Introduction of Cyber Security

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity posture has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, a unified threat management gateway system can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation. People, processes, and technology must all complement one another to create an effective defense from cyberattacks.

People

Users must understand and comply with basic data protection and privacy security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

Processes

Organizations must have a framework for how they deal with both attempted and successful cyberattacks. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, Domain Name System (DNS) filtering, malware protection, antivirus software, and email security solutions.

Definition & Importance

Cyber Security is the technique of **protecting** your systems, digital devices, networks, and all of the data stored in the devices from cyber attacks. By acquiring knowledge of cyber attacks and cyber security we can secure and defend ourselves from various cyber attacks like **phishing** and **DDoS** attacks.

Phishing: Phishing is a **cyber attack** where hackers trick users into revealing sensitive data like **passwords, banking details, or session tokens** through fake emails, messages, or websites. It uses social engineering to impersonate trusted sources and often includes **malicious links or attachments** to steal information.

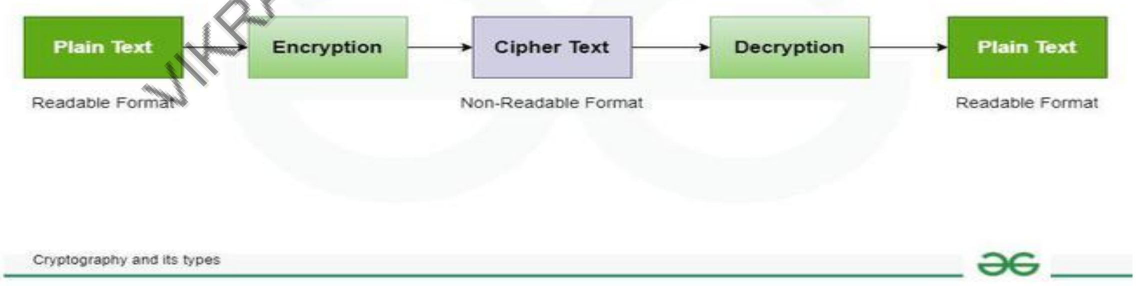
DDoS: A **Distributed Denial-of-Service (DDoS) attack** is a cyberattack where hackers overload a network, server, or website with excessive traffic, making it slow or completely unavailable. Attackers use **botnets** (infected devices) and **amplification techniques** (DNS reflection, NTP amplification) to flood the target. DDoS attacks disrupt services, cause downtime, and bypass security defenses like firewalls and rate limiting.

One crucial aspect of cybersecurity is Encryption, which ensures that sensitive information remains private and readable only to authorized users. This is especially important for **financial transactions, personal communications, and corporate databases** to prevent data theft and unauthorized access

In short, cybersecurity keeps your online world safe and secure. It ensures that sensitive information remains confidential, intact, and accessible only to authorized users. Whether it's securing personal information, financial transactions, or corporate databases.

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.



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.

What is Plaintext

Plaintext is an encryption technique, that converts an encrypted message. It refers to any readable data, including binary files, that can be seen or used without the requirement for a decryption key or device. Plain text is often used for several tasks, such as document creation, coding, and email communication. Plaintext implies any communication, document, or file that is meant to be or has already been encrypted. A cryptosystem accepts plaintext as input and produces ciphertext as output.

Plaintext In cryptography plain readable text, is either before it is encrypted into ciphertext or after it is decoded. Plaintext refers to any communication, document, file, or other type of data that is not encrypted. Plaintext kept in a computer file must be protected since its contents are fully accessible and hence potentially actionable if stolen, leaked, or distributed without authorization. If data is to be saved, the storage media, device, components, and backups must all be secure. If plaintext is saved in a computer file, the storage media, the system, and its components, and any backups must all be secure. When sensitive data is handled on computers with removable mass storage, the physical security of the removed disk is crucial.

Applications of Plaintext

- Plaintext is used in command-line interfaces, which are text-based interfaces that allow you to communicate with computers. Humans can easily read and input commands using simple text.
- Plaintext in cryptography is used to write papers such as articles, reports, and essays since it is simple to read and understand and without any formatting or multimedia components that may be distracting.
- Plaintext is one of the formats used in email communication to transmit and receive messages. The messages are not structured and do not contain multimedia components.

Examples of Plaintext

- Plaintext is preferred in the majority of applications. For example, Plaintext should appear in a browser, word processor, or email client.

- Password protection for PowerShell scripts To prevent disclosing such credentials in their scripts, developers must exercise caution.
- Plaintext stored in computer files must be protected since unlawful theft, disclosure, or transfer exposes its contents, making them potentially actionable.
- These credentials are exposed if plaintext passwords are used in application configuration files. Developers that use unencrypted passwords in their source code are less likely to leak their credentials.
- They are protecting passwords in PowerShell scripts. Developers must use caution to prevent revealing such passwords in their programs.

Benefits of Plaintext

Below are some benefits of plaintext

- Plaintext offers a lot of advantages over rich text, including its simplicity, universality, and compatibility with any platform, device, or program.
- It is also lightweight, making it simple to store, back up, and transport.
- Plaintext is also searchable, readable, and editable by people and machines.
- Plaintext in cryptography is easy to open on different platforms.

Drawbacks of Plaintext

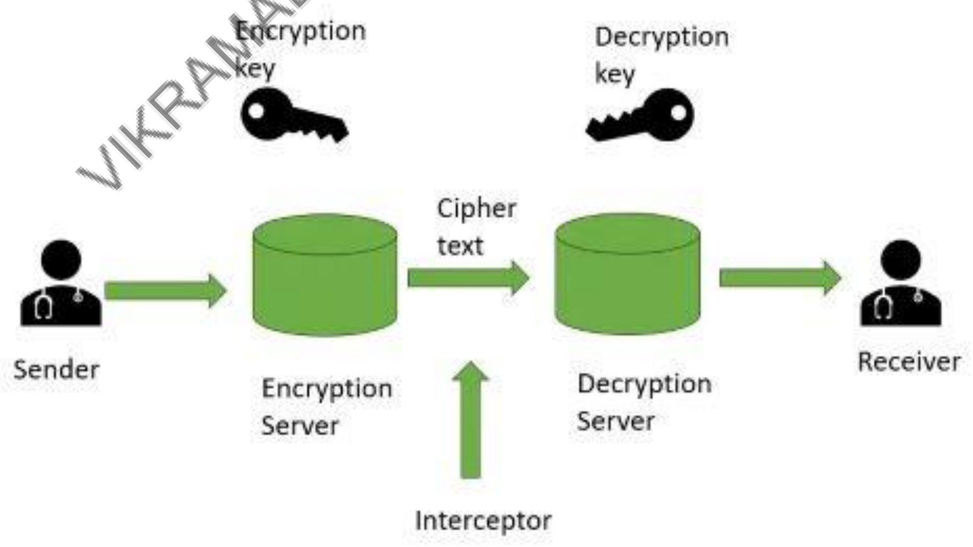
Below are some drawbacks of plaintext

- Plaintext, while typically easier to write and maintain, has several drawbacks as compared to rich text. For example, it lacks visual appeal, diversity, and focus, and does not accommodate multimedia features.
- Plaintext has no standardized process to specify the data format.
- Plaintext provides limited opportunities to highlight important sections, call your readers' attention to specific aspects, or give visual signals.
- Plaintext may not keep the document's original layout or look when viewed or printed, and it may fail to convey the intended content or tone without additional context or signals.

Ciphertext

Ciphertext is the jumbled-up, unreadable string created when you apply encryption to normal, legible data called plaintext. Only an intended recipient with the correct decryption key can convert ciphertext into plaintext. Encrypting plaintext into ciphertext makes the actual information illegible and incomprehensible to unauthorized people or systems. The understanding of the real worth of ciphertext in securing business data demands revisiting some of its basic characteristics and differences from plaintext:

1. **Definition and Purpose:** Ciphertext in cryptography means the scrambled output of an encryption process applied to plaintext. Its ordinary purpose is to maintain the confidentiality of information by turning it into a form that, for all practical purposes, would seem meaningless without the proper decryption key.
2. **Appearance:** Plaintext is directly readable to humans, whereas ciphertext often can be mistaken for random characters, numbers, or symbols. Obfuscation may therefore sometimes be carried out deliberately to make sure that the sender knows the original message or data being transmitted remains unknown to others.
3. **Security:** Plaintext is less secure since it can be read and understood by any entity that might get hold of the information. On the other hand, ciphertext offers quite a good level of security since it is only decoded by the entity or person with the correct decryption key or technique.
4. **Processing Requirements:** Plaintext can be processed, read, or manipulated directly. Ciphertext, however, needs to be decrypted before it can be read, processed, or operated on; hence, it brings along an added layer of complexity for extra security to handle the data at every single process.



Difference between Plaintext and Cipher text

Encryption algorithms perform complicated mathematical operations to turn plaintext into ciphertext. Using cryptographic keys, these algorithms scramble the original data, making it very hard—sometimes impossible—to reverse-engineer without an appropriate decryption key.

Let’s look at a simple example to illustrate this process.

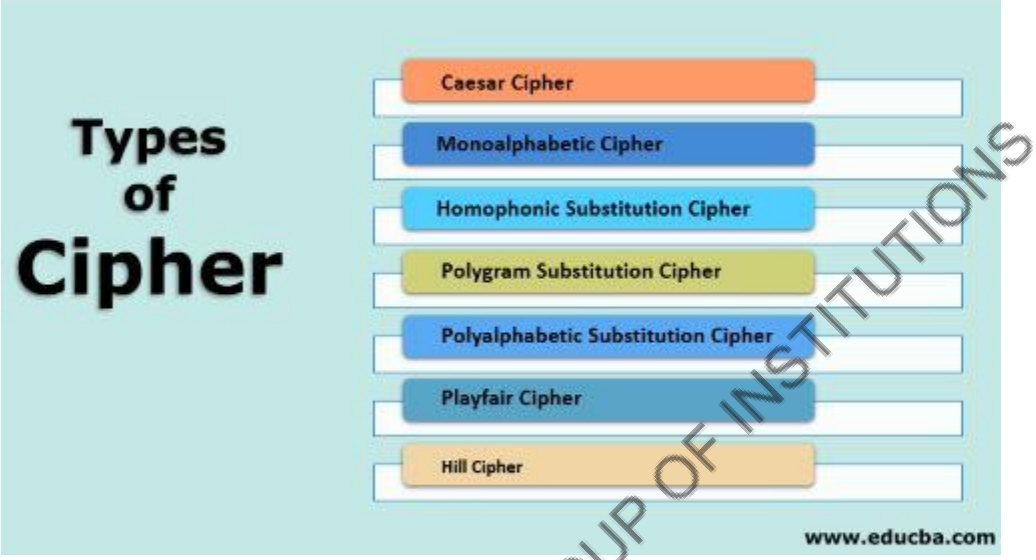
Consider the case where a business wants to securely send the message “CONFIDENTIAL REPORT” to a partner. Using a basic substitution cipher in which each letter is replaced by the letter three positions ahead in the alphabet, the steps would be:

Plaintext: CONFIDENTIAL REPORT**, Cipher text:** FRQILGHQWLDO UHSRUW

In this example, anyone intercepting the cipher text “FRQILGHQWLDO UHSRUW” gets a string of letters highly resembling randomness. However, this intended recipient can easily decipher this message into the original plaintext, because he knows that the encryption is done by shifting the letters three letters back. It is crucial to remember that the business encryption methodologies used in this real world, for example, are many times more advanced.

In modern encryption algorithms, complex mathematical functions are applied for encryption using very large keys, hence it is virtually impossible for unauthorized parties to decipher a cipher text without having the correct decryption key.

Types of Cipher


Types of Cipher
Caesar Cipher
Monoalphabetic Cipher
Homophonic Substitution Cipher
Polygram Substitution Cipher
Polyalphabetic Substitution Cipher
Playfair Cipher
Hill Cipher
www.educba.com

Caesar Cipher

It is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext. It is a simplest form of substitution cipher scheme.

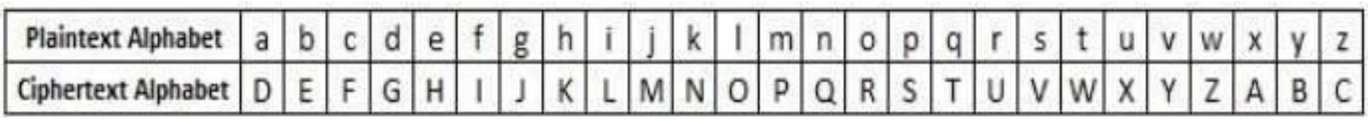
This cryptosystem is generally referred to as the **Shift Cipher**. The concept is to replace each alphabet by another alphabet which is ‘shifted’ by some fixed number between 0 and 25.

For this type of scheme, both sender and receiver agree on a ‘secret shift number’ for shifting the alphabet. This number which is between 0 and 25 becomes the key of encryption.

The name ‘Caesar Cipher’ is occasionally used to describe the Shift Cipher when the ‘shift of three’ is used.

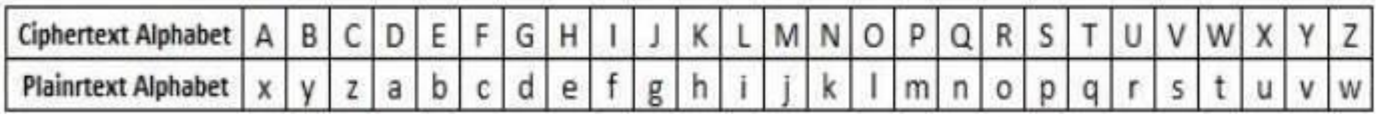
Process of Shift Cipher

- In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
- The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext ‘tutorial’ is encrypted to the ciphertext ‘WXWRULDO’. Here is the ciphertext alphabet for a Shift of 3 −



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
- He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence the ciphertext 'WXWRULDO' is decrypted to 'tutorial'. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown below –



Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plainrtext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Security Value

Caesar Cipher is **not a secure** cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

Monoalphabetic and Polyalphabetic Cipher

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalysis.

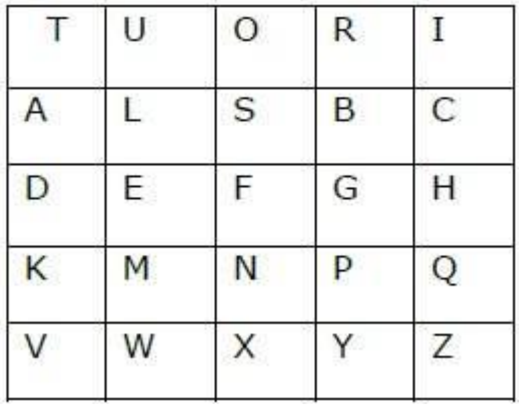
Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, **playfair and Vigenere Cipher are polyalphabetic ciphers**.

Playfair Cipher

In this scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher.

In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

The sender and the receiver deicide on a particular key, say 'tutorials'. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be –



T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

Process of Playfair Cipher

- First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message "hide money". It will be written as −
  HI DE MO NE YZ
- The rules of encryption are −
  - If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

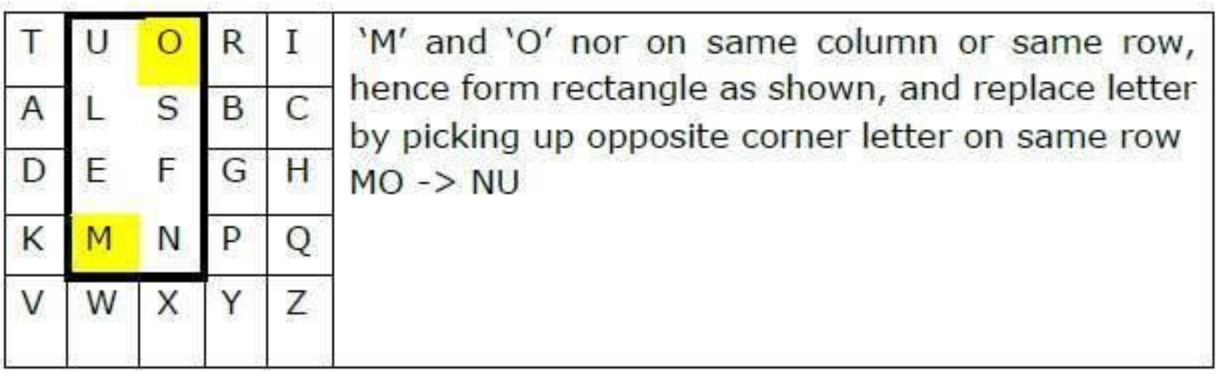
'H' and 'I' are in same column, hence take letter below them to replace. HI → QC

- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

'D' and 'E' are in same row, hence take letter to the right of them to replace. DE → EF

- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.



T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

'M' and 'O' nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row MO -> NU

Using these rules, the result of the encryption of 'hide money' with the key of 'tutorials' would be −

QC EF NU MF ZV

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Security Value

It is also a substitution cipher and is difficult to break compared to the simple substitution cipher. As in case of substitution cipher, cryptanalysis is possible on the Playfair cipher as well, however it would be against 625 possible pairs of letters (25x25 alphabets) instead of 26 different possible alphabets.

The Playfair cipher was used mainly to protect important, yet non-critical secrets, as it is quick to use and requires no special equipment.

