04/01/2023- FN

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

Question Paper Code : 90426

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2022.

Sixth/Seventh Semester

Computer Science and Engineering

CS 8792 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to: Computer and Communication Engineering / Electronics and Communication Engineering / Electronics and telecommunication engineering/ Information technology)

(Regulation 2017)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the key principles of security?
2. Distinguish active and passive attack with example.
3. If a bit error occurs in plain text block b1, how far does the error propagate in CBC mode of DES?
4. Find gcd (56, 86) using Euclid's algorithm.
5. User X and Y exchange the key using Diffie-Hellmann algorithm. Assume a=5 q= 11 XA=2 XB=3, Find the value of YA, YB and k.
6. What mathematical problem is behind security of the ElGamal cryptosystem?
7. Name the four requirements defined by Kerberos.
8. Differentiate MAC and Hash function.
9. Why E-mail compatibility function in PGP required?
10. Define virus. Specify the types of viruses.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Explain the network security model and its important parameters with a neat block diagram. (8)

(ii) Compare Substitution and Transposition techniques with examples. (5)

Or

(b) Outline any four types of cryptanalysis attack and explain with neat sketches. How this attack is made possible? (13)

12. (a) Explain in detail on the design principles of block cipher and the modes of operation. (13)

Or

(b) Discuss properties that are satisfied by Groups, Rings and Fields. (13)

13. (a) Users A and B use the Diffie Hellmann key exchange technique, a common prime q=11 and a primitive root alpha=7.

(i) If user A has private key XA=3.What is A's public key YA? (4)

(ii) If user B has private key XB=6. What is B's public key YB? (4)

(iii) What is the shared secret key? Write the Algorithm (5)

Or

(b) Identify the possible threats for RSA algorithm and list their counter measures. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5. (13)

14. (a) Many websites require users to register before they can access information or services. Suppose that you register at such a website, but when you return later you've forgotten your password. The website then asks you to enter your email address which you do. Later, you receive your original password via email. Discuss several security concerns with this approach to deal with forgotten passwords. (13)

Or

(b) What is a digital signature? Explain the key generation, signing and signature verification algorithm. Bring out the steps followed to create a digital signature. (13)

15. (a) (i) With a neat sketch explain the IPsec scenario and IPsec Services. (8)

(ii) What is a worm? Name any four known worms. (2)

(iii) What are the different types of viruses? How do they get into the systems? (3)

Or

(b) How does PGP provides confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. (13)

PART C — (1 × 15 = 15 marks)

16. (a) "Attacks are the techniques that attackers use to exploit the vulnerabilities in applications. Attacks are often confused with vulnerabilities, so please try to be sure that the attack you are describing is something that an attacker would do, rather than a weakness in an application". (8)

Consider any domain of your choice (Example Web Application IoT, Operating System etc.) List down any eight attacks in the chosen domain and mention the root cause of the attack. (7)

Or

(b) Consider a simple LAN consisting of a number of clients, a server, a mail server and Internet access. A firewall is designed to divide this LAN into three isolated segments namely internet segment server segment and clients segment. We are writing the rules to allow only the required service to be accessed from one segment to other.

Our firewall is now configured to allow only http requests to the web server and no access at all from outside to our internal LAN.

(i) Does this mean that the web server is secure?

(ii) Is the rest of the internal LAN secure?

Justify your answer and suggest ideas how to ensure security to the given scenario.

———————