VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of the UGC Act, 1956)

Reg. No. :

Final Assessment Test (FAT) - May 2024

Programme	B.Tech.	Semester	WINTER SEMESTER 2023 - 24
Course Title	CRYPTOGRAPHY AND NETWORK SECURITY	Course Code	BCSE309L
Faculty Name	Prof. N G Bhuvaneswari Amma	Slot	F2+TF2
		Class Nbr	CH2023240501468
Time	3 Hours	Max. Marks	100

General Instructions:

- Write only Register Number in the Question Paper where space is provided (right-side at the top) & do not write any other details.

Answer all questions (10 X 10 Marks = 100 Marks)

01. In a secret code-breaking game, Ms.Reeta sends Ms.Reena a message encrypted with modular arithmetic using the Chinese Remainder Theorem (CRT). Ms.Reena must decipher the message to reveal the hidden clue. [10]

Ms.Reeta sends the following three clues to Ms.Reena:

Clue 1: $x \equiv 17 \pmod{23}$

Clue 2: $x \equiv 32 \pmod{41}$

Clue 3: $x \equiv 56 \pmod{67}$

Find the positive integer solution for x

02. i. Compare and contrast the strengths and weaknesses of IDEA encryption algorithm with those of other widely used encryption algorithms such as AES and DES. (4 marks) [10]

ii. Assume you are tasked with implementing the RC4 encryption algorithm for a project. Your team needs a clear understanding of the steps involved in the RC4 algorithm to ensure proper implementation and integration. Discuss the steps involved in RC4 to provide a comprehensive guide for your team. (6 marks)

03. Ms.Dusty, a researcher, needs to send a brief encrypted message to her colleague Mr.Mark, containing the results of a recent experiment. They have decided to use RSA encryption to protect the confidentiality of their findings. Ms.Dusty wants to send the message "SUCCESS" to Mr.Mark. Given Mr.Mark's public key, which consists of a modulus n=143 and an encryption exponent e=7, Ms.Dusty needs to encrypt the message using RSA encryption.[Note: Value of 'A'-0,'B'-1,…] [10]

i. Compute Ms.Mark's private key. (3 marks)

ii. Encrypt each character of the message "SUCCESS" to provide the service of confidentiality. (7 marks)

04. A security engineer employs elliptic curve cryptography (ECC) to ensure secure communication between users. He selects an elliptic curve E with equation $y^2=x^3+5x+7$ over finite field $\mathbb{F}17$. He also chooses a base point G=(13,5) on the curve and private key as 3. [10]

i) The given curve generates 22 points. Does the point (11,4) exists on the given curve? (4 marks)

ii) Compute the public key of the security engineer. (6 marks)

05. Assume Ms.Sahana is signing up to gmail with a new password. It passes through MD5 and generates hash that stored on the server. When Ms.Sahana tries to login again, she has to enter the password. It passes the entered password through the hash function again to generate a digest. If the computed digest matches the one on the server, the login is verified. Show this entire scenario with detailed steps of MD5. [10]

06. Ms.Alice wants to sign and send a message to Mr.Bob using the ElGamal Digital Signature Algorithm. They have agreed upon the prime number p = 17 and primitive root g=7. [10]

i. Ms.Alice chooses the private key as a = 12 and a random number k = 11 to sign the message m = 13. Determine her public key and the signature. (5 marks)

ii. Show how Mr.Bob is going to verify the received signature. (4 marks)

iii.Can Ms.Alice choose the random number k = 10 instead of k = 11? Justify (1 mark)

07. Mr.Alex is communicating with a bank's computer system. He needs to deal with issues like how long his login stays valid and to ensure the bank server is authentic and secure. How does he handle this using Kerberos authentication service? [10]

08. Mr.Rusty is the lead developer for an e-commerce platform that handles millions of transactions daily. His task is to ensure that all communications between clients and servers are secure, particularly sensitive data such as credit card information. In light of recent security breaches in similar platforms, discuss how he would architect the implementation of Secure Socket Layer (SSL) to safeguard data transmission considering factors such as certificate management, protocol versions and cipher suites. [10]

09. You are a cybersecurity consultant working with a financial institution that handles sensitive client information. The institution is concerned about the security of their email communications, especially when exchanging confidential financial documents and customer data with clients and partners. They are considering the implementation of Pretty Good Privacy (PGP) to enhance the security of their email communication. Discuss the varied services provided by PGP for secure email communication. [10]

10. i. An employee installs malicious software on their work computer, trying to bypass the company's security measures. How can a rule-based intrusion detection system detect and prevent the spread of this malware within the network? (7 marks) [10]

ii. In a large financial institution, there's a growing concern about insider threats that could compromise sensitive financial data or lead to fraudulent activities. Suggest and discuss a proactive solution to detect and mitigate insider threats before they escalate into major security incidents. (3 marks)