Vigenere Cipher or Polygram Cipher

This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext.

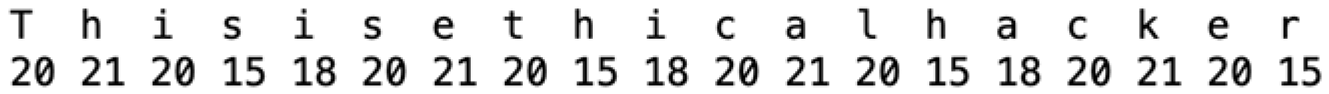
For example, let's assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value: In this case,

p → 16, o → 15, i → 9, n → 14, and t → 20.

Thus, the key is: 16 15 9 14 20.

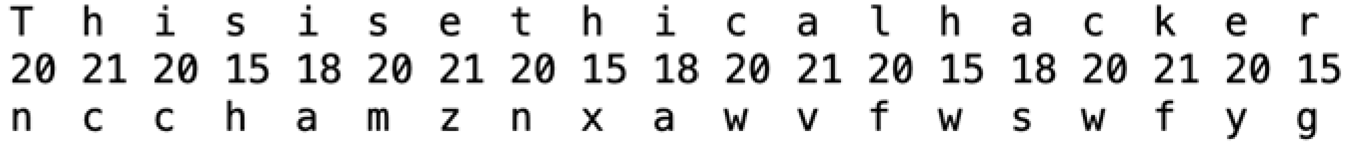
Process of Vigenere Cipher

- The sender and the receiver decide on a key. Say 'point' is the key. Numeric representation of this key is '16 15 9 14 20'.
- The sender wants to encrypt the message, say 'attack from south east'. He will arrange plaintext and numeric key as follows −



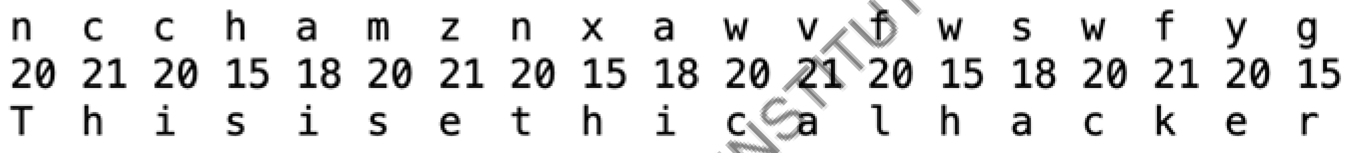
T	h	i	s	i	s	e	t	h	i	c	a	l	h	a	c	k	e	r
20	21	20	15	18	20	21	20	15	18	20	21	20	15	18	20	21	20	15

- He now shifts each plaintext alphabet by the number written below it to create ciphertext as shown below −



T	h	i	s	i	s	e	t	h	i	c	a	l	h	a	c	k	e	r
20	21	20	15	18	20	21	20	15	18	20	21	20	15	18	20	21	20	15
n	c	c	h	a	m	z	n	x	a	w	v	f	w	s	w	f	y	g

- Here, each plaintext character has been shifted by a different amount – and that amount is determined by the key. The key must be less than or equal to the size of the message.
- For decryption, the receiver uses the same key and shifts received ciphertext in reverse order to obtain the plaintext.



n	c	c	h	a	m	z	n	x	a	w	v	f	w	s	w	f	y	g
20	21	20	15	18	20	21	20	15	18	20	21	20	15	18	20	21	20	15
T	h	i	s	i	s	e	t	h	i	c	a	l	h	a	c	k	e	r

Security Value

Vigenere Cipher was designed by tweaking the standard Caesar cipher to reduce the effectiveness of cryptanalysis on the ciphertext and make a cryptosystem more robust. It is significantly **more secure than a regular Caesar Cipher**.

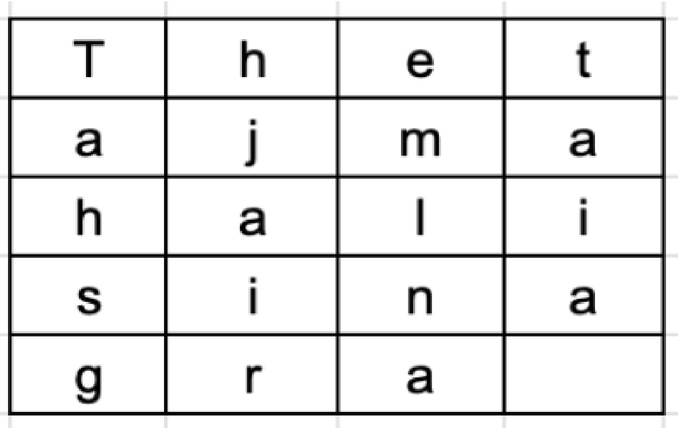
In the history, it was regularly used for protecting sensitive political and military information. It was referred to as the **unbreakable cipher** due to the difficulty it posed to the cryptanalysis.

Transposition Cipher

It is another type of cipher where the order of the alphabets in the plaintext is rearranged to create the ciphertext. The actual plaintext alphabets are not replaced.

An example is a ‘simple columnar transposition’ cipher where the plaintext is written horizontally with a certain alphabet width. Then the ciphertext is read vertically as shown.

For example, the plaintext is “golden statue is in eleventh cave” and the secret random key chosen is “five”. We arrange this text horizontally in table with number of column equal to key value. The resulting text is shown below.



T	h	e	t
a	j	m	a
h	a	l	i
s	i	n	a
g	r	a	

The ciphertext is obtained by reading column vertically downward from first to last column. The ciphertext is 'gnuneaoseenvltiltedasehetivc'.

To decrypt, the receiver prepares similar table. The number of columns is equal to key number. The number of rows is obtained by dividing number of total ciphertext alphabets by key value and rounding of the quotient to next integer value.

The receiver then writes the received ciphertext vertically down and from left to right column. To obtain the text, he reads horizontally left to right and from top to bottom row.

Playfair Cipher

The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.
It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.
The Playfair Cipher Encryption Algorithm:
The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5):**

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
   For example:

PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.
Plain Text: “hello”
After Split: ‘he’ ‘lx’ ‘lo’
Here **‘x’** is the bogus letter.
2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter
Plain Text: “helloe”
AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’
Here **‘z’** is the bogus letter.

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
  For example:

Diagraph: "me"
Encrypted Text: cl
Encryption:
m -> c
e -> l

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
  For example:

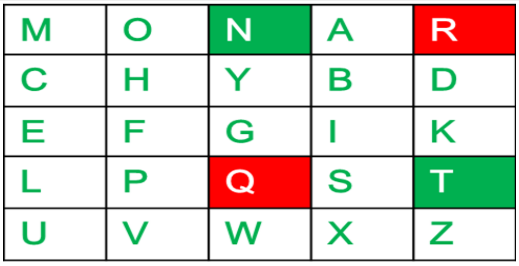
Diagraph: "st"
Encrypted Text: tl
Encryption:
s -> t
t -> l

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

Diagraph: "nt"
Encrypted Text: rq
Encryption:
 n -> r
 t -> q



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:
 i -> g
 n -> a
 s -> t
 t -> l
 r -> m
 u -> z
 m -> c
 e -> l
 n -> r
 t -> q
 s -> t
 z -> x

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:

```
Input  : Plaintext: ACT

         Key: GYBNQKURP

Output : Ciphertext: POH
```

Input : Plaintext: GFG

Key: HILLMAGIC

Output : Ciphertext: SWK

Encryption

We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of ‘POH’

Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext ‘POH’:

which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Encryption

Encryption is the process of transforming plaintext data into ciphertext with the help of an algorithm and an encryption key. Ciphertext is basically unreadable without the decryption key, adding another degree of security to sensitive data. Encryption methods differ in complexity, with some being more secure than others.

Decryption

Decryption is the process of transforming ciphertext back into plaintext using the decryption key. Only persons or entities that have the right decryption key may access the original data. Decryption should be done securely to avoid unauthorised access to sensitive information.

Types of Encryption

Encryption is a crucial aspect of securing information, and there are two main types: symmetric encryption and asymmetric encryption.

Symmetric Encryption: Symmetric encryption is a method where the same key is employed for both the encryption and decryption processes. In this approach, the key used to secure the data must be shared between the entities involved in communication. This simplicity is advantageous for efficiency, making symmetric encryption particularly suitable for scenarios involving the encryption and decryption of large volumes of data. Notable symmetric encryption algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). However, a potential drawback is the necessity for a secure method of key exchange between communicating parties.

Asymmetric Encryption: Asymmetric encryption, on the other hand, utilizes a pair of keys — a public key for encryption and a private key for decryption. The public key can be openly distributed, allowing anyone to encrypt messages, while the private key must be kept confidential for decrypting the received messages. Asymmetric encryption is computationally more intensive compared to symmetric encryption but offers a higher level of security. This method is commonly used for secure key exchange, ensuring a confidential communication channel, and for implementing digital signatures. Well-known asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC).

Types of Decryption

Decryption is the process of converting encrypted data back into its original, readable form. There are two main types of decryption methods: symmetric decryption and asymmetric decryption.

Symmetric Decryption: Symmetric decryption is a cryptographic process where the same key that was used for encrypting the data is utilized to reverse the encryption and retrieve the original information. This method operates on the principle of a shared secret key between the parties involved in the communication. The efficiency of symmetric decryption lies in its simplicity and speed, as the algorithm's computational overhead is relatively low. However, the challenge with symmetric decryption lies in securely exchanging and managing the shared secret key. Any compromise of this key could potentially lead to unauthorized access to the decrypted information. Symmetric decryption is commonly employed in scenarios where the need for rapid and efficient data processing is crucial, such as in large-scale data encryption and decryption tasks.

Asymmetric Decryption: In contrast, asymmetric decryption involves a pair of keys — a private key for decryption and a corresponding public key for encryption. The public key is freely distributed, allowing anyone to encrypt messages, while only the possessor of the private key can decrypt and access the original information. While asymmetric decryption offers enhanced security and eliminates the need for a shared secret key, it comes at the cost of increased computational complexity. The process demands more computational resources compared to symmetric decryption. Asymmetric decryption is often utilized in situations where the primary concern is securing communication channels and ensuring the authenticity of messages, making it suitable for tasks like secure key exchange and digital signatures.

Components

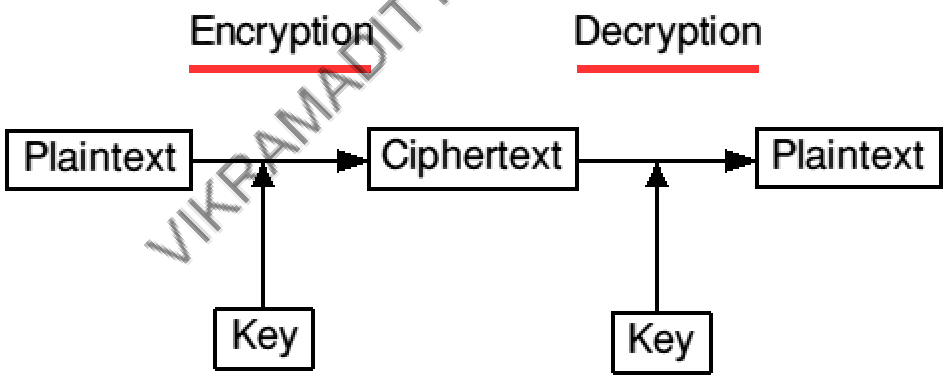


Fig. 2. Components of Encryption and Decryption

1. **Plaintext:** Plaintext refers to the original, unencrypted message that a sender wishes to keep secure in a cryptosystem. It represents the information that needs safeguarding from unauthorised access or

interception. Through a process called encryption, the plaintext is transformed into ciphertext, rendering it scrambled and unintelligible to anyone without the proper decryption key. The primary goal of encryption is to ensure that even if an attacker intercepts the communication, they won't be able to understand the content without the proper decryption key. This helps to maintain the confidentiality and integrity of the information being communicated.

2. **Ciphertext:** In a cryptosystem, the ciphertext is the result of applying a specific encryption algorithm to a plaintext message, which obscures the original content and renders it unintelligible to anyone who doesn't possess the necessary information to reverse the process (i.e., decryption). The ciphertext is what is transmitted over an insecure channel to protect the confidentiality of the information being sent.

3. **Encryption algorithm:** An encryption algorithm is a set of mathematical rules and operations used to convert readable data (plaintext) into unreadable code (ciphertext) using a specific key. Its main purpose is to secure information during storage or transmission, making it accessible only to authorised users.

4. **Decryption algorithm:** A decryption algorithm is a mathematical procedure or set of rules used to convert encrypted data back into its original, readable form. It is an essential component of a cryptosystem, which is a system designed to secure communication or information by converting it into a form that is unintelligible to anyone except those with the appropriate decryption key.

5. **Encryption Key:** An encryption key is a vital component of a cryptosystem, facilitating the secure handling of information. It consists

of a distinct, randomly generated series of bits employed in the process of encoding and decoding data. The level of security is contingent on the key's length, with longer keys affording greater protection. Symmetric systems employ a single key for both encryption and decryption, whereas asymmetric systems utilise separate public and private keys. It is imperative to handle and protect encryption keys diligently to uphold the confidentiality and integrity of sensitive data.

6. **Decryption Key:** A decryption key is an essential element of a cryptosystem, enabling the reversal of encryption. It encompasses a mathematical algorithm and a confidential value or set of values. This algorithm directs the conversion of encrypted data back into its original, understandable state. The key acts as the input for this process, ensuring that only authorised individuals possessing the correct key can decode the information. Without the appropriate decryption key, it is computationally impractical to restore encrypted data to its original form.

Shared Key and Public Key

In network security, both shared keys (symmetric key cryptography) and public keys (asymmetric key cryptography) are used for different purposes.

1. Shared Key (Symmetric Key Cryptography):

Single Key for Encryption and Decryption: Symmetric key cryptography involves the use of a single shared key for both encryption and decryption. This means that the same key is used by both the sender and the receiver.

Faster Processing: Symmetric key algorithms are generally faster and require less computational power than their asymmetric counterparts.

Advantages of encryption:

1. **Confidentiality:** Encryption ensures that unauthorized individuals or entities cannot access sensitive information. Even if an attacker intercepts the data, they would be unable to understand or use it without the appropriate decryption key.

2. **Data Integrity:** Encryption helps maintain the integrity of data during transmission. It ensures that the data has not been altered or tampered with while in transit, as any modification would result in decryption failure.

3. **Authentication:** Encryption is often used in combination with authentication mechanisms to verify the identity of the communicating parties. This ensures that data is exchanged only between trusted and authenticated entities.

4. **Securing Wireless Communication:** In wireless networks, data is susceptible to interception. Encryption, such as WPA (Wi-Fi Protected Access) for Wi-Fi networks, helps secure wireless communication by encrypting the data, making it challenging for unauthorized users to decipher.

Advantages of decryption:

1. **Data Access:** Decryption allows authorized users to access and retrieve sensitive information, ensuring that only those with the appropriate credentials can view the data.

2. **Data Integrity:** Decrypting data ensures that it hasn’t been tampered with during transmission or storage, maintaining the integrity of the information.

3. **Compliance:** In certain industries or regions, compliance regulations may require organizations to decrypt and monitor data to meet legal and regulatory standards.

4. **User Authentication:** Decryption is often part of the process of user authentication, confirming the identity of individuals seeking access to protected systems or information.

Disadvantages of encryption:

1. **Performance Impact:** Encryption and decryption processes can introduce computational overhead, which can slow down the performance of devices and systems, particularly on older or less powerful hardware.

2. **Data Recovery Challenges:** If an encryption key is lost or forgotten, it can be extremely difficult or even impossible to recover the encrypted data. Data recovery can be a significant challenge in such cases.

3. **Key Management Complexity:** Managing encryption keys is a critical aspect of encryption. If keys are lost, compromised, or mishandled, it can lead to data inaccessibility or security breaches. Key management can be complex and resource-intensive.

4. **Compatibility Issues:** Different encryption algorithms and standards may not be compatible with each other, leading to challenges when trying to exchange encrypted data between systems that use different encryption methods.

Disadvantages of Decryption:

1. **Security Risks:** Decryption is the process of revealing sensitive information, and if not done securely, it can expose data to unauthorised access or breaches. An attacker gaining access to decryption keys or the decrypted data can be a significant security risk.

2. **Data Integrity:** In some cases, decryption may not guarantee data integrity. Data may have been tampered with or altered during transmission, and the decryption process doesn't address these integrity concerns.

3. **Access Control Challenges:** Decryption can create challenges in implementing proper access control mechanisms. If decrypted data is accessed by unauthorised parties, it can lead to data leaks.

4. **Legal and Compliance Issues:** In certain cases, decryption may be subject to legal and compliance requirements. Organisations may need to ensure that they are in compliance with such regulations, which can be complex and costly.

Limitations for encryption and decryption

1. Key Management: One of the primary challenges is key management. Securely generating, distributing, storing, and revoking encryption keys can be complex, especially in large-scale systems. Poor key management can compromise the effectiveness of encryption.

2. Performance Overhead: The process of encrypting and decrypting data requires computational resources. In some cases, especially with strong encryption algorithms, this can introduce a performance overhead that may impact system responsiveness, particularly in resource-constrained environments.

