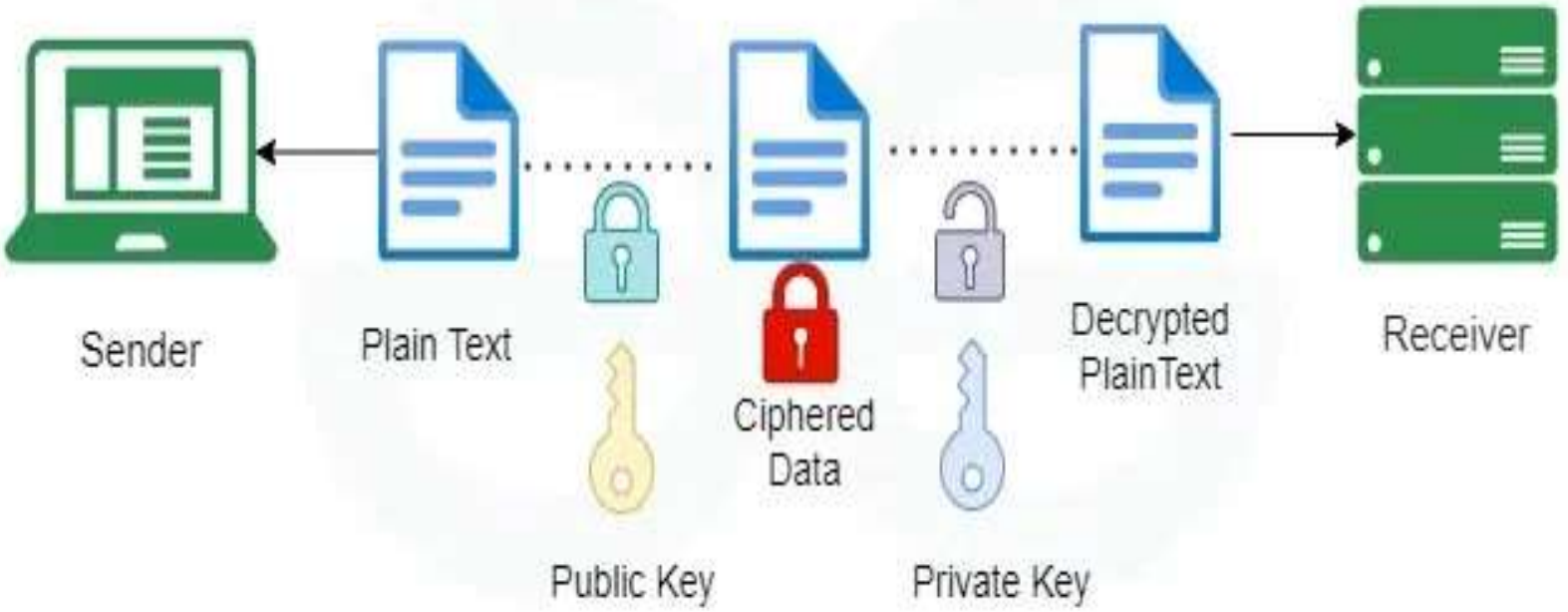
➡ Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key.

➡ The most popular asymmetric key cryptography algorithm is the RSA algorithm.

Rivest Shamir Adleman (RSA) is a well-known public-key or asymmetric cryptographic algorithm. It protects sensitive data through encryption and decryption using a private and public key pair.

➡ First introduced in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, RSA is named after their last initials.

