Name → Ekta Nirania
Enroll.no → 08286319301
Subject → Cyber Security - 503

Ques 3
(i)
Ans) Computer virus.

(i) A living thing, too small to be seen without a special instrument (microscope), that causes disease in people, animal and plants.

(ii) Instruction that are put into a computer program in order to stop it working properly and destroy information.

In more technical term, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

A virus operates by inserting or attaching itself to a legitimate program or document that supports macos in order to execute its code.

(ii)

Phase) **Password Cracking:-** In cryptanalysis and computer security, password cracking is the process of recovering passwords from data has been stored in or transmitted by a computer system in scrambled form.

A common approach (brute force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password.

The purpose of password cracking might be to help a user recover a forgotten password to gain unauthorized access to a system, or to act as a preventive measure whereby system administrators check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence to which a judge has allowed access, when a particular file's permissions are restricted.

(i) Time needed for password searches
(ii) Easy to remember, hard to guess
(iii) Incidents
(iv) Prevention
(v) Software
(vi) See also
(vii) References
(viii) External links.

Que 12

Ans 2) IT act 2000 →

The Information Technology Act 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filling of documents with the Government agencies and further to amend The Indian Penal Code, The Indian Evidence Act, 1872, The Bankers Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention thereunder committed outside India by any person.

* Salient Features of IT Act 2000 :-

(i) Digital signature has been replaced with electronic signature to make it a more technology neutral act.

(ii) It elaborates on offense penalties, and branches.

(iii) It outlines the justice Dispensation Systems for Cyber crimes.

(iv) It provides for the constitution of the Cyber Regulations Advisory Committee.

(v) The Information Technology Act is based on the Indian Penal code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act 1934, etc.

Ques 5

Ans 5) **Digital Signature →**

Digital signatures can provide data integrity, authentication, and support for nonrepudiation. After a message has been signed, it can not be modified without being detected. A valid digital signature can only be created by the original singer (i.e, can not be forged) and they can prove also who signed the message.

A Digital signature is a mathematical scheme for verifying the authenticity of digital authenticity stamps. digital signatures can provide added assurances of the evidence to provenance.

This article considers a new electronic signature technique called 'Aadhaar e-KYC service' Legal admissibility of digital evidence in India.

Ques 6
Ans 2

Key logger :-

Keyloggers are type of monitoring software designed to record keystrokes made by a user.

One of the oldest forms of Cyber threat, these keystroke loggers record the information you type into a website or application and send it back to a third party.

Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees.

Law enforcement and intelligence agencies also uses keylogging for surveillance purpose.

The first keyloggers were used by the Soviet Union in the 1970s to monitor IBM electric typewriters used at embassies based in Moscow.

Que 7

Ans 7) Different types of Phishing Attacks :-

(i) Email Phishing. Most Phishing attacks are sent by email.

(ii) Spear Phishing. There are two other, more sophisticated, types of Phishing involving email.

(iii) Whaling. Whaling attacks are even more targeted, taking aim at senior executives.

(iv) Smishing and Vishing.

(v) Angler Phishing.

The goal here is to help familiarize you with many of the different types of phishing attacks that exist and provide