3.Key Length vs. Processing Time Tradeoff: Increasing the key length generally enhances security but may also increase the time and resources required for encryption and decryption. Finding the right balance between key length and processing time is crucial for optimizing performance.

4. Algorithm Vulnerabilities: Encryption algorithms, especially older or poorly designed ones, may have vulnerabilities that could be exploited by attackers. As computing power increases, some algorithms may become more susceptible to brute-force attacks.

5.Initial Secure Key Exchange: The secure exchange of encryption keys during the initial communication is critical. If this process is compromised, the entire security of the encrypted communication may be at risk. Methods like public-key cryptography help address this concern but require careful implementation.

6. User Authentication: While encryption protects data in transit or at rest, it does not inherently address user authentication. An attacker with valid credentials can still access encrypted data, emphasizing the importance of combining encryption with robust authentication mechanisms.

Challenges: The main challenge with symmetric key cryptography is securely distributing and managing the shared key. If an unauthorized party gains access to the key, they can decrypt the communication.

2. Public Key (Asymmetric Key Cryptography):

Key Pair: Asymmetric key cryptography uses a pair of keys — a public key and a private key. The public key is shared openly, while the private key is kept secret.

Encryption and Decryption: Data encrypted with the public key can only be decrypted by the corresponding private key, and vice versa. This provides a higher level of security compared to symmetric key cryptography.

Digital Signatures: Public key cryptography is often used for creating digital signatures. The sender uses their private key to sign a message, and the recipient can verify the signature using the sender’s public key. This ensures the authenticity of the message.

Key Exchange: Public key cryptography helps in secure key exchange. Two parties can use each other’s public keys to establish a shared secret key for symmetric key cryptography.

Use Cases:

Symmetric Key: Often used for encrypting large amounts of data due to its efficiency. For example, in VPNs (Virtual Private Networks) or disk encryption.

Asymmetric Key: Commonly used for secure communication, digital signatures, and key exchange in protocols like SSL/TLS for secure web browsing, SSH for secure shell communication, and PGP for secure email.

In many systems, a combination of both symmetric and asymmetric key cryptography is used to leverage the strengths of each approach. For example, a secure communication session might begin with asymmetric key exchange for secure key establishment, followed by symmetric key cryptography for the bulk of the data transfer due to its efficiency.

Uses:

Encryption and decryption play crucial roles in ensuring the security of data and communications in various aspects of network security. Here are specific use cases for encryption and decryption:

Data Confidentiality and Integrity: Encryption and decryption are pivotal in maintaining the confidentiality and integrity of sensitive data during transmission and storage. Protocols such as SSL/TLS encrypt data during online transactions and secure web browsing, ensuring that unauthorized entities cannot eavesdrop on or tamper with the exchanged information, thereby safeguarding the privacy and reliability of data.

Secure Email Communication: In secure email communication, encryption and decryption technologies like PGP and S/MIME are employed to protect the content of emails. These protocols use asymmetric cryptography to secure the messages, ensuring that only the intended recipients with the corresponding decryption keys can access the email content. This prevents unauthorized interception and tampering, enhancing the overall confidentiality and privacy of electronic communication.

Symmetric Key Algorithms

Symmetric key algorithms are a type of cryptographic technique that uses a shared secret key for both encryption and decryption. This means that the same key is used to encode and decode the message. Symmetric key algorithms are generally faster and more efficient than asymmetric key algorithms, but they require that the sender and receiver of a message share a secret key.

Here are some of the basic principles of symmetric key algorithms −

- **The same key is used for both encryption and decryption** − In symmetric key algorithms, the same key is used to both encrypt and decrypt the message. This means that the sender and receiver of a message must share the same secret key in order to communicate securely.
- **Symmetric key algorithms are faster and more efficient than asymmetric key algorithms** − Symmetric key algorithms are generally faster and more efficient than asymmetric key algorithms, as they do not require the use of complex mathematical operations such as exponentiation. This makes them well-suited for applications that require fast encryption and decryption, such as securing communication over the internet.
- **Symmetric key algorithms are less secure than asymmetric key algorithms** − While symmetric key algorithms are generally faster and more efficient than asymmetric key algorithms, they are also less secure. This is because the same key is used for both encryption and decryption, which means that if the key is compromised, the security of the entire system is compromised.

Overall, symmetric key algorithms are an important type of cryptographic technique that are used to secure communication and protect data. While they are generally faster and more efficient than asymmetric key algorithms, they are also less secure and require that the sender and receiver of a message share a secret key.

Cryptographic Strength of Symmetric Algorithms

The cryptographic strength of a symmetric key algorithm refers to its ability to resist attacks and protect the confidentiality of the information it is used to encrypt. The cryptographic strength of a symmetric key algorithm is determined by a variety of factors, including −

- **Key size** − The size of the key used in a symmetric key algorithm is a major determinant of its cryptographic strength. In general, the larger the key size, the stronger the algorithm.

- **Block size** − The block size of a symmetric key algorithm refers to the size of the blocks of data that are encrypted and decrypted using the algorithm. A larger block size can increase the cryptographic strength of the algorithm.
- **Number of rounds** − The number of rounds in a symmetric key algorithm refers to the number of times that the encryption and decryption process is repeated. A larger number of rounds can increase the cryptographic strength of the algorithm.
- **Resistance to attacks** − The resistance of a symmetric key algorithm to attacks, such as brute-force attacks or differential cryptanalysis, is another factor that determines its cryptographic strength. Algorithms that are resistant to these types of attacks are generally considered to be stronger.

Overall, the cryptographic strength of a symmetric key algorithm is determined by a combination of these and other factors. Stronger algorithms are generally more resistant to attacks and more effective at protecting the confidentiality of the information they are used to encrypt.

Types of Symmetric Key Algorithms

There are several different types of symmetric key algorithms, including −

- **Block ciphers** − Block ciphers are symmetric key algorithms that operate on fixed-size blocks of data and use a secret key to encrypt and decrypt the data. Examples of block ciphers include the Advanced Encryption Standard (AES) and Blowfish.
- **Stream ciphers** − Stream ciphers are symmetric key algorithms that operate on a stream of data and use a secret key to encrypt and decrypt the data. Stream ciphers are generally faster and more efficient than block ciphers, but they are also generally considered to be less secure.
- **Feistel ciphers** − Feistel ciphers are a type of block cipher that are based on a structure known as a Feistel network. They are widely used in symmetric key algorithms and are known for their efficiency and ease of implementation.
- **Substitution-permutation ciphers** − Substitution-permutation ciphers are a type of block cipher that use both substitution and permutation operations to encrypt and decrypt data. They are known for their strong cryptographic properties and are used in many modern symmetric key algorithms.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a highly trusted **encryption algorithm** used to secure data by converting it into an unreadable format without the proper key. It is developed by the National Institute of Standards and Technology (NIST) in 2001. It is is widely used today as it is much stronger than DES and triple DES despite being harder to implement. **AES encryption** uses various **key lengths** (128, 192, or 256 bits) to provide strong protection against unauthorized access. This **data security** measure is efficient and widely implemented in securing **internet communication**, protecting **sensitive data**, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

- AES is a Block Cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

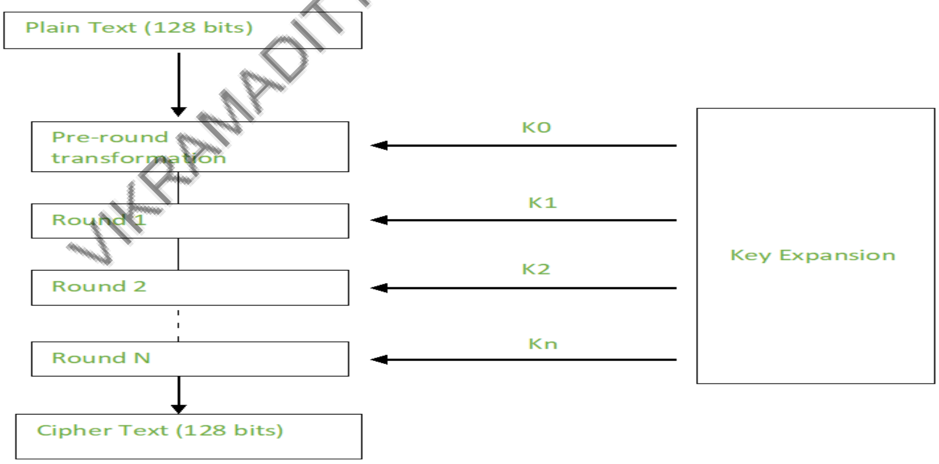
That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text. AES relies on the substitution-permutation network principle, which is performed using a series of linked operations that involve replacing and shuffling the input data.

Working of The Cipher

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length as follows :

N (Number of Rounds)	Key Size (in bits)
10	128
12	192
14	256

Creation of Round Keys

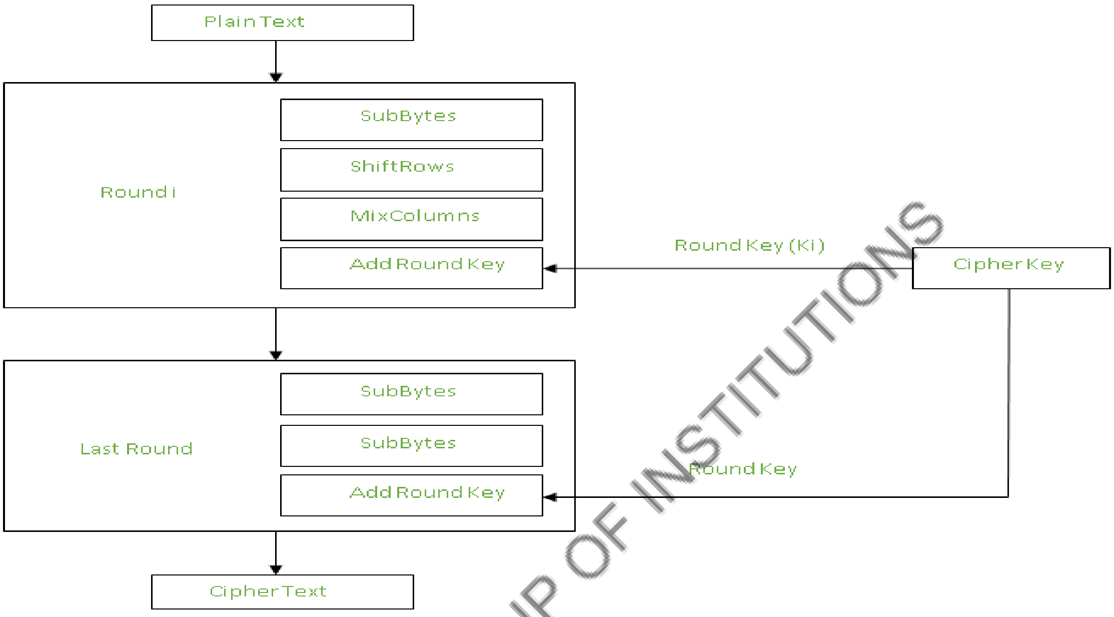


A Key Schedule algorithm calculates all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

Encryption

AES considers each block as a 16-byte (4 byte x 4 byte = 128) grid in a column-major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]



Added Round Keys (AES)

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

Step1. Sub Bytes

This step implements the substitution.

In this step, each byte is substituted by another byte. It is performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16-byte (4 x 4) matrix like before.

The next two steps implement the permutation.

Step2. Shift Rows

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

Step 3: Mix Columns

This step is a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

[c0] [2 3 1 1] [b0]
| c1 | = | 1 2 3 1 | | b1 |
| c2 | | 1 1 2 3 | | b2 |
[c3] [3 1 1 2] [b3]

Step 4: Add Round Keys

- Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes are not considered as a grid but just as 128 bits of data.
- After all these rounds 128 bits of encrypted data are given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round of decryption are as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so I will explain the steps with notable differences.

Inverse MixColumns

- This step is similar to the Mix Columns step in encryption but differs in the matrix used to carry out the operation.
- Mix Columns Operation each column is mixed independent of the other.
- Matrix multiplication is used. The output of this step is the matrix multiplication of the old values and a

constant matrix

[b0] = [14 11 13 9] [c0]
[b1]=[9 14 11 13] [c1]
[b2] =[13 9 14 11] [c2]
[b3]=[11 13 9 14] [c3]

Inverse SubBytes

- Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

- Function Substitute performs a byte substitution on each byte of the input word. For this purpose, it uses an S-box.

Applications of AES

AES is widely used in many applications which require secure data storage and transmission. Some common use cases include:

- **Wireless security:** AES is used in securing wireless networks, such as Wi-Fi networks, to ensure data confidentiality and prevent unauthorized access.
- **Database Encryption:** AES can be applied to encrypt sensitive data stored in databases. This helps protect personal information, financial records, and other confidential data from unauthorized access in case of a data breach.
- **Secure communications:** AES is widely used in protocols such as internet communications, email, instant messaging, and voice/video calls. It ensures that the data remains confidential.
- **Data storage:** AES is used to encrypt sensitive data stored on hard drives, USB drives, and other storage media, protecting it from unauthorized access in case of loss or theft.
- **Virtual Private Networks (VPNs):** AES is commonly used in VPN protocols to secure the communication between a user’s device and a remote server. It ensures that data sent and received through the VPN remains private and cannot be deciphered by eavesdroppers.
- **Secure Storage of Passwords:** AES encryption is commonly employed to store passwords securely. Instead of storing plaintext passwords, the encrypted version is stored. This adds an extra layer of security and protects user credentials in case of unauthorized access to the storage.
- **File and Disk Encryption:** AES is used to encrypt files and folders on computers, external storage devices, and cloud storage. It protects sensitive data stored on devices or during data transfer to prevent unauthorized access.

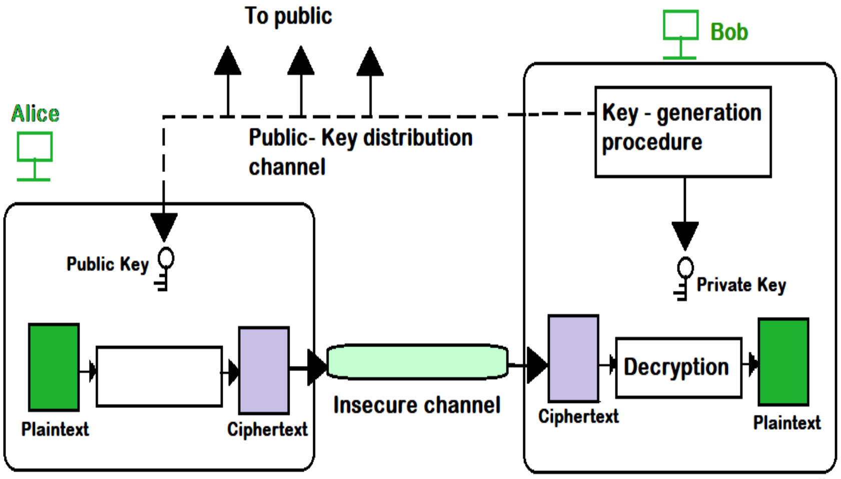
Asymmetric Key Cryptography

In asymmetric Key cryptography, there are two keys, also known as key pairs: a public key and a private key. The public key is publicly distributed. Anyone can use this public key to encrypt messages, but only the recipient, who holds the corresponding private key, can decrypt those messages. "Public-key cryptography" is another representation used to refer to Asymmetric Key cryptography.

This cryptographic system addresses two major challenges faced in traditional (symmetric) cryptography: **key distribution and digital signatures.** Asymmetric algorithms use one key for encrypting data and another, related key for decrypting it. These algorithms possess an important feature:

- It's impossible to figure out the decryption key just by knowing the encryption key and the cryptographic algorithm.
- Either of the two keys can be used for encryption, while the other is used for decryption.

Asymmetric-key cryptography uses mathematical functions to transform plaintext and ciphertext represented as numbers for encryption and decryption, while



symmetric-key cryptography involves symbol substitution or permutation. In asymmetric-key cryptography, plaintext and ciphertext are treated as integers, requiring encoding and decoding processes for encryption and decryption.

General idea of asymmetric-key cryptosyste

Characteristics of Asymmetric Key Cryptography

Security Responsibility

- In asymmetric cryptography, the burden of security primarily falls on the receiver, like Bob.
- Bob must generate both a private and a public key, with the public key distributed to the community.
- Distribution occurs through a public-key channel, which doesn't need secrecy but requires authentication and integrity to prevent impersonation.

Unique Key Pairs

- Bob and Alice can't share the same key pair for two-way communication.
- Each entity in the community, including Bob and Alice, must create its own private and public keys.
- Alice uses Bob's public key to encrypt messages to him, while she needs her own key pair for responses.

Key Management

- Bob needs only one private key to receive messages from anyone in the community.
- Alice, on the other hand, needs multiple public keys—one for each entity she communicates with.
- This means Alice requires a collection of public keys for effective communication.