Asymmetric Key Cryptography



Hash Functions

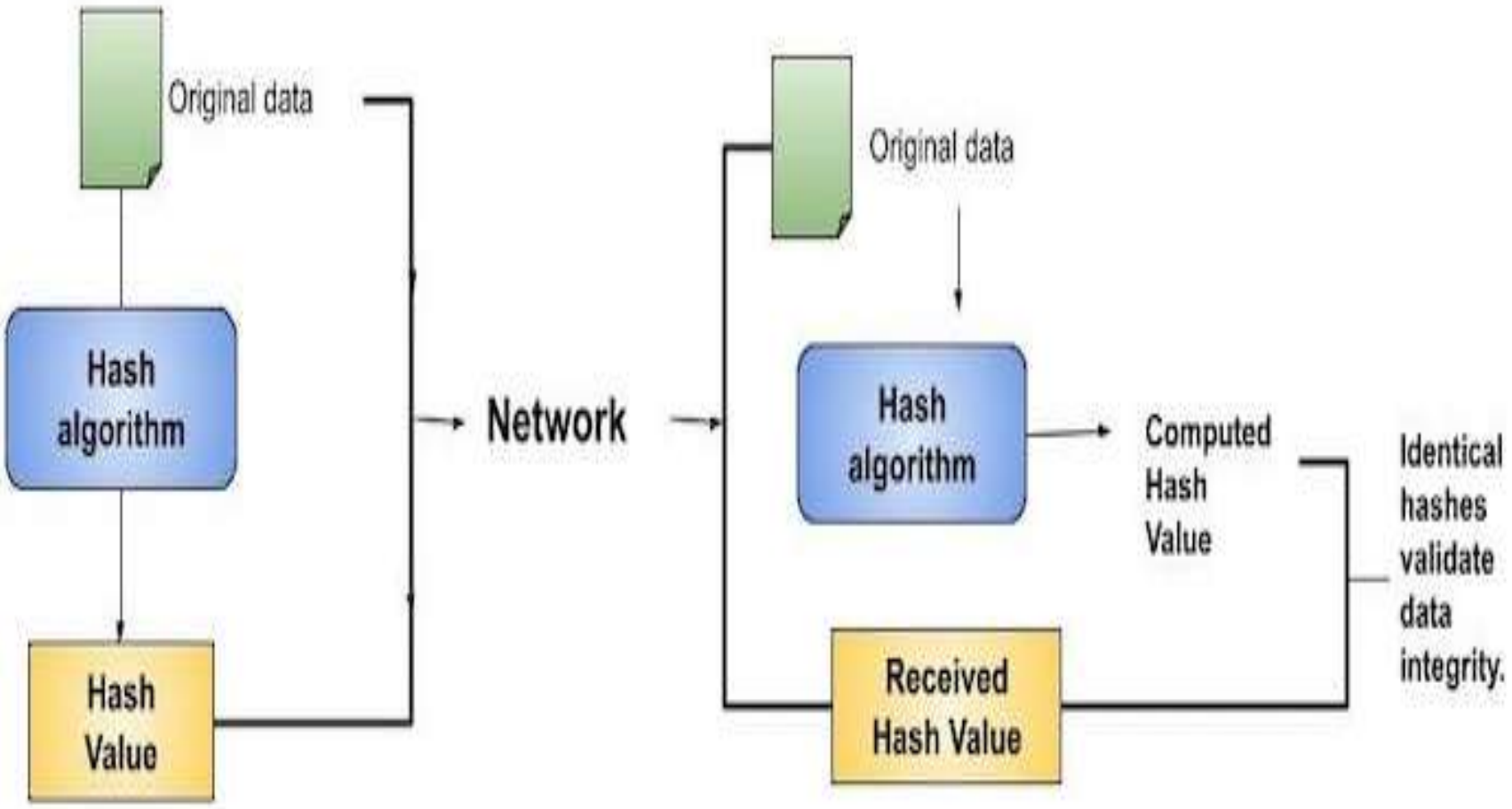
- There is no usage of any key in this algorithm.
- A hash function in cryptography is like a mathematical function that takes various inputs, like messages or data, and transforms them into fixed-length strings of characters.

  Many operating systems use hash functions to encrypt passwords.

  example: Cryptocurrency, password security, and communication security all use hash functions.

