## Definitions

1) **Computer Security: Computer Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization.**
2) **Assets:** Asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software and confidential information.
3) **Vulnerability:** It is a weakness in computer system & network. The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful. Vulnerability testing should be performed on an on-going basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed. Such vulnerabilities are not particular to technology — they can also apply to social factors

such as individual authentication and authorization policies.

4) **Threats:** a threat is an action by attacker who tries to exploit vulnerabilities to damage assets. Threats can be identified by the damage done to assets
5) **Information: Information** is organized or classified data, which has some meaningful values for the receiver. Information is the processed data on which knowledge, decisions and actions are based.

6) **Risk:** Risk is probability of threats that may occur because of presence of vulnerability in a system OR Risk is any event or action that could cause a loss or damage to computer hardware, software, data, or information.
7) **Access Control:** Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to modify data or resources. Access control is

to specify, control and limit the access to the host system or application, which prevents unauthorized use to
access or modify data or resources

8) **Virus** Virus is a program which attaches itself to another program and causes damage to the computer system or the network. It is loaded onto your computer without your knowledge and runs against your wishes.

1) **Worm:** a worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

2) **Intruder: *Intruders* are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access. Intruders are of three types, namely, *masquerader*, *misfeasor* and *clandestine user*.**

3) **Insider: Typically, an insider threat in cybersecurity refers to an individual using their authorized access to an organization's data and resources to harm the company's equipment, information, networks, and systems**

4) **DOS: DoS attacks are attempts to interrupt a website or network's operations by overwhelming it with traffic. The attacker achieves this by sending an enormous amount of requests to the target server, which causes it to**

**slow down or even crash, making it inaccessible to legitimate users**

5) **DDOS:** Distributed **Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DoS attack.**
6) **A DDoS attack uses multiple servers and Internet connections to flood the targeted resource**
7) **Operating system security** The OS must protect itself from security breaches, such as runaway processes ( denial of service ), memory-access violations, stack overflow violations, the launching of programs with excessive privileges, and many others.
8) **Hotfix** Normally this term is given to small software update designed to address a particular problem like buffer overflow in an application that exposes the system to attacks.
9) **Patch:** This term is generally applied to more formal, larger s/w updates that may address several or many s/w problems. Patches often contain improvement or additional capabilities & fixes for known bugs.

10) **Service packs** *service pack* is a collection of updates and fixes, called patches, for an operating system or a software program. Many of these patches are often released before a larger service

pack, but the service pack allows for an easy, single installation.

**OR**

A service pack (SP) is an update, often combining previously released updates, that helps make Windows more reliable. Service packs can include security and performance improvements and support for new types of hardware

**11) Authentication: Authentication is the process of verifying the identity of a user or information. User authentication is the process of verifying the identity of a user when that user logs in to a computer system.**

**Process of determining identity in following 3 ways:**

i. **Something you know:**
   1. **Common identification mechanism: user ID, password**
   2. **Should not be shared with anyone else**

ii. **Something you have:**
   1. **Use of something like lock and key**

2. **Only individuals having valid key can open the lock**

iii. **Something about you:**

1. **Something unique about you: finger print, DNA**

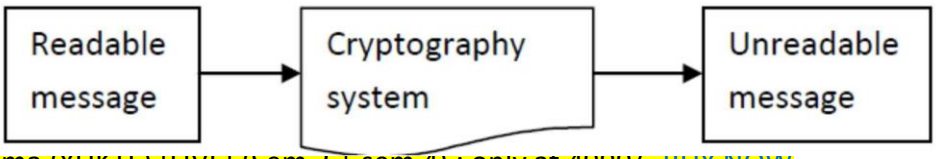
12) **Authorization: it is the process of verifying that a known person has the authority to perform a certain operation. Authorization cannot occur without authentication**

13) **Biometrics** Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural characteristics

14) **Plaintext:** plaintext also known as clear text mean anyone who knows the language can easily read the message

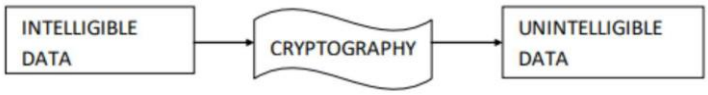
15) **Ciphertext:** when plaintext is codified with the help of any suitable scheme , then the resultant message is known as ciphertext

16) **Cryptography** It is art & science of achieving security by encoding messages to make them non-readable.



or

Cryptography is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible




17) **Cryptanalysis** Cryptanalysis is the art or science comprising the principles and methods of transforming an unintelligible message

**18)** back into an intelligible message without the knowledge of key.


19) **Cryptology** Cryptology is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible and unintelligible message back to intelligible one.


