:(Intro to ICT):-

Semestor 01:-

:Information Security & Privacy:-

Information Security and privacy deals with study of tools and techniques to protect and hide a computer system information from being intentional or unathorized access is known as Information Security.

:Security Threads:-

Security threads may be a computer program, a person or an event that violates or break the security system.

→ A thread may cause the loss of data or stolen secret information.

Types of Threads:-

(i) Intentional Threads:-

Intentional Threads means "planned", an unathorized user may delete sensitive data intentionaly. Intentional threats refer to the purposeful actions resulting in theft or damage of computer resources and data.

(ii) Unintentional Threats:-

Unintentional Threats are considered to be human error, environmental hazards and computer failures.

Unintentional means "Bymistake or Bychance", an unathorized user may delete sensitive data.

The data may be corruped due to:

(i) ~~Technical~~ Sudden break of electricity

(ii) Technical failure of hardware

(iii) Due to Virus Attack.

Solutions for Information Threats:-

(i) **User Right:-**

Only authorized user may access data with certain rights.

(ii) **Backup of data:-**

Take back of data on regular basis which helps to restore data if it lost.

(iii) **Password Protection:-**

A password is set to access the resources or information of computer.

Mon Tue Wed Thu Fri Sat

Date: __/__/20__

(iv) **Encryption:-**

By using symmetric and Asymmetric algorithm encrupt plain information text into unread form. It is used in network security to secure sensitive information.

(v) **Data Scanning:-**

For secure our informations or data we must should be used antivirus software to protect and remove virus and other kinds of harm software.

Name :- Hamza Ali
Class :- BSIT 1st Semester
Roll No :- IT-G1-143
Assignment :- Into to ICT

Topic:-
"Computer Viruses and their Types."

Computer Viruses:-

A computer virus is a type of harmful software, or malware that infects computer and corrupts their data and software. Virus is also a programs that are develop for damage the computer components and other sensitive information resources. Many viruses pretend to be legitimate programs to trick users into executing them on their devices.

:- Types of Viruses :-

There are nine main virus types, some of which could be packaged with other malware to increase the chance of infection and damage. The nine major categories for viruses on computer are:

1. Boot Sector Virus

The computer drive has a sector solely responsible for pointing to the operating system so that it can boot into the interface. A boot sector virus damages or controls the boot sector on the drive.

Attackers usually use Harmful USB devices to spread this computer virus.

The virus is activated when users plug in the USB drive

and boot their machine.

2. Web Scripting Virus

Most Browsers have defenses against malicious web scripts, but unsupported browsers have vulnerabilities allowing attackers to run code on the local device.

3. Browser Hijacker

A computer virus that can change the settings on your browser will hijack browser favorites, the home page, URL and search preferences.

The site could be a phishing site or an adware page used to steal data or make money for the attacker.

4. Resident Virus.

A virus that can access computer memory and sit dormant until a payload is delivered is considered a resident virus.

This melware may stay dormant until a specific date or time or when a user performs an action.

5. Direct Action Virus

When a user executes a seemingly harmless file attached to malicious code, direct-action viruses delivers a ~~plaqto~~ payload immediately. These computer viruses can also remain dormant until a specific action is taken or a timeframe passes.

6. Polymorphic Virus

Melware authors can use polymorphic code to change the program's footprint to avoid detection. Therefore, its more difficult for an antivirus to detect and remove them.

7. File Infector Virus

To persits on a system, a threat actor uses files infector viruses to inject malicious code into critical files that run the operating system or important programs. The computer virus is activated when the system boots or the programs run.

8. Multipartite Virus

These malicious programs spread across a network or other systems by copying themselves or injecting code into critical computer resources.

9. Macro Virus

Microsoft Offices files can run macros that can be used to download additional malware or run malicious code. Macro viruses deliver a payload, when the file is opened and the

macro runs.

10. Network Virus:

Network Viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network.

11. Trojan Horse

A Trojan Horse is a type of program that pretends to be something it is not to get onto a device and infect it with melware.

A Trojan Horse virus is a virus disguised to look like something it is not. For Example,

DATE: _____ DAY: _____

viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies.

12. Worm

A computer worm is not a virus. Worms do not needs a host system and it can spread between systems and network without users actions, whereas a virus requires users to execute its code.

-:(Intro to ICT):-

Semester 01:-

Information Security by using Cryptography Techniques:-

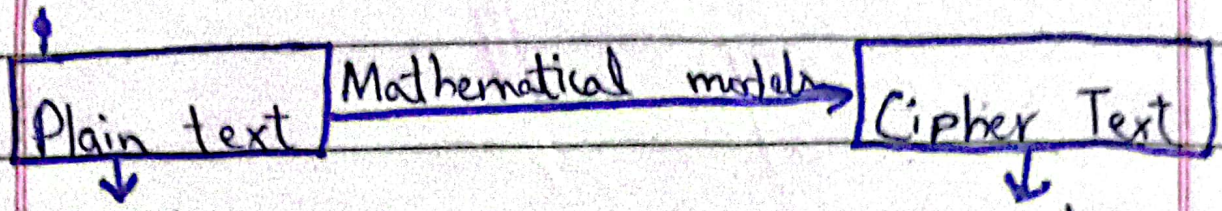
Cryptography ensures the integrity of data using hashing algorithms and message digests. By providing codes and digital keys to ensure that what is recieved is genuine and from the sender.

Encryption:-

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative from known as Ciphertext.

In this process, the useful information is converted into

meaningless information by using mathematical models for securing the original information over the internet.



Decryption:-

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

In this process, the encrypted data is converted into original form.

-: Cryptography :-

Cryptography is the practise and study of techniques for secure communication in the presence of adversarial behavior. Cryptography is the subfield of network security which deals with the study of Encryption and decryption Algorithm or techniques for securing information over the internet.

-. Types of Cryptography :-

There are three types of Cryptography.

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Public Key Cryptography

(i) **Symmetric Cryptography:-**

It is an encryption system where the sender and reciever of message use a single common Key to encrypt and decrypt messages.
Symmetric Key System are faster and ~~reciever~~ simpler but the problem is that sender and reciever have to somehow exchange Key in a secure manner.
The most popular symmetric Key cryptography system are:

- Data Encryption System (DES)
- Advanced Encryption System (AES)

(ii) **Asymmetric Cryptography:-**

Under this action (system) a pair of Keys is used to encrypt and decrypt information.
A reciever's public Key is used

for decryption - Public Key and private Key are different. Even if the public key is known by everyone the intended reciever can only decode it because he alone know his private key.

The most popular asymmetric key cryptography algorithm is RSA algorithm.