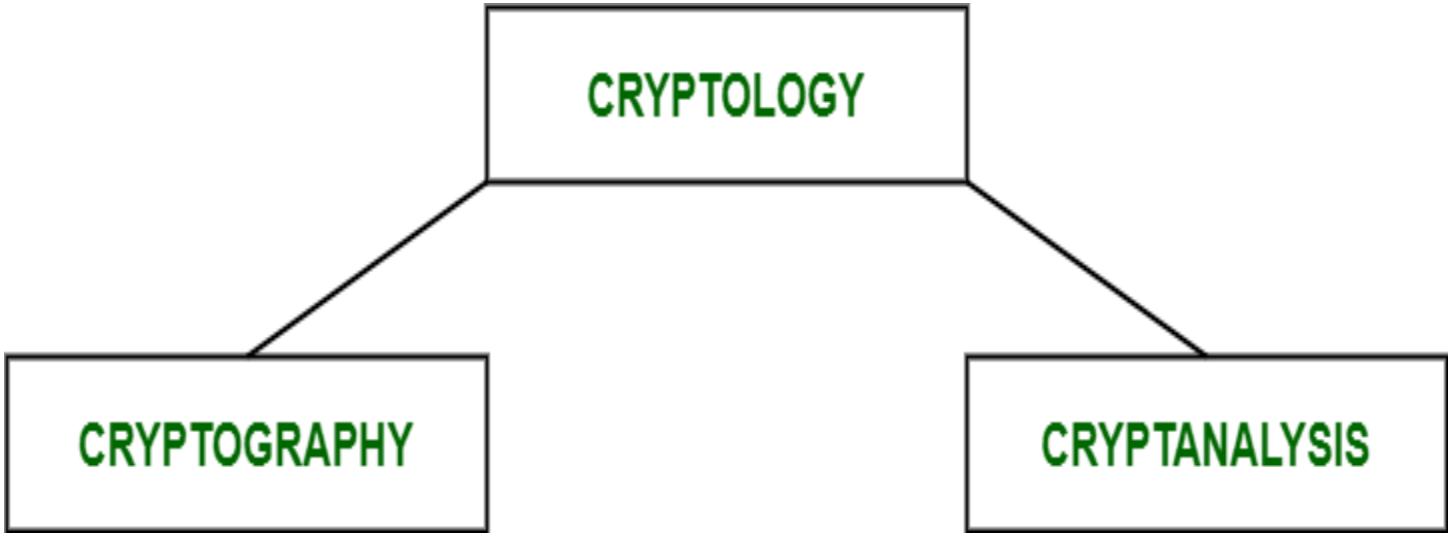
  Convert to messages to Hash Function as a Characters values.

Message	Hash Function	Output (Hash Value)
(128-bit, 16-byte)	32 characters	3A10 0B15 B943 0B17 11F2 E38F 0593 9A9A