**20) Encryption:** Encryption is the process of converting readable plaintext into unreadable ciphertext to protect sensitive information from unauthorized access. This transformation is achieved using encryption algorithms that

scramble the data into an indecipherable format. Only authorized parties with the correct decryption key can revert the ciphertext back to its original plaintext form

**Encryption is the process of converting a normal message (plain text) into a meaningless message (ciphertext).**

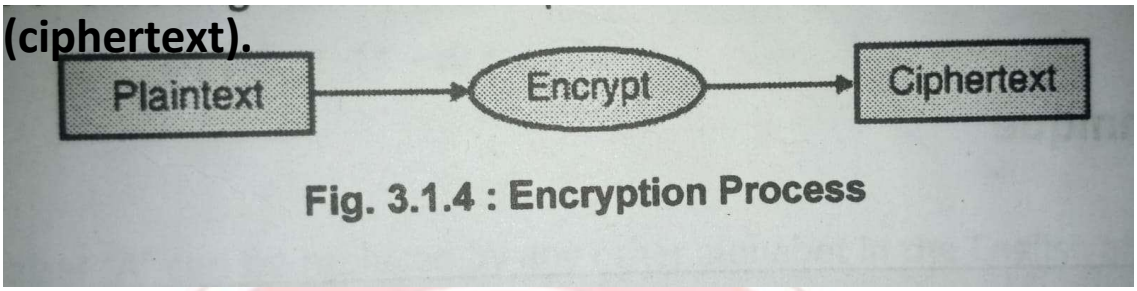



Fig. 3.1.4 : Encryption Process

**21) Decryption: Decryption is the process of converting a meaningless message (ciphertext) into its original form (plaintext)**
**Decryption is the process of converting data that has been rendered unreadable through encryption back to its original, readable form.**

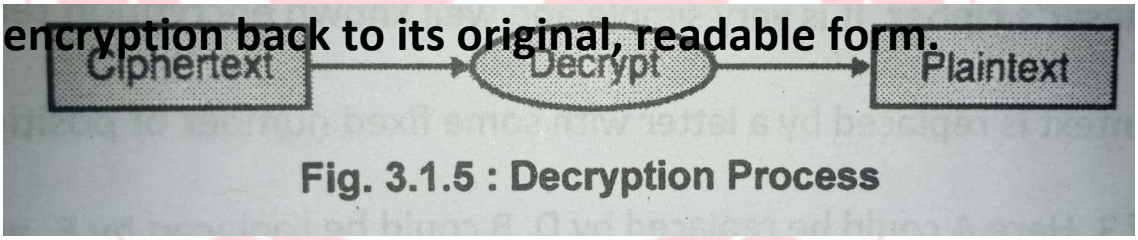



Fig. 3.1.5 : Decryption Process

22) **Steganography** Steganography is the art and science of writing hidden message in such a way that no one apart from sender and intended recipient suspects the existence of the message.

**23) Cyber Crime : Cybercrime refers to illegal activities carried out using computers and the Internet. These crimes can range from stealing personal information and financial fraud to hacking and spreading malicious**

**software. Cybercrime poses significant risks to individuals, businesses, and governments worldwide.**

**24) Hacking: An effort to attack a computer system or a private network inside a computer is known as hacking**

**25) Digital forgery: the crime of falsely altering or manipulating a document with the intension of misleading others**

**26) Cyberstalking:** Cyber Stalking means following some ones activity over internet. This can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

OR

Cyberstalking/ Harassment refers to the use of the internet and other technologies to harass or stalk another person online, and is potentially a crime in the India under IT act-2000. This online

harassment, which is an extension of cyberbullying and in person stalking, can take the form of e-mails, text messages, social media posts, and more and is often methodical, deliberate, and persistent.

27) **E-mail Harassment:** Email harassment is usually understood to be a form of stalking in which one or more people send consistent, unwanted, and often threatening electronic messages to someone else

28) **Firewall** A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

**29) Access control:** Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to modify data or resources. Access control is to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources

30) **Information** is organized or classified data, which has some meaningful values for the receiver.

Information is the processed data on which knowledge, decisions and actions are based.

31) **Confidentiality:** The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

OR

The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

32) **IDS: Intrusion Detection System (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network**

**or system for malicious activities or policy violations.**

33) **Accountability** The principle of accountability specifies that every individual who works with an information system should have specific

responsibilities for information assurance.The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person
who has managerial responsibility for information assurance. One **example** would be a policy statement that all employees must avoid installing outside software on a company-owned information infrastructure.
OR
The security goal that generates the requirement for actions of an entity
to be traced uniquely to that entity