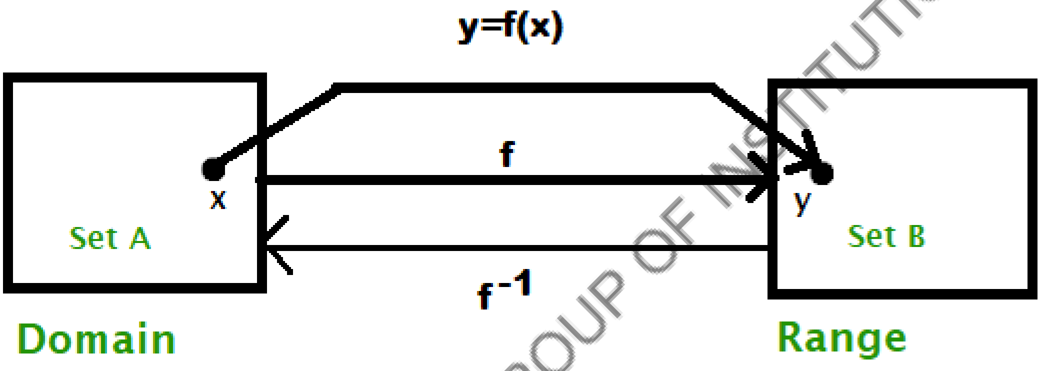
Key Components

- **Plaintext**: This refers to the original, readable message or data that is inputted into the encryption algorithm.
- **Encryption algorithm**: This algorithm transforms the plaintext in various ways.

- **Public and private keys**: A pair of keys chosen so that if one is used for encryption, the other is used for decryption. The specific transformations performed depend on whether the public or private key is provided as input.
- **Ciphertext**: The encrypted, scrambled message produced as output. It can be find using both the plaintext and the key, but uf there are different keys then it will give different ciphertexts for the same message or plaintext.
- **Decryption algorithm**: This algorithm takes the ciphertext and the corresponding key and retrieves the original plaintext.

Concept of the Trapdoor One-Way Function

Asymmetric-key cryptography lies in the concept of the trapdoor one-way function.Imagine a function as a simple rule we follow in math. It takes something from one group (let's call it "Set A") and matches it with something in another group (we'll call this one "Set B"). It's like connecting dots from one set to another, as can be seen below.



A function as rule mapping a domain to a range

Now, let's talk about something called a one-way function (OWF). It's a special kind of function that has two important qualities:

- f is easy to compute. We can also say that x, y = f (x) can be easily calculated.
- f–1 is difficult to compute. We can also say that, given y, it is computationally not feasible to evaluate x = f–1(y)

Now, let's add a secret ingredient to our one-way function, making it a trapdoor one-way function (TOWF). This type of function has a third feature:

- If it is given y and a trapdoor (secret), then x can be easily calculated.

If you have "y" and a special secret (let's call it a "trapdoor"), then you can easily figure out what "x" was. So, even though it's normally hard to go from "y" back to "x," if you have this secret code, it becomes a lot easier.

We can write it as follows: A trapdoor one-way function is a relative of invertible functions fp, such that:

- **Y = fp(X) easy, if p and X are known**
- **X = fp-1(Y) easy, if p and Y are known**
- **X = fp-1(Y) infeasible, if Y is known but p is not known**

Primary Terminologies

- **Asymmetric Keys:** Two keys, one public and one private, that are used together for different tasks like locking and unlocking information or verifying signatures.
- **Public Key Certificate:** A digital document signed by a trusted authority's private key that confirms a person's identity and links it to their public key. This document shows that the person controls the private key associated with the public key.
- **Public Key (Asymmetric) Cryptographic Algorithm:** A way to encode information that uses two keys, one public and one private. It's designed so that figuring out the private key from the public one is extremely hard.
- **Public Key Infrastructure (PKI):** It is the collection of policies, procedures, server platforms, software and workstations that is used for the objective of administering certificates and public-private key pairs, it also has the ability to publish, maintain, and revoke public key certificates.

Working

- **Key Generation**: Each user generates a pair of keys for encrypting and decrypting messages. One of the keys is made public, stored in a register or accessible file, while the other key remains private. Users collect public keys from others.
- **Encryption:** The sender encrypts the message using the public key of reciever. This transforms the message into an unreadable format (ciphertext). When Alice wants to send a confidential message to Bob, Alice encrypts it using Bob's public key.
- **Decryption:** The recipient uses their private key to decrypt the ciphertext back to the original message (plaintext). Upon receiving the message, Bob decrypts it using his private key. Only Bob can decrypt the message because only he has his private key.

In this setup, all participants possess public keys, while private keys are locally generated and never distributed. As long as a user's private key remains secure and undisclosed, incoming communications are safe. The system can change its private key at any time and publish the corresponding public key to replace the old one.

Algorithms

There are several algorithms used in asymmetric key cryptography, some of them are as follows:

- RSA (Rivest–Shamir–Adleman)
- Elliptic Curve Cryptography (ECC)
- Diffie-Hellman
- DSS (Digital Signature Standard)

RSA (Rivest–Shamir–Adleman)

It is commonly utilized to ensure secure communication and for creating digital signatures. It Uses large integer prime numbers for key generation. It Encrypts data with the public key and decrypts with the private key. It is Slower than some other algorithms but offers strong security.

Key Generation

- Choose/Select two large prime numbers, p and q.
- Calculate $n=p*qn=p*q$.
- Calculate φ(n) = (p-1)(q-1), where φ is Euler's totient function.
- Choose an integer e, that $1<e<\varphi(n)1<e<\varphi(n)$ and $gcd(e,\varphi(n))=1gcd(e,\varphi(n))=1$.
- Compute d, the modular multiplicative inverse of e modulo φ(n).
- Public key: $(e,n)(e,n)$
- Private key: $(d,n)(d,n)$

Encryption

- Convert plaintext message into an integer m.
- Compute ciphertext $c=memodnc=m^{e}modn$.

Decryption

- Calculate the plaintext message $m=cdmodnm=c^{d}modn$.

Elliptic Curve Cryptography (ECC)

It gives equal protection to RSA with shorter key sizes. The concept behind this is based on the mathematical properties of elliptic curves. It is Faster and more efficient for resource-constrained devices. It Gaining popularity in mobile security and the Internet of Things (IoT).

Key Generation

- Select an elliptic curve over a finite field.
- Choose a base point on the curve and a large prime order.
- Select a private key, which is a random integer k.
- Now, Using the elliptic curve scalar multiplication, you need to find the public key by multiplying the base point by the private key.

Encryption and Decryption

- ECC is primarily used for key exchange, such as in the Elliptic Curve Diffie-Hellman (ECDH) algorithm, rather than directly for encryption/decryption.

Diffie-Hellman Key Exchange

It doesn't directly encrypt data but establishes a shared secret key for secure communication. Two parties can generate a common secret key without ever exchanging it directly. It often used in conjunction with other algorithms like RSA for key exchange.

Key Exchange

- Sender and receiver agree on a large prime number p and a primitive root g modulo p.
- Each party selects a secret key: a and b.
- Party A computes public key $A=gamodpA=g^{a}modp$ and sends it to Party B.
- Party B computes public key $B=gbmodpB=g^{b}modp$ and sends it to Party A.
- Both parties compute the shared secret: $s=Abmodp=Bamodps=A^{b}modp=B^{a}modp$.

Security

- Diffie-Hellman does not provide proper authentication; it sets a shared secret between two parties.

Digital Signature Standard (DSS)

It Uses a variant of the ElGamal encryption scheme. It is primarily for digital signatures, ensuring message authenticity and integrity. The sender signs a message with their private key, receiver verifies with the sender's public key. It is often used for secure emails and software signing.

Key Generation

- DSS uses the Digital Signature Algorithm (DSA), which relies on discrete logarithm problems in a finite field.
- Generate a prime number p and a prime divisor q of p-1.
- Choose a generator g such that $\mathrm{gqmodp=1}g^{q}modp=1$.
- Generate private key x, a random integer between 1 and q-1.
- Calculate the public key $\mathrm{y=gxmodp}y=g^{x}modp$.

Signing

- Calculate a hash of the message.
- Generate any random number k such that it lies between 1 and q-1.
- Calculate $\mathrm{r=(gkmodp)modq}r=(g^{k}modp)modq$.
- Calculate s = k^{-1} * (hash + x * r) mod q.
- The signature is the pair (r, s).

Verification

- Recalculate the hash of the message.
- Compute w = s^{-1} mod q.
- Compute $\mathrm{u1=(hash*w)modq}u1=(hash*w)modq$ and $\mathrm{u2=(r*w)modq}u2=(r*w)modq$.
- Now, we need to calculate v as v = ((g^{u1} * y^{u2}) mod p) mod q.
- If v is equal to r, it means that the signature is verified.

Applications

- **Encryption / Decryption:** Messages are encrypted using the recipient's public key, ensuring only the intended recipient can decrypt it.
- **Digital Signature:** Senders authenticate messages by signing them with their private key, verifying their identity and ensuring message integrity.
- **Key Exchange:** Parties cooperate to establish a shared session key securely, facilitating encrypted communication. This can involve the private key(s) of one or both parties.

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
DSS	No	Yes	No

Advantages

- **Enhanced Security:** The private key remains secret, making it difficult for someone to decrypt intercepted messages.
- **Secure Key Distribution:** Public keys can be shared openly without compromising security, unlike symmetric keys that require secure distribution.

Public-Key Cryptanalysis

Cryptanalysis is the study of studying cryptographic systems to understand their vulnerabilities or weaknesses, often with the goal of breaking or bypassing their security measures.

When it comes to public-key encryption schemes, cryptanalysis has some challenges and risks:

- **Brute-Force Attack:** Imagine trying every single key combination to unlock a padlock. This is a brute-force attack. Public-key encryption is vulnerable to brute-force attacks just like symmetric encryption. The solution is similar: using large keys. The larger the key, the more difficult it is to guess correctly. Also, Public-key encryption relies on complex math functions. As the key size increases, these functions become more difficult and slower to use. We need a key size that's large enough to resist brute-force attacks but still allows for practical encryption and decryption speeds. Currently, public-key encryption is often used for specific tasks like key management and digital signatures because of this trade-off between security and speed.
- **Finding the Private Key from the Public Key:** Ideally, the private key should be impossible to guess from the public key. Mathematically, this hasn't been definitively proven for any public-key algorithm, including the popular RSA algorithm. This is a concern because new mathematical breakthroughs could potentially crack these systems in the future.
- **Probable-Message Attack (Unique to Public-Key Systems):** Suppose a message consists solely of a 56-bit DES key, an adversary could encrypt all possible 56-bit DES keys using the public key and deduce the encrypted key by matching ciphertext. Consequently, regardless of the public-key scheme's key size, the attack reduces to a brute-force assault on a 56-bit key. This attack can be countered by appending random bits to simple messages.

Types of attacks in network security

While there are countless types of attacks used every day, you could realistically break the majority of them down into the following 4 categories:

1. **1. Malware Attacks:** Malware stands for malicious software. This encompasses a wide range of harmful programs that can infiltrate a network through

vulnerabilities. Malware can steal data, corrupt files, disrupt operations, or even take control of systems. Examples include viruses, worms, Trojan horses, ransomware, and spyware.

2.
3. **2. Phishing Attacks:** Phishing attacks attempt to trick users into revealing sensitive information, such as usernames, passwords, or credit card details. Phishers often use emails or fraudulent websites that appear legitimate. Once a user enters their information, the attacker can steal it and misuse it.
4.
5. **3. Password Attacks:** These attacks target passwords to gain unauthorized access to a network or system. Hackers can employ various techniques to crack passwords, including brute-force attacks (trying every possible combination), dictionary attacks (using common words and phrases), and social engineering (tricking users into revealing their passwords).
6.
7. **4. Denial-of-Service (DoS) Attacks:** DoS attacks aim to overwhelm a network or system with traffic, making it unavailable to legitimate users. Attackers can flood the target with a massive amount of data requests, causing it to crash or become unresponsive. This can disrupt critical operations and cause significant financial losses.
8.

What are the four 4 types of security threats?

We can categorize most security threats into just 4 broad categories based on the goals of the attackers:

1. **Exploiting Weaknesses:** This category covers threats that take advantage of vulnerabilities in systems or human behavior. This includes:
2.

- **Malware Attacks:** Malicious software exploits weaknesses in software or security measures to gain access and cause harm.
- **Unauthorized Access:** Hackers exploit vulnerabilities in software, steal passwords, or use physical means to gain unauthorized entry.
- **Social Engineering:** Attackers exploit human trust and manipulate people into giving up sensitive information or clicking on malicious links.

3. **Disrupting Availability:** This category focuses on threats that aim to prevent authorized users from accessing systems or resources. This includes:
4.

- **Denial-of-Service (DoS) Attacks:** These attacks overwhelm a system or network with traffic, making it unavailable to legitimate users.

- **Physical Attacks:** Damaging physical infrastructure or disrupting power supplies can also prevent access.

5. **Stealing Data:** This category covers threats that aim to obtain confidential or sensitive information. This includes:
6.

- **Malware Attacks:** Many malware types, like spyware and ransomware, target data theft.
- **Social Engineering:** Social engineering scams often aim to trick people into revealing personal information or login credentials.
- **Physical Attacks:** Stealing devices or accessing physical storage can be used to steal data.

7. **Disrupting Integrity:** This category focuses on threats that aim to alter, modify, or destroy data. This includes:
8.

- **Malware Attacks:** Viruses, worms, and some ransomware can corrupt or destroy data.
- **Unauthorized Access:** Once attackers gain access, they can tamper with data for malicious purposes.

By grouping threats under these categories, we can get a broader understanding of their goals and how they achieve them. It's important to note that some threats can fall into multiple categories. For example, a ransomware attack might disrupt availability by encrypting data, while also aiming to steal money through extortion (disrupting integrity).

Firewall

A **firewall** acts as a barrier between you**r internal network** and **external threats.** It monitors and controls **incoming and outgoing network traffic** based on predefined security rules. Firewalls protect your devices from unauthorized access and block harmful data packets.

Types of Firewall

- **Packet-Filtering Firewall**: Filters data packets based on rules like IP address, port, and protocol.
- **Stateful Inspection Firewall**: Tracks active connections and matches incoming packets with existing ones.
- **Proxy Firewall**: Acts as a middleman, inspecting and filtering requests for added security.
- **Next-Generation Firewall (NGFW)**: Offers advanced features like intrusion prevention and application control.

- **Cloud Firewall**: Protects cloud-based environments; ideal for distributed networks.
- **Web Application Firewall (WAF)**: Shields web apps from attacks like SQL injections and cross-site scripting.

How Does Firewall Works

- **Traffic Monitoring**: The firewall constantly watches all data (called "**packets**") trying to enter or leave your network.
- **Rules-Based Filtering**: It uses a set of rules to decide whether to **allow** or **block traffic**. **For Example:**
- **Allow:** Safe traffic like visiting a website or receiving an email.
- **Block:** Suspicious traffic like hacking attempts or malware.
- **Acts as a Gatekeeper**: Only traffic that meets the rules is allowed through; everything else is stopped.

Key Features of Firewalls

- Monitors network traffic.
- Blocks unauthorized access.
- Filters harmful content and data packets.
- Prevents malware and hacking attempts.

VPNs

A **VPN** (Virtual Private Network) creates a secure and encrypted connection between your device and a VPN server. It masks your IP address and encrypts all data, ensuring privacy and security when browsing the internet.

Types of VPN

- **Remote Access VPN**: Securely connects individuals to private networks, ideal for remote work.
- **Site-to-Site VPN**: Links entire networks securely, often used by businesses with multiple locations.
- **Client-Based VPN**: Requires a software app to connect securely to a VPN server.
- **Network-Based VPN**: Configured at the router level to secure all devices on a network.
- **PPTP VPN**: Basic encryption, suitable for simple, low-security tasks.
- **L2TP/IPsec VPN**: Combines tunneling with strong encryption for secure remote connections.
- **OpenVPN**: Secure and customizable, widely used with **SSL/TLS encryption**.
- **WireGuard VPN**: Lightweight, fast, and highly secure with modern encryption.

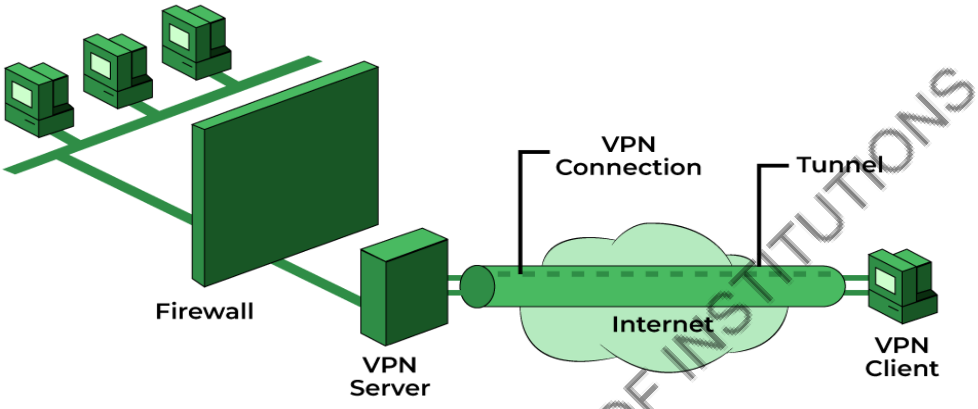
How Does VPN Works

- **You Connect to the VPN**: When you turn on a VPN app, it connects your **device to a VPN server** (usually in a different location).
- **Encryption**: Your internet traffic (like **websites you visit or files you download**) is **encrypted** (scrambled) so no one can read it.
- **Secure Tunnel**: Your encrypted data travels through a secure "**tunnel**" to the VPN server.