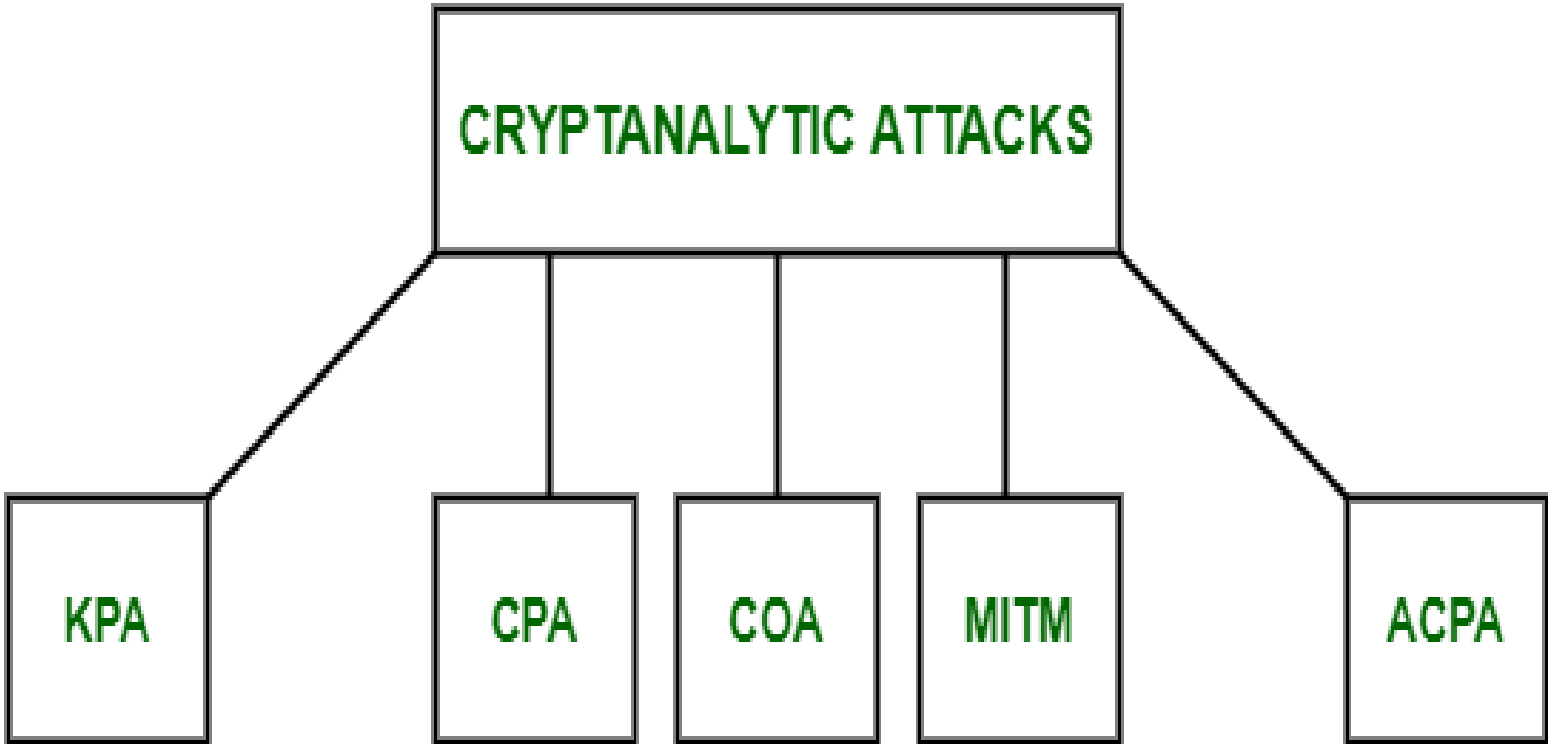

Original data
Hash algorithm
Hash Value
Network
Original data
Hash algorithm
Computed Hash Value
Received Hash Value
Identical hashes validate data integrity.

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**.



To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called **Cryptanalytic attacks.**



KPA : Known-Plaintext Analysis
CPA : Chosen-Plaintext Analysis
COA : Ciphertext-Only Analysis
MITM : Man-In-The-Middle
ACPA : Adaptive Chosen-Plaintext Analysis.

NETWORK SECURITY :

→ Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

Protocols : Digital Signature Standards (DSS)

- Sign any document online efficiently and organize your workflow with the user-friendly and highly secure e-signature platform **SignNow.** With this, you can easily share any electronic documents for signature, keep track of them, and even sign the documents on any device.

It is used to ensure the validity and integrity of a message, software, or digital document. The National Institute of Standards and Technology (NIST).

- **Digital Signature Standard (DSS)** is a Federal Information Processing Standard(FIPS) which defines algorithms that are used to generate digital signatures with the help of Secure Hash Algorithm(SHA) for the authentication of electronic documents.

