Unique Paper Code : 62347627

Name of the paper : Information Security and Cyber Laws

Name of the Course : B A Programme

Semester : VI

Duration : 3 hours

Maximum Marks : 75

Year of Admission : 2015, 2016, 2017 and 2018

Attempt any four questions.

All questions carry equal marks.

Complete answer to a question should be uploaded in the form of a single PDF file.

1.

- What is meant by the term Computer Security.
- Describe the CIA triangle in respect of information security.
- Differentiate between DoS and DdoS attacks.
- *'Data is often the most valuable asset of an organization', comment.*

2.

- What are social engineering attacks? Enumerate three types of social engineering attacks. Describe any one of them in detail.
- Suppose a credit card company sends you a message: "Do not share your OTP with anyone. Our representatives will never call you to verify it." What kind of attack is being prevented by the credit card company by such messages? Mention two strategies employed by attackers to initiate such attacks, giving a suitable example of each.
- A website has a hidden code that gets downloaded on the computer of the user who visits that website. This code then monitors all the activities that take place on that computer. What type of attack is being executed here? Describe one way of preventing such attacks.

3.

- What is meant by the terms: macro virus and memory resident virus. Bring out the difference between a worm and a virus by describing how they operate.
- An internet email user received an email with an attachment named "Happy2021". When the user clicked on it, a video with a message "Happy 2021" was played. While this was happening a code got downloaded on the user's computer and it attached the same code to all the mails that the user sent. What type of software attack was it? Give another scenario/ way by which a system may be infected with the above attack.
- What are virus hoaxes? How did the virus hoax ***Goodtimes*** impact the information systems?

4.

- Differentiate between Law and Ethics.
- Enumerate five criteria that must be met for a policy to become enforceable.
- What is meant by the terms: *identity theft* and *cross-site scripting?*
- Suppose a person fraudulently/ dishonestly makes use of the digital signature and /or password of another person. Which section of IT Act will be applicable in such a case. What are the penalties and punishment under the said section of the IT Act?

5.

- What is a firewall?
- How do the following types of firewall enforce address restrictions:
  - static filtering?
  - dynamic filtering?
  - stateful packet inspection (SPI)?
- What do you understand by the term risk identification? Draw a diagram that illustrates the various components of risk identification.
- Enumerate four functions of access control systems. Briefly describe each of them.

6.

- Give block diagrams that illustrate the working of each of the following:
  - symmetric encryption
  - asymmetric encryption
- The following ciphertext was encrypted using a *Caesar cipher* with a shift of 4: **`M pszi csy`**. Decrypt this message to obtain the corresponding plain text. Show the steps in the decryption process.
- The ciphertext was obtained using the *Rail Fence cipher* with key 3: **`RFEHALECCPEINIR`**. Decrypt this message to obtain the corresponding plain text. Show the steps in the decryption process.
- Differentiate between Section 67 and Section 67A of the IT Act 2008.
- Given the plaintexts **`COMPUTER`**, generate their corresponding ciphertexts using Vigenère cipher using the keyword **`DELHI`**.