- **Server Sends Data**: The VPN server decrypts your data and sends it to the website or service you're accessing.
- **Website Sees the VPN Server**: The website only sees the VPN server's IP address and location, not yours.

Key Features of VPNs

- Encrypts data for secure communication.
- Masks IP addresses to enhance anonymity.
- Provides access to **geo-restricted content**.
- Protects users on public Wi-Fi networks.



Firewall vs. VPN

Secure Socket Layer (SSL)

SSL or Secure Sockets Layer, is an Internet security protocol that encrypts data to keep it safe. It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications. SSL is the older version of what we now call TLS (Transport Layer Security).

Websites using SSL/TLS have "HTTPS" in their URL instead of "HTTP."

Working of SSL

- **Encryption**: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.
- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.
- **Data Integrity**: SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.

Importance of SSL

Originally, data on the web was transmitted in plaintext, making it easy for anyone who intercepted the message to read it. For example, if someone logged into their email account, their username and password would travel across the Internet unprotected.

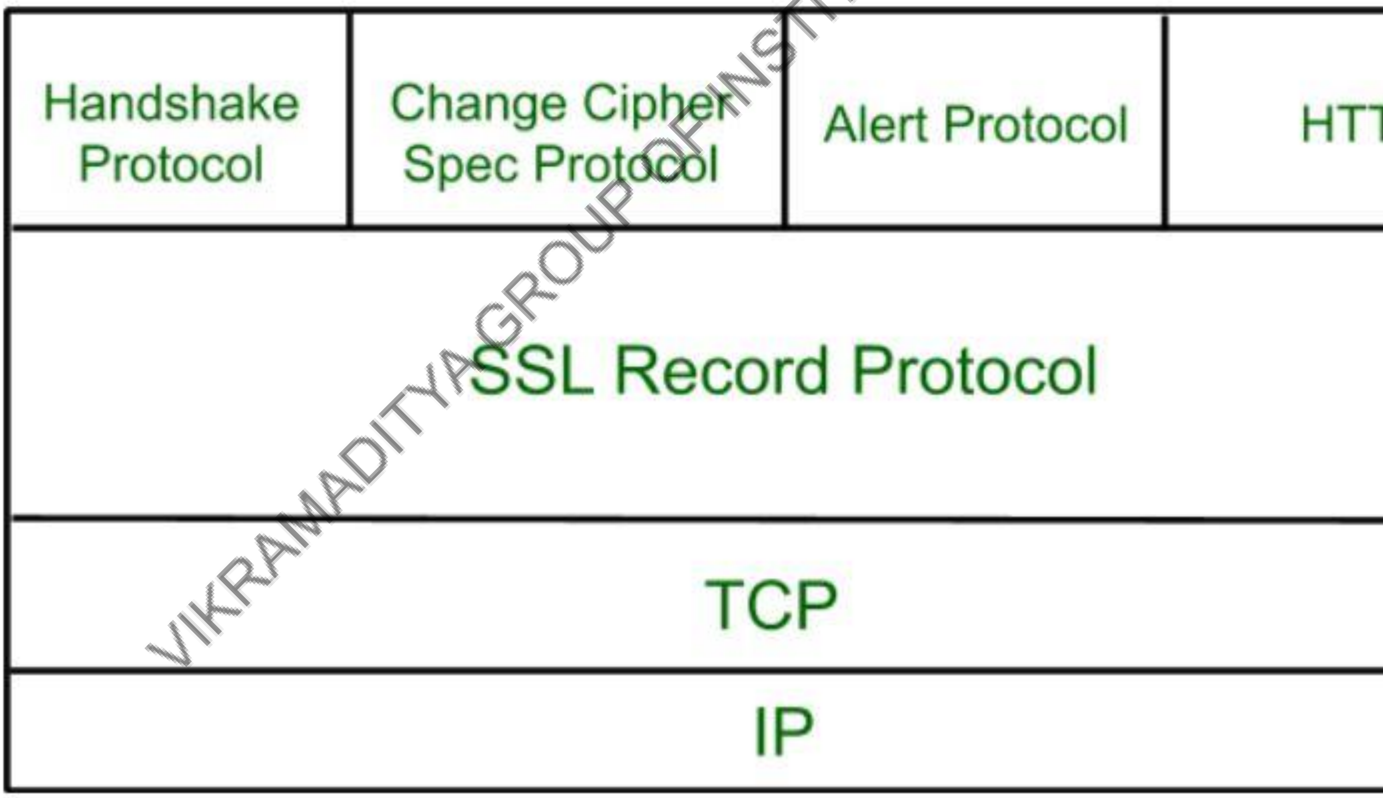
SSL was created to solve this problem and protect user privacy. By encrypting data between a user and a web server, SSL ensures that anyone who intercepts the data sees only a scrambled mess of characters. This keeps the user’s login credentials safe, visible only to the email service.

Additionally, SSL helps prevent cyber attacks by:

- **Authenticating Web Servers**: Ensuring that users are connecting to the legitimate website, not a fake one set up by attackers.
- **Preventing Data Tampering**: Acting like a tamper-proof seal, SSL ensures that the data sent and received hasn’t been altered during transit.

Secure Socket Layer Protocols

1. SSL Record Protocol
2. Handshake Protocol
3. Change-Cipher Spec Protocol
4. Alert Protocol



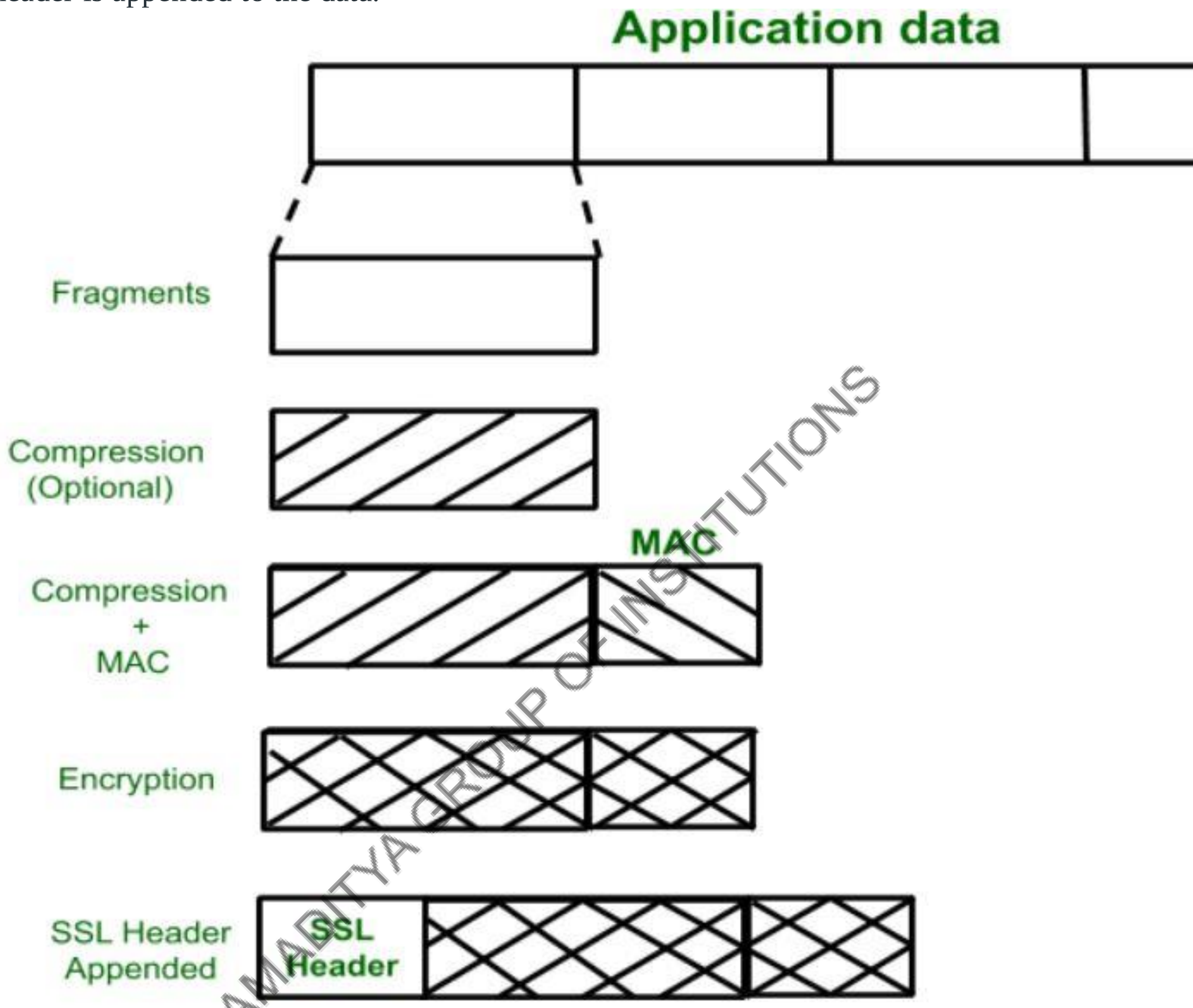
SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message

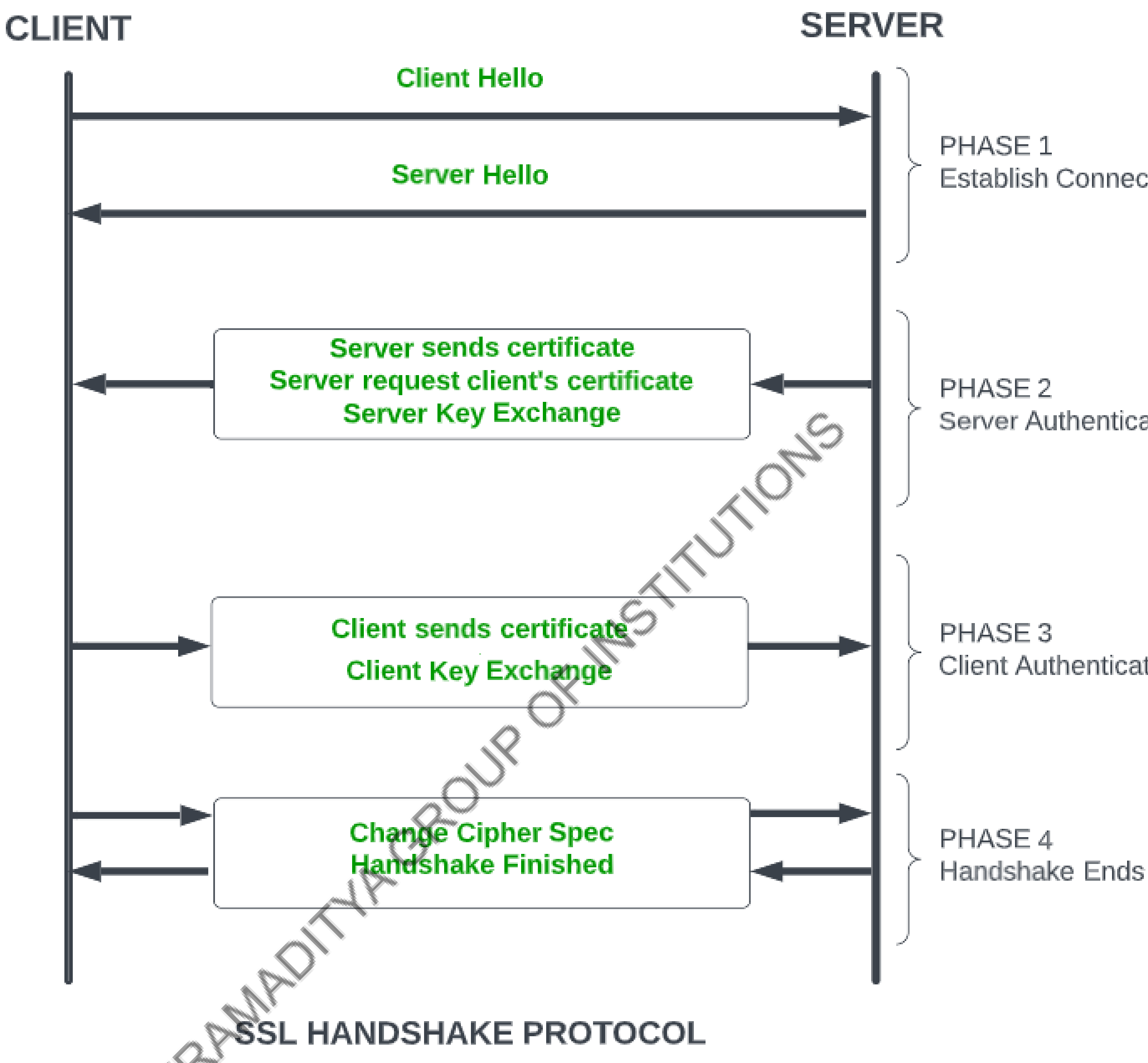
Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends it certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending it certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change Cipher Spec occurs and after this the Handshake Protocol ends.

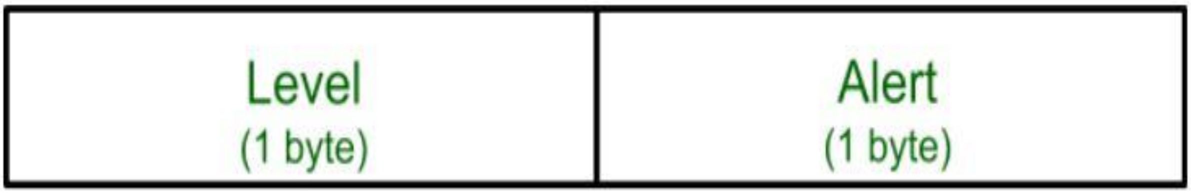


SSL Handshake Protocol Phases diagrammatic representation

Change-Cipher Protocol

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state. Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol
This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



Level (1 byte)	Alert (1 byte)

The level is further classified into two parts:
Warning (level = 1)
This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad Certificate:** When the received certificate is corrupt.
- **No Certificate:** When an appropriate certificate is not available.
- **Certificate Expired:** When a certificate has expired.
- **Certificate Unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
- **Close Notify**: It notifies that the sender will no longer send any messages in the connection.
- **Unsupported Certificate:** The type of certificate received is not supported.
- **Certificate Revoked:** The certificate received is in revocation list.

Fatal Error (level = 2):
This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are :

- **Handshake Failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.
- **Decompression Failure**: When the decompression function receives improper input.
- **Illegal Parameters:** When a field is out of range or inconsistent with other fields.
- **Bad Record MAC:** When an incorrect MAC was received.
- **Unexpected Message:** When an inappropriate message is received.

The second byte in the Alert protocol describes the error.

Salient Features of Secure Socket Layer

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Versions of SSL

SSL 1 – Never released due to high insecurity
SSL 2 – Released in 1995
SSL 3 – Released in 1996
TLS 1.0 – Released in 1999
TLS 1.1 – Released in 2006
TLS 1.2 – Released in 2008
TLS 1.3 – Released in 2018

Transport Layer Security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.
There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of TLS:
The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

Transport Layer Security (TLS) continues to play a critical role in securing data transmission over networks, especially on the internet. Let's delve deeper into its workings and significance:

Enhanced Security Features:

TLS employs a variety of cryptographic algorithms to provide a secure communication channel. This includes symmetric encryption algorithms like AES (Advanced Encryption Standard) and asymmetric algorithms like RSA and Diffie-Hellman key exchange. Additionally, TLS supports various hash functions for message integrity, such as SHA-256, ensuring that data remains confidential and unaltered during transit.

Certificate-Based Authentication:

One of the key components of TLS is its certificate-based authentication mechanism. When a client connects to a server, the server presents its digital certificate, which includes its public key and other identifying information. The client verifies the authenticity of the certificate using trusted root certificates stored locally or provided by a trusted authority, thereby establishing the server's identity.

Forward Secrecy:

TLS supports forward secrecy, a crucial security feature that ensures that even if an attacker compromises the server's private key in the future, they cannot decrypt past communications. This is achieved by generating ephemeral session keys for each session, which are not stored and thus cannot be compromised retroactively.

TLS Handshake Protocol:

The TLS handshake protocol is a crucial phase in establishing a secure connection between the client and the server. It involves multiple steps, including negotiating the TLS version, cipher suite, and exchanging cryptographic parameters. The handshake concludes with the exchange of key material used to derive session keys for encrypting and decrypting data.

Perfect Forward Secrecy (PFS):

Perfect Forward Secrecy is an advanced feature supported by TLS that ensures the confidentiality of past sessions even if the long-term secret keys are compromised. With PFS, each session key is derived independently, providing an additional layer of security against potential key compromise.

TLS Deployment Best Practices:

To ensure the effectiveness of TLS, it's essential to follow best practices in its deployment. This includes regularly updating TLS configurations to support the latest cryptographic standards and protocols, disabling deprecated algorithms and cipher suites, and keeping certificates up-to-date with strong key lengths.

Continual Evolution:
TLS standards continue to evolve to address emerging security threats and vulnerabilities. Ongoing efforts by standards bodies, such as the Internet Engineering Task Force (IETF), ensure that TLS remains robust and resilient against evolving attack vectors.