- You can refer the below diagram for RSA here,

  M = Message or Plaintext

  H = Hash Function

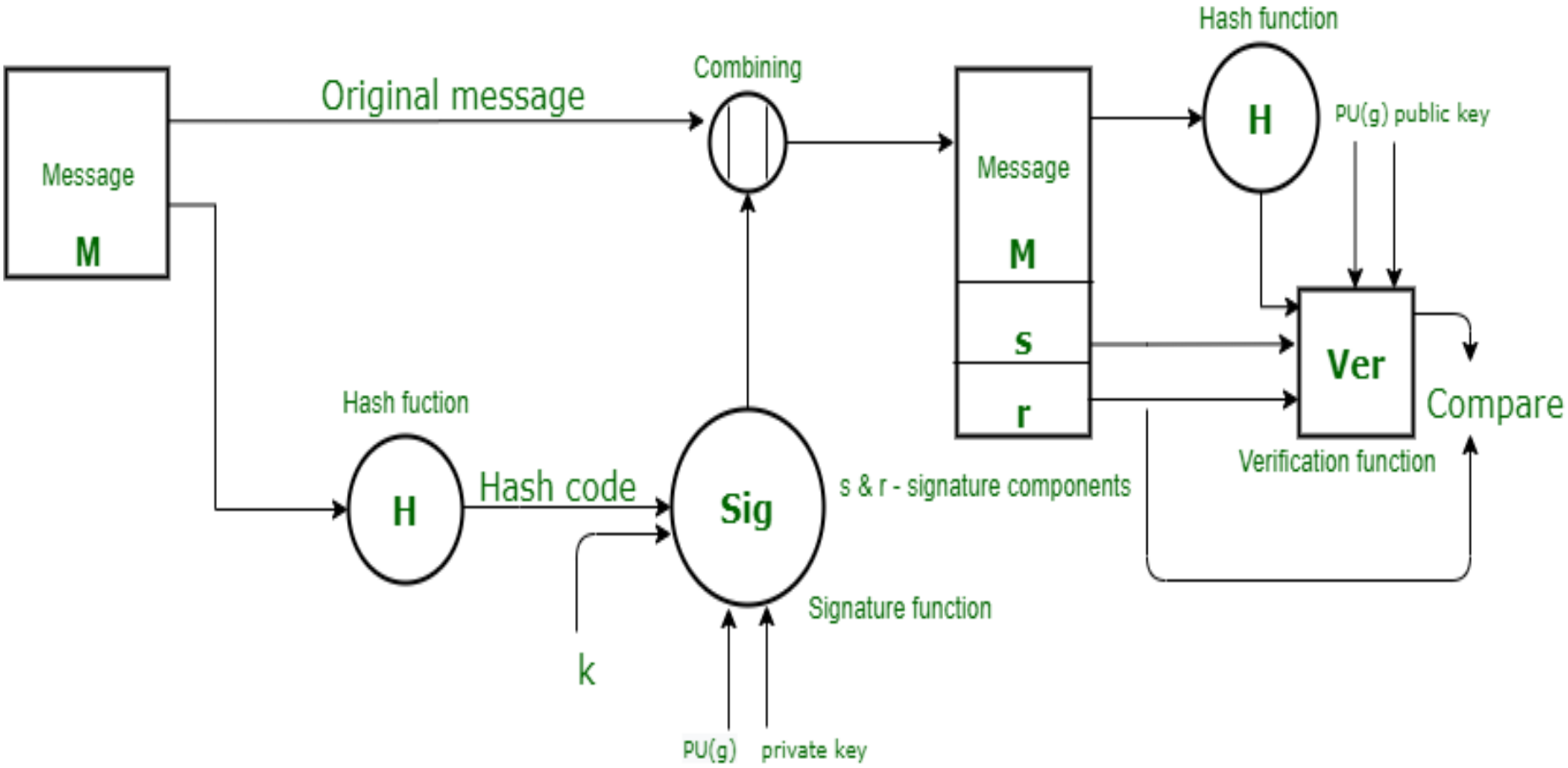
  || = bundle the plaintext and hash function (hash digest)

