Reg. No. : | | | | | | | | | | | | |

Question Paper Code: 1046107

B.E. / B.Tech. DEGREE EXAMINATIONS, NOV / DEC 2024
Sixth Semester
Computer Science and Engineering
U20CS602 – CRYPTOGRAPHY AND NETWORK SECURITY
(Regulation 2020)

Time: Three Hours Maximum: 100 Marks

Answer ALL questions

PART – A (10 x 2 = 20 Marks)

1. What is the best phishing?

2. One of your friends has recently been a victim of a social engineering attack since someone has stolen her username and password for accessing her work email. This name, 'social engineering' looks quite strange to you as it puts together engineering with social issues. What does social engineering mean in a security context?

3. What is meant by cryptography and cryptanalysis?

4. Differentiate between a mono-alphabet cipher and a polyalphabetic cipher.

5. What is collision resistant attack or birthday paradox?

6. What is a trap-door one-way function?

7. What are the properties a digital signature should have?

8. Differentiate MAC and Hash function?

9. List the design goals of firewalls?

10. What is mean by SET? What are the features of SET?

PART – B (5 x 16 = 80 Marks)

11. (a) i) Illustrate OSI security architecture. Why it has considered as primary security parameters for IT and Information security system? Justify your answer with a real time scenario.

ii) Which technique is used to masquerade a person, program or an address as another by falsifying the data with purpose of unauthorized? Also, using Online purchasing system scenario, describe how DNS cache, Search Engine, and ARP poisoning techniques are differ from each other?

(8+8)

(OR)

(b) Consider yourself as running Techno ware software development industry, in that you have been facing repeated virus attacks while managing confidential data. As an authorized person, how will you identify the type of virus attack? Also, describe different types of virus that usually affect your sensitive data. (16)

12. (a) Consider the scenario,
The input plain text hello world, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as: holewdlo lr. Now, the receiver has to use the same table to decrypt the cipher text to plain text.
Implement the suitable Pseudo code for the above scenario.

(16)

(OR)

(b) What is Cryptanalysis? With suitable example, explain how does it is differ from substitution cipher method? (16)

13. (a) Employees working from home, remote workers around the world or in country offices as well as customers, suppliers and partners. All of them need to access specific data, documents and information on the company network quickly, conveniently and securely. As a security analyst, which Asymmetric key cipher technique will you recommend to secure remote access of data? (16)

(OR)

(b) i) What is a prime's primality test in mathematics of asymmetric key cryptography? Explain with real time example. (6)

ii) If P is prime and 'a' is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$, for this context, elaborate Fermat's theorem that play important roles in public-key cryptography. (10)

14. (a) A hash function maps a variable-length message into a fixed length hash value, or message digest. For message authentication, a secure hash function must be combined in some fashion with a secret key. In the context of communications across a network,
    i) List down different authentication requirements that help to identify the attacks. (8)
    ii) Give a brief about different authentication functions for the same context. (8)

(OR)

(b) Give a brief about following two hash algorithms with suitable example: (16)
- Secure Hash Algorithm
- Message Digest MD5

15. (a) The security administrator notices that the router is generating a lot of false positives for signatures 1000, 3154 and 8000. The system administrator knows that there is an application on the network that is causing signature 1000 to fire, and it is not an application that should cause security concerns.
    i) Explain the commands to disable the signatures initially and re initialize the firewall IDS
    ii) Show the verification of configuration for the above scenario

(10+6)

(OR)

(b) Assume a Denial Of Service attack has been targeted on the organization. As a security analyst, discuss in detail any five types of DoS that can flood the traffic of the target victim with necessary illustrations. (16)

---------xxx--------