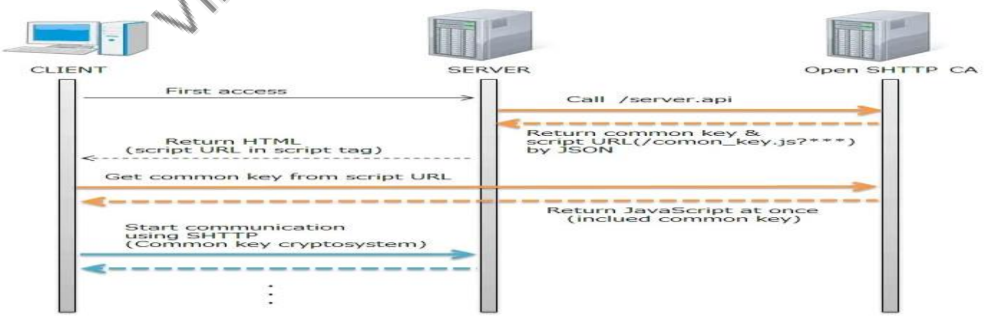
Conclusion:
In an increasingly interconnected world where data privacy and security are paramount, Transport Layer Security (TLS) serves as a foundational technology for securing communication over networks. By providing encryption, authentication, and integrity protection, TLS enables secure data transmission, safeguarding sensitive information from unauthorized access and tampering. As cyber threats evolve, TLS will continue to evolve, adapting to new challenges and reinforcing the security posture of digital communications.

S-HTTP (Secure Hypertext Transfer Protocol)

Secure Hypertext Transfer Protocol (S-HTTP) is a protocol used for encrypting HTTP traffic, enhancing the security of data as it travels across the World Wide Web. Essentially, S-HTTP is designed to secure individual messages transmitted between clients and servers, differentiating itself from other security protocols by its granularity and message-oriented approach.

Basic Functionality and Principles

The primary functionality of S-HTTP is to provide end-to-end encryption of web communications. It achieves this by encrypting the data before transmission and decrypting it upon receipt. This process ensures confidentiality and protects against eavesdropping and tampering. S-HTTP supports various encryption algorithms, enabling flexible security arrangements based on the needs of the communication parties. Furthermore, it provides options for authentication, ensuring that both sender and receiver can verify each other's identity, adding an additional layer of security to web interactions.



How S-HTTP Works

Technical Mechanism and Encryption Process

S-HTTP operates by encrypting individual HTTP messages, unlike other protocols that encrypt the entire communication session. This mechanism provides flexibility in securing specific parts of the data being transmitted. Each message, whether it's a request from the client or a response from the server, is encrypted independently.

The encryption process involves several key steps:

1. **Encryption Initiation:** When a message is ready for transmission, S-HTTP initiates encryption using a selected algorithm.
2. **Key Exchange:** S-HTTP supports various key exchange mechanisms. These keys are used to encrypt and decrypt messages at both ends.
3. **Data Encryption:** The actual data in the HTTP message is encrypted using the agreed-upon encryption standards, rendering it unreadable to unauthorized parties.
4. **Transmission and Decryption:** Once the encrypted message reaches its destination, it is decrypted using the corresponding decryption key.

Setting Up and Configuring S-HTTP

To set up S-HTTP:

1. **Server and Client Configuration:** Both the server and client must support S-HTTP. This involves configuring the web server and client applications to handle S-HTTP requests and responses.
2. **Certificate Management:** Obtain and install digital certificates to facilitate authentication and key exchange.
3. **Selecting Encryption Algorithms:** Choose suitable encryption algorithms based on the required level of security and the capabilities of the server and client.

S-HTTP vs. HTTPS: Understanding the Differences

Comparative Analysis of Protocols

While both S-HTTP and HTTPS are designed to secure HTTP communications, they differ fundamentally in their approach:

- **Encryption Scope:** Secure-HTTP encrypts individual messages, whereas HTTPS encrypts the entire communication session.
- **Flexibility:** SHTTP offers more flexibility in terms of what parts of the communication are encrypted. HTTPS, on the other hand, provides a uniform layer of encryption over all data exchanged.
- **Compatibility:** The Secure Hypertext Transfer Protocol can coexist with regular HTTP on a single server, while HTTPS typically requires a dedicated port.

Challenges and Limitations of S-HTTP

Technical Constraints

One of the major technical challenges facing S-HTTP was the complexity of its implementation. The protocol's message-specific encryption approach required more processing power and presented challenges in efficiently managing encryption keys. Moreover, the necessity for both client and server to support S-HTTP added to the complexity, making it less attractive compared to more straightforward alternatives like HTTPS

Secure Electronic Transaction (SET)

SET is a security protocol that enhances online payment security and integrity, especially those involving debit and credit cards. SET protects electronic payments by encrypting personal card details and authenticating users through digital certificates. SET ensures that only authorised parties can access sensitive information and that transactions are not tampered with. SET was developed in the late 1990s by Visa and Mastercard, in collaboration with several technology and Internet companies, such as Microsoft, IBM, Verisign and Netscape. The aim was to create a standard and universal protocol for securing online payments and promoting the growth of e-commerce.

SET is not a payment system, but a security framework that can be linked with existing payment systems. It is founded on the principles of Public Key Infrastructure (PKI). PKI relies on the use of both public and private keys to secure data through encryption and decryption, alongside digital certificates. This plays a crucial role in authenticating the parties engaged in the transaction.

How Does Secure Electronic Transaction Work?

Here is the step-by-step functioning of the secure electronic payment systems –

1. Customer Account Setup

You must open a credit card account with a bank supporting electronic payments and the SET protocol. You can visit the bank's website or contact customer service to do so.

2. Certificate Issuance to Customer

Once your identity is verified, you will receive a digital certificate from a trusted Certificate Authority (CA). This certificate contains essential details such as your name, public key, expiry date and certificate number. The CA ensures the authenticity and integrity of this certificate.

3. Merchant Certificate

To establish trustworthiness, merchants also obtain a digital certificate. This certificate verifies their identity and allows them to accept credit cards from certain issuers for secure electronic transactions.

4. Placing an Order

Browse through the merchant's website and select the items you wish to buy. This creates a record of your order on the merchant's site.

5. Merchant Verification

To assure authenticity, merchants send you their digital certificates, along with the order details. This helps you identify valid and authorised merchants.

6. Order and Payment Details

Next, you securely transmit your encrypted order and payment details to the merchant using your digital certificate for identification. The merchant cannot read this information but can verify your identity through your digital certificate.

7. Payment Authorisation Request

The merchant forwards the payment details to the payment gateway through an acquirer. They request payment authorisation from the payment gateway, which acts as an intermediary between the merchant and your credit card issuer.

8. Payment Gateway Authorisation

The payment gateway cross-verifies your credit card information with the issuer for authorising or rejecting the payment request. This verification process ensures online payment security by confirming that your credit card is valid and has sufficient funds.

9. Order Confirmation

Upon successful payment authorisation, the merchant confirms the order, providing payment authorisation details and purchase information.

10. Goods and Services Provision

Once the order is confirmed, the merchant provides the requested goods or services. This can include shipping physical products or granting access to digital content.

11. Payment Request by Merchant

Finally, after providing goods or services, the merchant requests payment from the payment gateway. The payment gateway interacts with various financial organisations, including the credit card issuer, acquirer and clearing house, to facilitate fund transfer from your account to the merchant's account.

Security Architecture of Secure Electronic Transaction

1. SET Digital Certificates

Digital certificates are issued by trusted third parties called Certificate Authorities, which verify the identity and public key of the certificate holder.

Cardholder certificates are assigned to you by your card issuer, such as a bank or credit card company. These certificates contain your name, account number, expiration date, and public key. Cardholder certificates allow you to prove your identity and payment information to merchants and payment gateways, reducing the threat of fraud and identity theft.

2. SET Dual Signatures

Digital signatures are utilised for card authentication during transactions. Each transaction generates encrypted digital signatures for the merchant, customer and associated financial institutions. This secures the transaction by encrypting order information with the merchant's public key and payment information with the acquiring bank's public key.

3. SET Digital Wallet

SET activates your digital wallet through a password-based self-authentication process to enable secure payments. After authentication, your device sends the purchase and payment details to the merchant. Upon successful authentication, the issuing bank provides payment authorisation to the acquiring bank, hence informing the merchant of the success of the transaction.

What are the Benefits of Secure Electronic Transactions?

Some of the most popular advantages of Secure Electronic Transactions are:

1. **Growing online sales:** With a projected growth of over 50% in global online retail sales in the next four years, it is essential to prioritise customer account security. Potential risks associated with fraud, data breaches and hacked accounts make it imperative for businesses to implement robust security measures.
2. **Mitigating security risks:** The SET protocol was introduced as a solution to secure credit card transactions over networks. Its advanced encryption and algorithm systems are specifically designed to address security challenges associated with online payments. By leveraging SET, businesses can engage in secure payments, protect sensitive customer data and prevent unauthorised access.
3. **Use of digital certificates:** SET issues digital certificates to users during transactions. These certificates are verified using digital signatures and certificates among all involved parties, including merchants, cardholders and financial entities. This ensures the authenticity and integrity of the transaction, reducing the risk of fraudulent activities.
4. **Ensuring privacy and confidentiality:** The combination of digital signatures and certificates in the SET protocol ensures complete privacy and confidentiality for transactions. It safeguards sensitive information

from unauthorised access or interception during transmission, instilling trust in customers while conducting online transactions.

Email Security

ntroduction to Email 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. In this article, we will understand the concept of **email security**, how we can protect our email, email security policies, and email security best practices, and one of the features of email is an email that we can use to protect the email from unauthorized access.

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. It can be achieved through a combination of technical and non-technical measures.

Some standard technical measures include the encryption of email messages to protect their contents, the use of digital signatures to verify the authenticity of the sender, and email filtering systems to block unwanted emails and malware, and the non-technical measures may include training employees on how to recognize and respond to phishing attacks and other email security threats, establishing policies and procedures for email use and management, and conducting regular security audits to identify and address vulnerabilities.

Why is email security important?

- **Protection Against Cyberattacks:** Email is a top goal for cybercriminals. Malware, phishing attacks, and other threats often arrive via email. In fact, 94% of malware is delivered through email channels1. By implementing robust email security measures, organizations can defend against these threats.
- **Reducing Risk:** Cybersecurity incidents can have devastating consequences, including financial losses, operational disruptions, and damage to an organization’s reputation. Effective email security helps protect your brand, reputation, and bottom line.
- **Compliance:** Email security ensures compliance with data protection laws like GDPR and HIPAA. By safeguarding sensitive information, organizations avoid legal fines and other intangible costs associated with cyberattacks.
- **Productivity Enhancement:** With email security in place, disruptions caused by threats like phishing emails are minimized. This allows organizations to focus more on business growth and less on handling security incidents.

Benefits of Email Security

- **Shielding Against Phishing and Spoofing Attacks:** Email security isn’t just about tech jargon; it’s like having a digital bodyguard. It helps spot and tackle threats like phishing or spoofing. These sneaky attacks can lead to serious breaches and even unleash malware or other nasty viruses.
- **Locking Down Data:** Think of email encryption as a virtual vault. It keeps sensitive info—like credit card numbers, bank accounts, and employee details—safe from prying eyes. No more accidental leaks or costly data breaches!
- **Whispers Only:** Secure email encryption ensures that only the right people get the message. It’s like passing a secret note in class—except the teacher won’t intercept it. Your confidential content stays confidential.
- **Spotting the Bad Apples:** Email security acts like a spam filter on steroids. It sniffs out malicious or spammy emails that might sneak past regular defenses. No more falling for those “You’ve won a million dollars!” scams!
- **Top-Secret Protection:** Imagine your company’s secrets—intellectual property, financial records, and classified info—wrapped in a digital force field. Email security shields them from cyber villains like hackers and cybercriminals.
- **Real-Time Guardian:** Zero-day exploits? Not on our watch! Email security solutions provide real-time protection. It’s like having a superhero squad that fights off malware and spam before they even knock on your inbox.
- **Locking Up Identity Theft:** Email encryption keeps attackers from swiping your login credentials or personal data. No more compromised accounts or identity theft nightmares.

Types of Email threats

- **Phishing:** Imagine a crafty imposter pretending to be your bank or favorite online store. They send you an email, asking for your sensitive info—like passwords or credit card details. Sneaky, right?
- **Social Engineering:** Think of it as digital manipulation. The bad guys sweet-talk or scare people into revealing confidential stuff. It’s like a cyber con artist pulling off a heist.
- **Spear Phishing:** This one’s like a sniper attack. Instead of casting a wide net, the attacker aims at specific individuals or organizations. They craft personalized emails, luring victims into their trap.
- **Ransomware:** Picture your files locked up in a digital vault. The villain—malicious software—holds them hostage until you pay a ransom. It’s like a cyber kidnapper!
- **Malware:** Sneaky software that infiltrates your computer without asking permission. It’s like a digital ninja wreaking havoc behind the scenes.
- **Spoofing:** Imagine someone wearing a disguise at a masquerade ball. Attackers forge email headers, making messages look legit—even when they’re not. Trust no masked stranger!

- **Man-in-the-Middle Attack:** Visualize a sneaky eavesdropper intercepting your messages. They can read, alter, or inject new content. It's like a cyber spy messing with your convo.
- **Data Exfiltration:** Sophisticated thieves sneak into an organization's email system. They swipe sensitive data—like secret recipes from a chef's kitchen. Recipe theft, anyone?
- **Denial of Service:** Attackers flood email servers with a deluge of messages. Servers buckle under the pressure, like a dam bursting. Chaos ensues!
- **Account Takeover:** Imagine a cyber burglar breaking into your email house. They use your account to send spam, phishing emails, or snoop around your secrets.
- **Identity Theft:** Someone swipes your personal info—name, address, social security number. They wear your identity like a stolen cloak, committing digital crimes.

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.
- **Use encryption:** It encrypts your email messages so that only the intended receiver can decipher them. Email encryption can be done by using the programs like PGP or S/MIME.
- Keep your software up to date. Ensure that the most recent security updates are installed on your operating system and email client.
- **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.
- **Choose a trustworthy email service provider:** Search for a service provider that protects your data using encryption and other security measures.
- **Use a VPN:** Using a VPN can help protect our email by encrypting our internet connection and disguising our IP address, making it more difficult for hackers to intercept our emails.
- **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.

Email Security Policies

The email policies are a set of regulations and standards for protecting the privacy, accuracy, and accessibility of email communication within the organization. An email security policy should include the following essential components:

- **Appropriate Use:** The policy should outline what comprises acceptable email usage inside the organization, including who is permitted to use email, how to use it, and for what purpose email we have to use.
- **Password and Authentication:** The policy should require strong passwords and two-factor authentication to ensure that only authorized users can access email accounts.
- **Encryption**: To avoid unwanted access, the policy should mandate that sensitive material be encrypted before being sent through email.
- **Virus Protection: T**he policy shall outline the period and timing of email messages and attachment collection.
- **Retention and Detection**: The policy should outline how long email messages and their attachments ought to be kept available, as well as when they should continue to be removed.
- **Training**: The policy should demand that all staff members take a course on email best practices, which includes how to identify phishing scams and other email-based threats.
- **Incident Reporting**: The policy should outline the reporting and investigation procedures for occurrences involving email security breaches or other problems.
- **Monitoring**: The policy should outline the procedures for monitoring email communications to ensure that it is being followed, including any logging or auditing that will be carried out.
- **Compliance**: The policy should ensure compliance with all essential laws and regulations, including the health
- Insurance rules, including the health portability and accountability act and the General Data Protection Regulation (GDPR)(HIPPA).
- **Enforcement:** The policy should specify the consequences for violating the email security policy, including disciplinary action and legal consequences if necessary.

What is an Information System?

An information system is a way to work with information using computers and other technology. It combines different parts like computer programs, physical devices, and networks. Businesses use information systems to collect important data. They use this data to run their operations smoothly. Information systems also help businesses talk to their customers. Using information systems makes businesses work better than their competitors.

Some companies like eBay, Amazon, Alibaba, and Google are built completely on using information systems and technology to work. These companies cannot operate without using information systems. In this article, we are going to discuss Information systems in detail along with the components and working of Information Systems.

What Are The Components of Information Systems?

- **Hardware:** Hardware is the physical parts you can touch like computers, disks, keyboards, and iPads. Hardware costs are lower now but using it can hurt the environment. Storage is now available in the "cloud" which you access through networks.
- **Software:** Software consists of programs that run on hardware. System software like Windows helps hardware work. Application software like Excel does specific tasks. Big companies buy special software for their needs. Some software is free to use.
- **Data consists of:** Data is just facts and numbers. When put together properly, data becomes useful information for businesses to make decisions.
- **Telecommunications:** Telecommunications connects computers and devices to share information. This can use wires or wireless signals like radio waves. Wires include fiber optics and cables. Wireless uses radio and microwave signals.

Examples of Information System

- Information systems are very important for businesses today. In the future, they will become even more important as more work is done by computers and AI.
- General information systems provide common services that many businesses need. For example, a database system helps organize all kinds of data. A company can use data in the database to understand trends, like what products customers buy at different times.
- Specialized information systems are designed for a specific purpose in a business. For example, an "expert system" can solve very complex problems in a specific area like medicine. The expert system can work faster and better than a person trying to solve the same problem alone.