  E = Encryption Algorithm

  D = Decryption Algorithm

  PU_a = Public key of sender

  PR_a = Private key of sender


SENDER A
RECEIVER B
Message
M
Original message
Combining
Hash function
H
PU(g) public key
Message
M
s
r
Ver
Compare
Verification function
Hash fuction
H
Hash code
Sig
s & r - signature components
Signature function
k
PU(g)
private key

- **Sender Side :**
- In DSS Approach, a hash code is generated out of the message and following inputs are given to the signature function –
- 1. The hash code.
- 2. The random number ‘k’ generated for that particular signature.
- 3. The private key of the sender i.e., PR(a).
- 4. A global public key(which is a set of parameters for the communicating principles) i.e., PU(g).

- **Receiver Side :**
- At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs –
- 1. The hash code generated by the receiver.
- 2. Signature components ‘s’ and ‘r’.
- 3. Public key of the sender.
- 4. Global public key.

The output of the verification function is compared with the signature component ‘r’. Both the values will match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.

Electronic Mail Security

- Email (short for electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks.
- With the help of this, we can send and receive text-based messages, often an attachment such as documents, images, or videos, from one person or organization to another.

- **What is Email Security?**

  Basically**, Email security** refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage. It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware.

Types of Email Attacks

- Cyber criminals use many different to hack email, and some methods can cause considerable damage to an organization's data and/or reputation. Malware, which is malicious software used to harm or manipulate a device or its data, can be placed on a computer using each of the following attacks.

- **Phishing:**
- **Spam**
- **Spoofing**
- **Identity Theft**

→ **Steps should be taken to Secure Email :**

Choose a secure password: Password must be at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.

- **Two-factor authentication:** Activate the two-factor authentication, which adds an additional layer of security to your email account by requiring a code in addition to your password.

- **Upgrade Your Application Regularly :**

  People now frequently access their email accounts through apps, although these tools are not perfect and can be taken advantage of by hackers. A cybercriminal might use a vulnerability, for example, to hack accounts and steal data or send spam mail. Because of this, it's important to update your programs frequently.

- **Beware of phishing scams:** Hackers try to steal your personal information by pretending as someone else in phishing scams. Be careful of emails that request private information or have suspicious links because these are the resources of the phishing attack.

MIME

- **Multipurpose Internet Mail Extension** (MIME).
- is a standard that was proposed by Bell Communications in 1991 in order to expand the limited capabilities of email.
- MIME is a kind of add-on or a supplementary protocol that allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet audio, video, images, application programs as well.
- Since MIME was able to transfer only text written file in a limited size English language with the help of the internet. At present, it is used by almost all e-mail related service companies such as Gmail, Yahoo-mail, Hotmail.

Need of MIME Protocol

- MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.
2. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.
3. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

- **Working of MIME** – Suppose a user wants to send an email through a user agent and it is in a non-ASCII format so there is a MIME protocol that converts it into 7-bit NVT ASCII format. The message is transferred through the e-mail system to the other side in the 7-bit format now MIME protocol again converts it back into non-ASCII code and now the user agent of the receiver side reads it and then information is finally read by the receiver. MIME header is basically inserted at the beginning of any e-mail transfer.

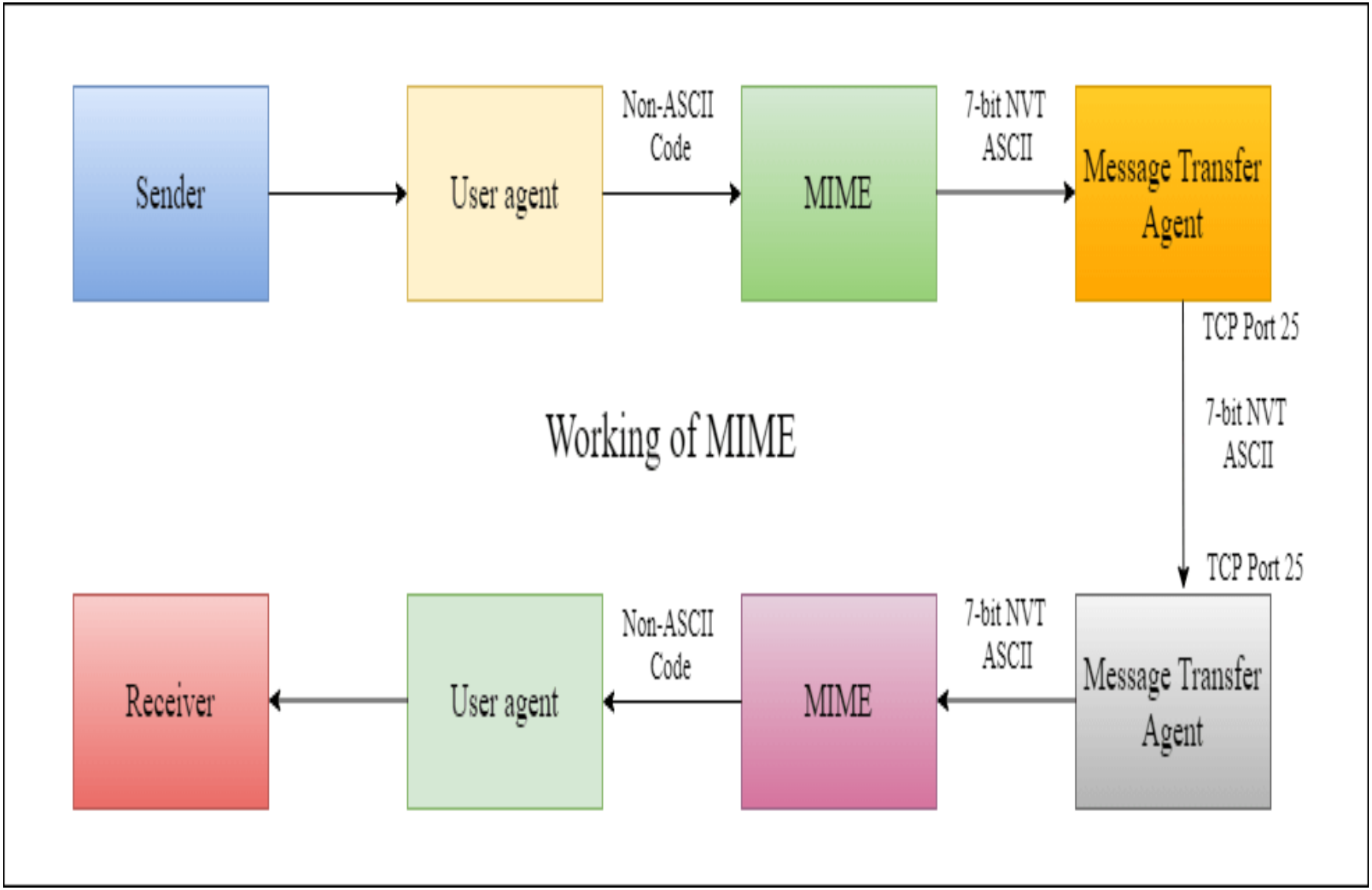
- **Features of MIME Protocol:**

1. It supports multiple attachments in a single e-mail.
2. It supports the non-ASCII characters.
3. It supports unlimited e-mail length.
4. It supports multiple languages.

Advantage of the MIME :

- It is capable of sending various types of files in a message, such as text, audio, video files.
- also provides the facility to send and receive emails in different languages like Hindi, French, Japanese, Chinese etc.
- It also provides the facility of connecting HTML and CSS to email, due to which people can design email as per their requirement and make it attractive and beautiful.
- It is capable of sending the information contained in an email regardless of its length.

It assigns a unique id to all e-mails.