Types of Information Systems

1. Operations Support Systems

These systems support specific business operations. For example, all banks use transaction processing systems to handle customer bank accounts and transactions. Operations support systems allow a company to manage a core business process.

2. Management Information Systems

These systems integrate hardware and software to help an organization's main functions. They collect data from different systems. The data is then analyzed to help managers make decisions for the business.

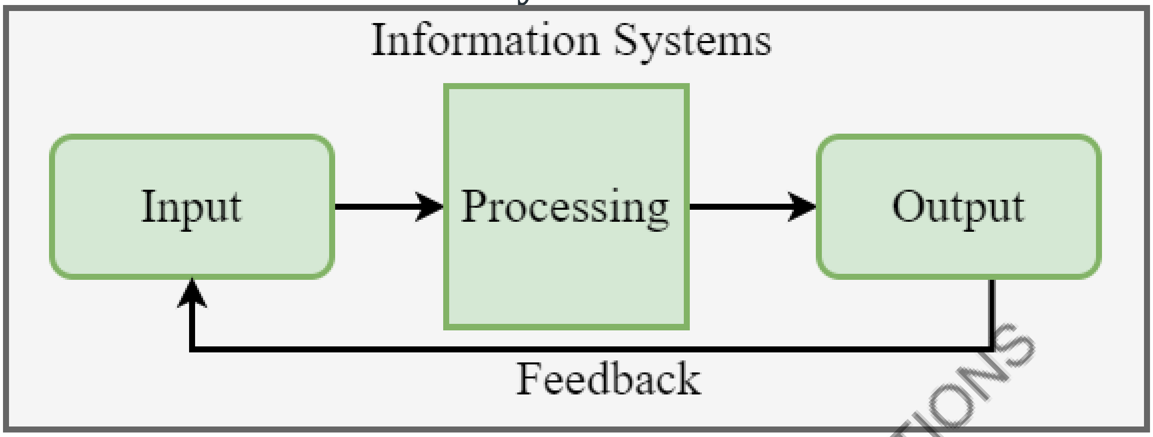
3. Decision Support Systems

These systems help organizations make informed decisions. They analyze rapidly changing information that cannot be planned in advance. Decision support systems can work automatically or with human operators. Using both humans and computers together works best.

4. Executive Information Systems

These are management support systems specifically for senior executives. Executive information systems help top managers make high-level decisions for the entire organization.

How Does Information System Work?



Working of information System

- **Input:** First the system collects data as input. This data can come from the typing, voice commands, touch screens, and sensors. The input data can be structured (organized) and unstructured (disorganized).
- **Processing:** Since the input data is raw the computers processor (CPU) has to organize it into the structured format. It does this through steps like the sorting, grouping, searching, analyzing, and making the reports.
- **Storage:** Next the organized data is stored temporarily or permanently. It gets stored in databases, hard drives, or solid-state drives.
- **Output:** The stored data is then analyzed and presented in a useful way like reports, dashboards, or data visualizations.
- **Feedback:** Finally the system gets feedback from users on their experience. This helps measure how well the system is working.

How to Manage Information Systems?

1. Set Policies and Procedures

Companies need to make clear rules on how to properly use and share data and information systems. Managers should assign specific duties to team members to monitor the systems. They should also hire people to audit (officially review) the processes.

2. Conduct Regular Audits

Check who is accessing systems and data trails (paths). Review how efficient the information systems are performing. Hire internal and external auditors to inspect system documentation and any changes made.

3. Operations Management

Information systems store a lot of private data. Companies must control data operations carefully. This includes documenting procedures, limiting who can access data servers, and managing data archives properly.

4. Physical Protection

It's not just software - the physical computer hardware and data centers need protection too. Have controls for temperature, power supply, and preventing service disruptions in the rooms housing the systems.

5. Identity Verification

Data security is very challenging. Use secure coding practices, firewalls, and identity verification like fingerprints, voice, or facial recognition to allow only approved people to access systems.

Threats to Information Security

Information security threats are actions or events that can compromise the confidentiality, integrity, or availability of data and systems. These threats can originate from various sources, such as individuals, groups, or natural events. Information Security threats can be many like Software attacks, theft of intellectual property, etc. In this article, we will discuss every point about threats to information security.

What is a Threat?

Threats are actions carried out primarily by hackers or attackers with malicious intent, to steal data, cause damage, or interfere with computer systems. **A threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, or harm objects. A threat is any potential danger that can harm your systems, data, or operations. In cybersecurity, threats include activities like hacking, malware attacks, or data breaches that aim to exploit vulnerabilities.

Recognizing and understanding these threats is crucial for implementing effective security measures. By identifying potential threats, you can better protect your sensitive information and maintain the integrity of your digital assets. Effective threat management is key to maintaining a secure and resilient cybersecurity posture.

What is Information Security?

Information security is the practice of protecting information by mitigating information risks. It involves protecting information systems and the information processed, stored, and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

Principles of Information Security

Information Security programs are built around 3 objectives, commonly known as CIA – Confidentiality, Integrity, and Availability.

- **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

- **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
- **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Common Information Security Threats

- **Virus:** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
- **Worms:** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
- **Bots:** Bots can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet**.
- **Adware:** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
- **Spyware:** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection. One of the most common example of spyware is KEYLOGGER. The basic job of

keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

- **Ransomware:** Ransomware is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
- **Scareware:** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
- **Rootkits:** **Rootkits** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
- **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

Information Security Solutions

- **Data Security Solutions**: These protect sensitive data from unauthorized access. Examples include encryption, access controls, and data loss prevention tools.
- **Network Security**: Focuses on securing communication channels and devices within a network. Firewalls, intrusion detection systems, and VPNs fall into this category.
- **Endpoint Security**: Protects individual devices (e.g., laptops, smartphones) from threats. Antivirus software and device management tools are common here.
- **Cloud Security**: Ensures data security in cloud environments. Encryption, access controls, and monitoring play key roles.
- **Identity and Access Management (IAM)**: Manages user access to systems and data. IAM solutions include single sign-on (SSO) and multi-factor authentication (MFA).
- **Security Information and Event Management (SIEM)**: **Security Information and Event Management (SIEM)** Collects and analyzes security-related data to detect and respond to threats.
- **Physical Security**: Protects physical assets (e.g., servers, data centers) through access controls, surveillance, and alarms.

Information Assurance

“Assurance” in security engineering is defined as the degree of confidence that the security needs of a system are satisfied.

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage and transmission of information. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

Undetected loopholes in the network can lead to unauthorized access, editing, copying or deleting of valuable information. This is where information assurance plays a key role.

Information assurance vs. cybersecurity

Information assurance predates the internet, and even though cybersecurity falls under the umbrella of IA, both play different roles in network security.

Focus

IA focuses on risk management and comes up with guidelines for keeping information secure, whether on physical (hard drives, PCs, laptops and tablets) or digital (cloud) systems. Cybersecurity focuses on setting up resilient network architecture to secure digital assets from unwarranted access.

Scope

IA is concerned with the business aspect of information. As a result, the scope is broader. Cybersecurity deals in the nitty-gritty to protect everything. As a result, the scope is more detailed.

Approach

IA is strategic, dealing with policy creation and deployment to keep information assets secure. It understands how an organization engages with information, the value of the information and how exposed that information happens to be. Cybersecurity is technical, dealing with security controls and tools to defend against cyberattacks.

Resources protected

IA protects data and information systems and includes both physical and digital data. Cybersecurity protects all digital investments, which include information, infrastructures, networks and applications.

Information assurance vs. information security

The NIST defines information security as the process of protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

The differences between information assurance and information security are more than just semantics.

Let’s break it down:

Focus

Information assurance focuses on quality, reliability and restoration of information. Information security focuses on deploying security solutions, encryption, policies and procedures to secure information.

Approach

IA is not concerned with the specific technology or tools used to protect information. Rather, it is centered around developing policies and standards. Information security directly deals with tools and technologies used to protect information. It’s a hands-on approach that safeguards data from cyberthreats.

Scope

IA stresses organizational risk management and overall information quality. As a result, IA has a broad scope. Information security stresses risk control and agreement. As a result, information security has a detailed scope.

Still not sure about the difference between information assurance, security and cybersecurity?

The purpose of IA is to reduce information risks by ensuring the information on which the business makes decisions is reliable. This purpose is achieved by following:

- **Risk management:** Businesses face legal fines and penalties if the information in the network is compromised. IA enables risk assessment to identify vulnerabilities and the potential impact on the business in terms of compliance, cost and operational continuity. The goal is to mitigate potential threats.
- **Encryption at rest and in transit:** IA mandates end-to-end encryption to protect privacy by ensuring no human or computer can read data at rest and in transit except the intended parties. The goal is to help businesses stay compliant with regulatory requirements and standards.
- **Data integrity:** Bad business decisions usually stem from bad data. IA focuses on auditing data collection and tracking process, improving transparency in the

organizational process. The goal is to manage data in a way that a future audit can retrace the process, leading to better decision-making.

Why do we need information assurance?

Adopting good IA best practices provides several benefits:

- **Operational benefits:**
- Resilient business processes
- Improved customer service
- Better information usage
- Improved responsiveness
- **Tactical benefits:**
- Easy compliance
- Better understanding of business opportunities
- Commitment from business partners and customers
- **Strategic benefits:**
- Better governance
- Cheaper equity
- More sales
- Lower costs
- **Organizational benefits:**
- Improved shareholder value
- Gain competitive advantage
- License to operate

How does information assurance work?

Information assurance is a strategic endeavor that extends beyond simply IT. The reality is that the legal and reputational ramifications that ensue from a data breach affect the entire organization. A proper security framework helps protect your organization and customers. IA is a work in progress that includes:

- **Strategy:** Develop Governance, Risk and Compliance (GRC) readiness by evaluating maturity as compared to your peers. Utilize key use cases to identify gaps and build roadmaps. Rationalize and prioritize GRC initiatives by aligning the essential requirements of your information and infrastructure with the organization’s objectives.

- **Design:** Design GRC programs and models to align with organizational policies. Exposures and risks should be quantified and classified to evaluate defined metrics. Once established, use these findings to define mitigation steps to manage risk and optimize speed, accuracy and efficiency of resolution.
- **Implementation:** Implement processes, policies, controls and technology that monitor operations against key metrics. Measure potential exposures in personnel, processes and technology controls in the context of IT infrastructure interdependencies.
- **Operations:** Mitigate exposures through continuous enforcement of policies. Detect violations and measure outcomes in comparison to your desired state. Use these learnings to continuously improve processes to maximize synergies and optimize outcomes.

Who is responsible for information assurance?

Conventionally, IA is seen as an incoherent function that is solely exclusive to the IT department. The reality is that the legal and reputational ramifications that ensue from a data breach affect the entire organization. It is essential to create a security-centric culture from top to bottom, with a focus on complying with information security regulations.

What are the five pillars of information assurance?

The CIA triad is considered the first model of information assurance introduced to define effective practices of assuring information security and integrity. Here are the following five pillars of IA that make information networks safe against all threats:

- Integrity (protection of information systems and assets)
- Availability (dependable access to information systems by authorized users)
- Authentication (the process of restricting access and confirming the identity of users)
- Confidentiality (restriction of access to authorized users only)
- Non-repudiation (forensic tracking to create a reliable “paper trail” of all actions)

Integrity

Information sent should always remain in its original state. Integrity means tampering or modification by bad actors should not occur. Therefore, the primary goal of this pillar is to set up safeguards to deter threats.

Availability

Easy data access helps users seamlessly access important information to perform critical tasks. Availability means those who need access to information can do so. Therefore, the primary goal of this pillar is to ensure systems always remain fully functional.

Authenticity

Verify the identity of a user (device) before allowing them to access data with methods like two-factor authentication, password management, biometrics and other devices. Authenticity means ensuring that those who have access to information are who they say they are. The primary goal of this pillar is to prevent identity theft.

Confidentiality

Protect private information from getting exposed by any unauthorized users, systems or networks. Confidentiality means data should be accessed only by those who have proper authorization. Therefore, the primary goal of this pillar is to avoid IP theft or the compromise of Personal Identifiable Information (PII) of customers.

Non-repudiation

It is important that the information system is able to provide proof of delivery to confirm that the data was properly transmitted. Non-repudiation means someone with access to your organization's information system cannot deny having completed an action within the system, as there should be methods in place to prove that they did make said action. The primary goal of this pillar is to guarantee that the digital signature is that of the intended party, thereby granting authorization to the protected information.

Cyber Security Risk Analysis

Risk analysis refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis. Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage.

Enterprise and organization used risk analysis:

- To anticipates and reduce the effect of harmful results occurred from adverse events.
- To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.

- To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
- To identify the impact of and prepare for changes in the enterprise environment.

Benefits of risk analysis

Every organization needs to understand about the risks associated with their information systems to effectively and efficiently protect their IT assets. Risk analysis can help an organization to improve their security in many ways. These are:

- Concerning financial and organizational impacts, it identifies, rate and compares the overall impact of risks related to the organization.
- It helps to identify gaps in information security and determine the next steps to eliminate the risks of security.
- It can also enhance the communication and decision-making processes related to information security.
- It improves security policies and procedures as well as develop cost-effective methods for implementing information security policies and procedures.
- It increases employee awareness about risks and security measures during the risk analysis process and understands the financial impacts of potential security risks.

Steps in the risk analysis process

The basic steps followed by a risk analysis process are:

Conduct a risk assessment survey:

Getting the input from management and department heads is critical to the risk assessment process. The risk assessment survey refers to begin documenting the specific risks or threats within each department.

Identify the risks:

This step is used to evaluate an IT system or other aspects of an organization to identify the risk related to software, hardware, data, and IT employees. It identifies the possible adverse events that could occur in an organization such as human error, flooding, fire, or earthquakes.

Analyse the risks:

Once the risks are evaluated and identified, the risk analysis process should analyse each risk that will occur, as well as determine the consequences linked with each risk. It also determines how they might affect the objectives of an IT project.

Develop a risk management plan:

After analysis of the Risk that provides an idea about which assets are valuable and which threats will probably affect the IT assets negatively, we would develop a plan for risk management to produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.

Implement the risk management plan:

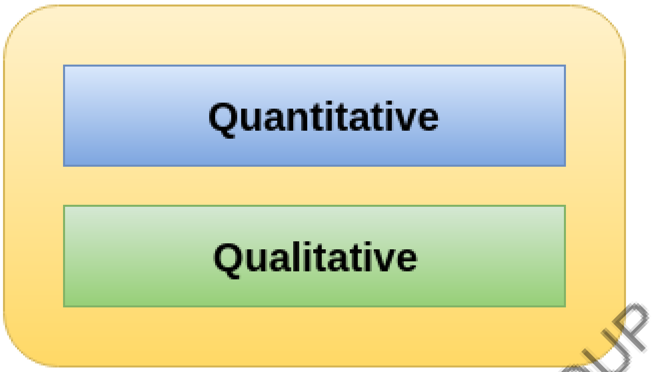
The primary goal of this step is to implement the measures to remove or reduce the analyses risks. We can remove or reduce the risk from starting with the highest priority and resolve or at least mitigate each risk so that it is no longer a threat.

Monitor the risks:

This step is responsible for monitoring the security risk on a regular basis for identifying, treating and managing risks that should be an essential part of any risk analysis process.

Types of Risk Analysis

The essential number of distinct approaches related to risk analysis are:



Types of Risk Analysis

Qualitative Risk Analysis

- The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.
- The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
- The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
- Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

Quantitative Risk Analysis

- The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.
- It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.

- Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which

Cyber Security Policy

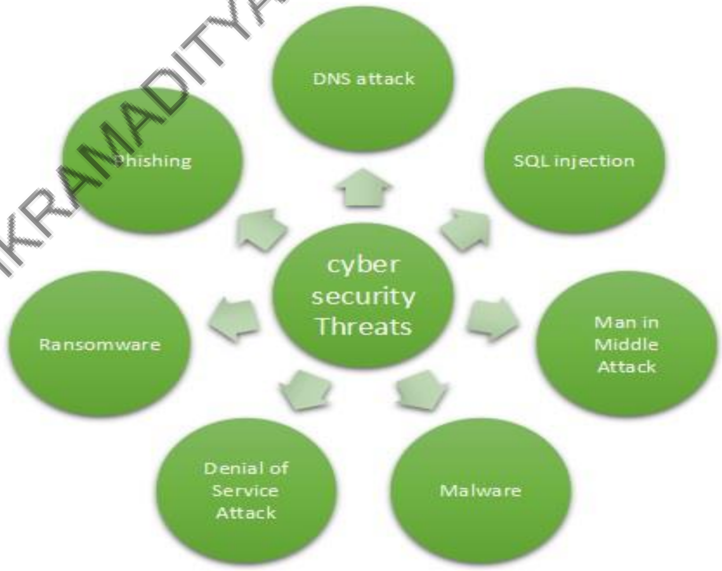
Cybersecurity plays a crucial role in the digital world. Securing information and data has become one of the most important challenges in the present day. Whenever we expect cybersecurity the primary thing that involves our mind is cyber crimes which are increasing immensely day by day. Various Governments and Organizations are taking many measures to stop these cybercrimes. Besides various measures, cybersecurity remains a massive concern to several.

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by the worldwide distribution of information and communication technology (ICT) devices and networks.

Insider threats affect more than 34% of organizations worldwide each year because of this, cybersecurity needs to be a top priority and concern for all employees within a company, not just the senior management and IT staff. Employees are frequently the weakest point in a company's security strategy because they unintentionally click on malicious links and attachments, share passwords, and fail to encrypt sensitive files. A cybersecurity policy that details each employee's obligations for safeguarding the organization's systems and data is a useful tool for educating staff members about the significance of security.

The Top Three Cybersecurity Trends

- **Ransomware**
- **Cyber attack Surface** (IoT supply chain and Remote work systems)
- **Threats to IT infrastructure**



In the extensive growth of the IT sector in different countries, ambitious plans for rapid social transformation and inclusive growth, and providing the right kind of focus for creating a secure computing environment and adequate trust and confidence in electronic transactions, software, services, devices, and networks, has become one of the compelling priorities for all.

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in cyberspace can be exploited for nefarious purposes. The protection of information cyberspace and preservation of the confidentiality, integrity, and availability of information in cyberspace is the essence of secure cyberspace.

Why Cyber Security Policies Are Important

Companies face potential risks to their systems and data. Many cyberattacks take advantage of an organization's employees in some way, exploiting negligence or tricking them into taking action through phishing or social engineering attacks The rise of remote work also poses additional threats due to growing BYOD policies and the potential for faulty equipment to connect therefore to corporate networks.

Cybersecurity policies help protect an organization from cyber threats and ensure compliance with applicable laws. These policies can reduce an organization's risk by training employees to avoid certain activities and enable effective incident response by defining policies for detection, prevention, and remediation.

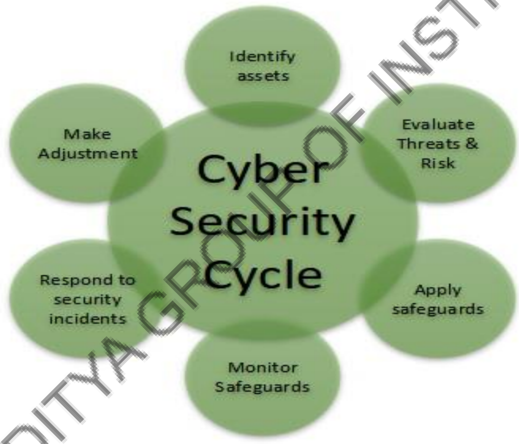


Fig:2 Cybersecurity Cycle

Types of Cyber Security Policies

1. Acceptable Use of Data Systems Policy

The purpose of this policy is to stipulate the suitable use of computer devices at the corporation/company. These rules protect the authorized user and therefore the company. Inappropriate use exposes the corporate to risks including virus attacks, compromise of network systems and services, and legal issues.

2. Account Management Policy

The purpose of this policy is to determine a typical for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at the corporation.

3. Anti-Virus

This policy was established to assist prevent attacks on corporate computers, networks, and technology systems from malware and other malicious code. This policy is meant to assist prevent damage to user applications, data, files, and hardware. Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for new viruses as soon as they are discovered. Anti-virus software is a must and a basic necessity for every system.

4. E-Commerce Policy

The frequency of cyber-attacks has been high in recent years. E-commerce security refers to the measures taken to secure businesses and their customers against cyber threats. This e-commerce policy is to be used as both a suggestion and a summary within the management of the E-Commerce electronic services.

5. E-Mail Policy

Email security may be a term for describing different procedures and techniques for shielding email accounts, content, and communication against unauthorized access, loss, or compromise. Email is usually wont to spread malware, spam, and phishing attacks. Attackers use deceptive messages to entice recipients to spare sensitive information, open attachments, or click on hyperlinks that install malware on the victim's device. Email is additionally a standard entry point for attackers looking to realize an edge in an enterprise network and acquire valuable company data. Email encryption involves encrypting, or disguising, the content of email messages to guard potentially sensitive information against being read by anyone aside from intended recipients. Email encryption often includes authentication. The purpose of this policy is to determine rules for the utilization of corporate email for sending, receiving, or storing electronic messages.

6. Hardware And Electronic Media Disposal Policy

The company-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

7. Security Incident Management Policy

This policy defines the need for reporting and responding to incidents associated with the company's information systems and operations. Incident response provides the corporation with the potential to spot when a security incident occurs.

8. Information Technology Purchasing Policy

The reason for this strategy is to characterize norms, methods, and limitations for the acquisition of all IT equipment, programming, PC-related parts, and specialized administrations bought with organization reserves. Acquisition of innovation and specialized administrations for the organization should be supported and facilitated through the IT Department.

9. Web Policy

The reason for this policy is to set up guidelines for the utilization of the organization’s Internet for access to the Internet or the Intranet.

10. Log Management Policy

Log management is often of great benefit during a sort of scenario, with proper management, to reinforce security, system performance, resource management, and regulatory compliance.

11. Network Security And VPN Acceptable Use Policy

The purpose of this policy is to define standards for connecting to the company’s network from any host. These standards are designed to attenuate the potential exposure to the corporation from damages, which can result from unauthorized use of the company’s resources. Damages include the loss of sensitive or company confidential data, property, damage to critical company internal systems, etc.

12. Password Policy

The concept of usernames and passwords has been a fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity. The purpose of this policy is to determine a typical for the creation of strong passwords, the protection of these passwords, and therefore the frequency of changing passwords must be followed.

13. Patch Management Policy

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the event and propagation of malicious software, which may disrupt normal business operations, additionally placing the corporation in danger. To effectively mitigate this risk, software “patches” are made available to get rid of a given security vulnerability.

14. Cloud Computing Adoption

The purpose of this policy is to make sure that the corporate can potentially make appropriate cloud adoption decisions and at an equivalent time doesn’t use, or allow the utilization of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed during this policy.

15. Server Security Policy

The purpose of this policy is to define standards and restrictions for the bottom configuration of internal server equipment owned and/or operated by or on the company’s internal network(s) or related technology resources via any channel.

16. Social Media Acceptable Use Policy

The use of external social media within organizations for business purposes is increasing. The corporation faces exposure to a particular amount of data that will be visible to friends of friends from social media. While this exposure may be a key mechanism driving value, it also can create an inappropriate conduit for information to pass between personal and business contacts. Tools to determine barriers between personal and personal networks and tools to centrally manage accounts are only starting to emerge. Involvement by the IT Department in security, privacy, and bandwidth concerns is of maximal importance.

17. Systems Monitoring And Auditing Policy

System monitoring and auditing are employed to work out if inappropriate actions have occurred within a data system. System monitoring is employed to look for these actions in real-time while system auditing looks for them after the very fact.

18. Vulnerability Assessment

The purpose of this policy is to determine standards for periodic vulnerability assessments. This policy reflects the company's commitment to spot and implementing security controls, which can keep risks to data system resources at reasonable and appropriate levels.

19. Website Operation Policy

The purpose of this policy is to determine guidelines concerning communication and updates of the company's public-facing website. Protecting the knowledge on and within the corporate website, with equivalent safety and confidentiality standards utilized within the transaction of all the corporate business, is significant to the company's success.

20. Workstation Configuration Security Policy

The purpose of this policy is to reinforce security and quality operating status for workstations utilized at the corporation. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to take care of these guidelines and to figure collaboratively with IT resources to take care of the rules that are deployed.

21. Server Virtualization

The purpose of this policy is to determine server virtualization requirements that outline the acquisition, use, and management of server virtualization technologies. This policy provides controls that make sure that Enterprise issues are considered, alongside business objectives, when making server virtualization-related decisions. Platform Architecture policies, standards, and guidelines are going to be wont to acquire, design, implement, and manage all server virtualization technologies.

22. Wireless Connectivity Policy

The purpose of this policy is to secure and protect the knowledge assets owned by the corporation and to determine awareness and safe practices for connecting to free and unsecured Wi-Fi, which can be provided by the corporation. The corporation provides computer devices, networks, and other electronic information systems for goals and initiatives. The corporation grants access to those resources as a privilege and must manage them responsibly to take care of the confidentiality, integrity, and availability of all information assets.

23. Telecommuting Policy

For the needs of this policy, a reference is formed to the defined telecommuting employee who regularly performs their work from an office that's not within a corporate building or suite. Casual telework by employees or remote work by non-employees isn't included herein. That specializes in the IT equipment typically provided to a telecommuter, this policy addresses the telecommuting work arrangement and therefore the responsibility for the equipment provided by the corporation.

24. Firewall

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the Internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence, firewalls play an important role in detecting malware.

25. Malware scanner

This is software that sometimes scans all the files and documents present within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are samples of malicious software that are often grouped and mentioned as malware.

Why Should be Cyber Security Policies developed?

A cybersecurity strategy has far-reaching implications throughout an organization and can affect multiple departments. For example, IT staff may be responsible for implementing the system, while legal or HR teams may be responsible for enforcing it.

As a result, it must be formed and managed by a cross-functional team comprised of IT, legal, HR, and management. This ensures that the plan is consistent with the strategic objectives of the agency and applicable law, and that potential technical measure or corrections can be effectively implemented.

How to Create a Cyber Security Policy

- **Identify the threat surface:** The organization has systems in place to address threats and risks. The first step in policy writing is to have a clear understanding of the policies and procedures that need to be regulated, such as the use of personal devices for business purposes.
- **Identify relevant requirements:** Corporate cybersecurity policies may also have internal and external motivations, such as corporate security objectives and regulatory requirements (HIPAA, PCI DSS, etc.). The next step in cybersecurity design is to define the requirements that the system must meet.
- **Creating a plan:** Once needs are identified, the next step is drafting a plan. This should be done by a team of stakeholders from IT, legal, HR and management.
- **Ask for feedback:** Cyber security policies are most effective if they are clear and understood by employees. Seeking information from informal employees in the organizational group can help avoid such misunderstandings and issues.
- **Train employees:** Once developed, the plan should be distributed through the organization. Also, employees should be trained on this process to follow their requirements.
- **Update your policy regularly:** Policies can become out dated and requirements can change. It should be reviewed and updated regularly.

How Do You Enforce A Security Policy?

There are several ways to enforce security policies within an organization including:

- **Communication** – Clearly communicate security policies to all employees to ensure they understand their responsibilities in maintaining the security of the organization. Providing training and resources for employees is critical to help them understand and adhere to the policies.
- **Access controls** – Access controls help enforce security policies by limiting access to systems and data to authorized users only. This can include processes such as user authentication and authorization or multi-factor authentication.
- **Monitoring and auditing** – Regular monitoring and auditing of systems can help detect policy violations and identify areas where additional controls are required.
- **Consequences** – Consequences for policy violations are needed to enforce security policies. Without some disciplinary action in place employees will continue to operate under the assumption that they can get away with it.

Cyber security standard

A cyber security standard is a set of guidelines or best practices that organizations can use to improve their cyber security posture.

Organizations can use cyber security standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. Standards can also provide guidance on how to respond to and recover from cyber security incidents.

Cyber security frameworks are generally applicable to all organizations, regardless of their size, industry, or sector. This page details the common cyber security compliance standards that form a strong basis for any cyber security strategy.

DFARS (Defense Federal Acquisition Regulation Supplement)

The DFARS (Defense Federal Acquisition Regulation Supplement) is a set of regulations issued by the DOD (Department of Defense) that supplements the Federal Acquisition Regulation. The DFARS provides guidance and procedures for acquiring supplies and services for the DOD.

DOD government acquisition officials, contractors, and subcontractors doing business with the DOD must adhere to the DFARS.

FISMA (Federal Information Security Management Act)

The FISMA (Federal Information Security Management Act) is a US federal law enacted as Title III of the E-Government Act of 2002. The law establishes a comprehensive framework for ensuring the security of information and information systems for all executive branch agencies.

The FISMA was put in place to strengthen information security within federal agencies, NIST, and the OMB (Office of Management and Budget). It requires federal agencies to implement information security programs to ensure their information and IT systems' confidentiality, integrity, and availability, including those provided or managed by other agencies or contractors.

HIPAA (Health Insurance Portability and Accountability Act)

The HIPAA (Health Insurance Portability and Accountability Act) is a set of federal regulations that protect the privacy of patients' health information. The HIPAA applies to all forms of health information, including paper records, electronic records, and oral communications.

It aims to make it easier for people to keep their health insurance when they change jobs, protect the confidentiality and security of health care information, and help the health care industry control its administrative costs.

ISO 22301

ISO 22301 is an international standard that outlines how organizations can ensure business continuity and protect themselves from disaster. The Standard provides a framework for a comprehensive BCMS (business continuity management system). It can be used by any organization, regardless of size, industry, or location.

ISO/IEC 27001

ISO 27001 is an international standard for information security that provides a framework for managing sensitive company information. The Standard includes requirements for developing an ISMS (information security management system), implementing security controls, and conducting risk assessments.

The Standard's framework is designed to help organizations manage their security practices in one place, consistently and cost-effectively.

ISO/IEC 27002

ISO 27002 is the code of practice for information security management. It provides guidance and recommendations on how to implement security controls within an organization. ISO 27002 supports the ISO 27001 standard, which provides the requirements for an ISMS.

ISO/IEC 27031

ISO 27031 is a standard for ICT (information and communications technology) preparedness for business continuity. It provides guidance on how organizations can use ICT to protect their business operations and ensure continuity in the event of an incident or a disaster.

Achieving compliance with ISO 27031 helps organizations understand the threats to ICT services, ensuring their safety in the event of an unplanned incident.

ISO/IEC 27032

ISO 27032 is an internationally recognized standard that provides guidance on cybersecurity for organizations. The Standard is designed to help organizations protect themselves against cyber attacks and manage the risks associated with the use of technology. It is based on a risk management approach and provides guidance on how to identify, assess, and manage cyber risks. The Standard also includes guidance on incident response and recovery.

ISO/IEC 27701

ISO 27701 specifies the requirements for a PIMS (privacy information management system) based on the requirements of ISO 27001. It is extended by a set of privacy-specific requirements, control objectives, and controls.

Organizations that have implemented ISO 27001 can use ISO 27701 to extend their security efforts to cover privacy management. This can help demonstrate compliance with data protection laws such as the California Privacy Rights Act (CPRA) and the EU General Data Protection Regulation (GDPR).

NIST CSF (Cybersecurity Framework)

The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a voluntary framework that provides a set of standards, guidelines, and best practices for managing cybersecurity risks.

The framework helps organizations to identify, assess, and manage their cybersecurity risks in a structured and repeatable manner. The framework is not mandatory, but it is increasingly being adopted by organizations as a voluntary measure to improve their cybersecurity posture.

Intellectual Property Rights

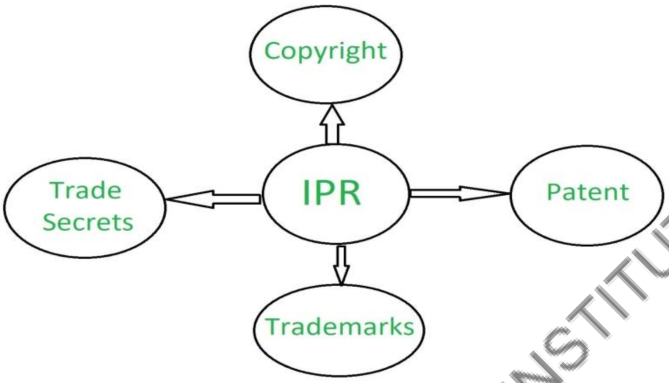
Intellectual property rights are the rights given to each and every person for the creation of new things according to their minds. IPR usually give the creator a complete right over the use of his/her creation for a certain period of time.

Intellectual property rights are the legal rights that cover the benefits given to individuals who are the owners and inventors of work and have created something unique with their intellectual creativity or capability. Every person related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in their business practices by them.

The creator/inventor gets complete rights against any misuse or use of work without his/her prior information. However, the rights are issued for a limited period of time to maintain equilibrium.

What are Intellectual Properties?

1. Industrial designs
2. Scientific discoveries
3. Protection against unfair competition
4. Literary, artistic, and scientific works
5. Inventions in all fields of human endeavor
6. Trademarks, service marks, commercial names, and designations



Types of Intellectual Property Rights:
Intellectual Property Rights can be classified into four types:

1. **Copyright:** Copyright is a term that describes ownership or control of the rights to the use and distribution of certain works of creative expression, including books, videos, movies, music, and computer programs.
2. **Patent:** A patent gives its owner the right to exclude others from making, using, selling, and importing an invention for a limited period of time. The patent rights are granted in exchange for enabling public disclosure of the invention.
3. **Trademark:** A Trademark is a Graphical representation that is used to distinguish the goods and services of one party from those of others. A Trademark may consist of a letter, number, word, phrase, logo, graphic, shape, smell, sound, or combination of these things.
4. **Trade Secrets:** Trade secret describes about the general formula of any product and the key behind any organization’s progress. It also includes various firms’ different secret formulas for the same products which differ in quality.

Advantages of Intellectual Property Rights:

The advantages of intellectual property rights are as follows:

- IPR yields exclusive rights to the creators or inventors.
- It encourages individuals to distribute and share information and data instead of keeping it confidential.
- It provides legal defense and offers the creators the incentive of their work.
- It helps in social and financial development.
- It inspires people to create new things without fear of intellectual theft.