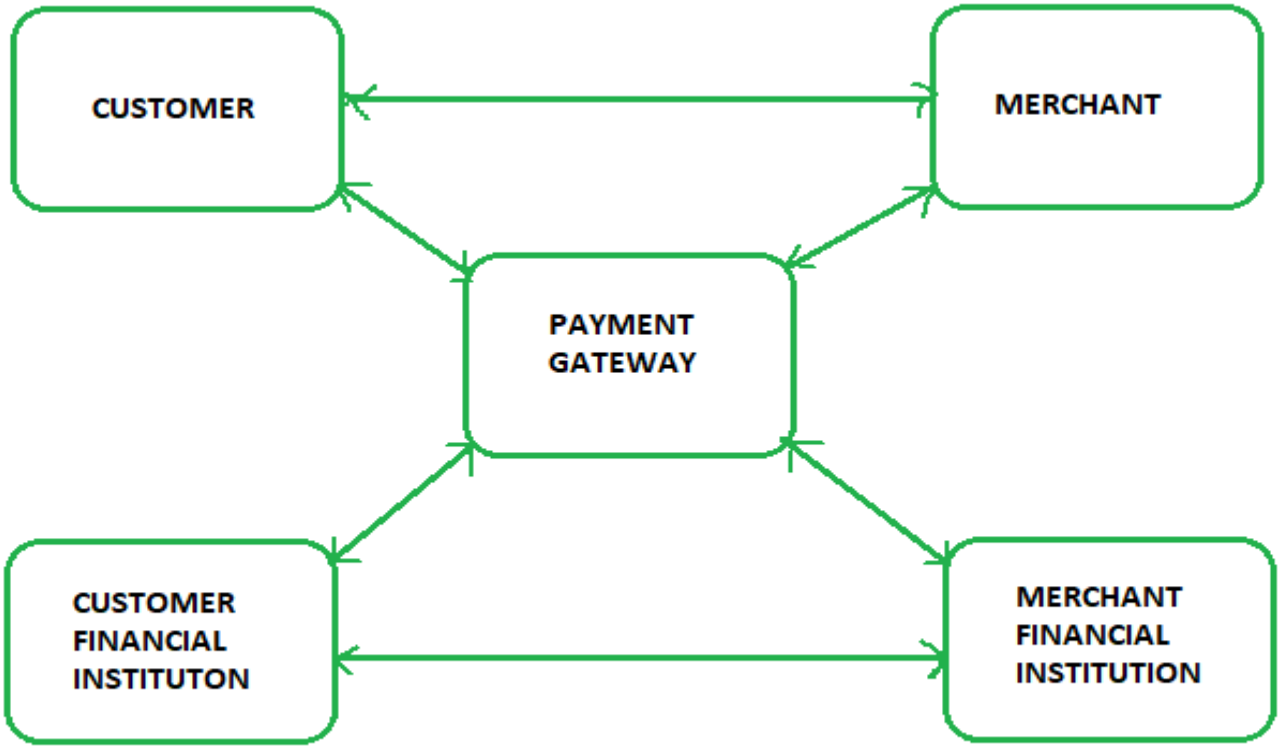

Sender
User agent
Non-ASCII Code
MIME
7-bit NVT ASCII
Message Transfer Agent
TCP Port 25
7-bit NVT ASCII
TCP Port 25
Working of MIME
Receiver
User agent
Non-ASCII Code
MIME
7-bit NVT ASCII
Message Transfer Agent

Web Security

- What is Web Security ?

  Web Security is an online security means Internet Security.

  solution that will restrict access to harmful websites, stop web-based risks, and manage staff internet usage. Web Security is very important nowadays. Websites are always prone to security threats/risks. For example- when you are transferring data between Client and server and you have to protect that data that security of data is your web security.


CUSTOMER
MERCHANT
PAYMENT
GATEWAY
CUSTOMER
FINANCIAL
INSTITUTON
MERCHANT
FINANCIAL
INSTITUTION