Department of Computer Science and Engineering, S V N I T, Surat
END-SEMESTER EXAMINATIONS, April 2024
B. Tech. – III (CSE) – 6th Semester
Course: (CS302) Information Security and Cryptography

Date: 15th April, 2024 **Time: 9:[redacted] am to 12:[redacted] pm** **Max Marks: 50**

Q.1(A) Use the given phrase to create a key matrix for 6x6 Playfair cipher. [5]
"IPL 2024 TURNOVER AT 13897 CR STARQ PAID 25 CR BUT MAX WICKETS BY YUZI CHAHAL"
Encrypt the following text using this Playfair cipher:
18 BALL 52 BY SKY YESS MI

Q.1(B) Answer any Two : [5]
1. Discuss/Compare security offered by Running key Vignere cipher and One Time Pad.
2. Discuss security of Polygram v/s Polyalphabetic cipher (also give examples).
3. Discuss Jeferson Cylinder (Wheel Cipher) and electro-mechanical rotor machines.

Q.2(A) List DES and AES parameters (size of key/block etc.) and compare their design features. [5]

Q.2(B) Answer any Two : [5]
1. Discuss side channel attacks with mitigation directives.
2. Discuss steganography – classical and modern techniques.
3. Discuss Stuxnet and Regin attacks.

Q.3 Answer any Four: [20]

1. In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17},
(a) What are the negatives of the following points?
P(5,8) Q(3,0) R(0,6)
(b) What is 2P if P = (1, 3)?
(c) Do the points P(2,0) and Q(6,3) lie on the elliptic curve ?

2. Alice uses Bob's RSA public key (e=17, n=19519) to send a four-character message to Bob using the (A↔0, B↔1,... Z↔25) encoding scheme and encrypting each character separately. Eve intercepts the ciphertext (6625 0 2968 17863) and decrypts the message without factoring the modulus. Find the plaintext and explain why Eve could easily break the ciphertext.

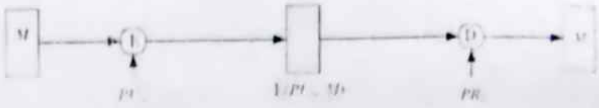
3. (a) Explain following properties for cryptographic hash function:
1. Pre-image resistance
2. Second pre-image resistance
3. Collision resistance
(b) Explain the use of hash function for maintaining one-way password file.

4. (a) Differentiate Entity authentication and Data-origin authentication. Give one example technique for each category.
(b) Explain the dictionary attack on password-based authentication. How it can be prevented using salt-based password authentication?

5. Consider the following uses of Encryption shown in figure 1, 2, 3 and 4; where PU_x : public key of x, PR_x : private key of x, E : Encryption function, D: Decryption function, M: Message. Fill up the table with Yes/No for each of the services provided:

	Confidentiality	Authentication	Digital Signature
Figure 1	✓	✗	✗
Figure 2	✓	✗	✗
Figure 3	✗	✓	✗
Figure 4	✓	✓	✓

(Figure 1)



(Figure 2)

(Figure 3)

(Figure 4)

Q.4 Answer any Five: [10]

1. Explain Existential Forgery and Selective Forgery for Digital Signature.
2. What are the advantages of applying digital signature on the hash of the message instead of the message itself ?
3. Which of the following is/are valid Galois field?
   (a) GF(12) (b) GF(13) (c) GF(16) (d) GF(17)
4. Differentiate HMAC and CMAC.
5. The Random Oracle can be thought of as choosing a random output y on being queried with a value x and remembering its choice. Explain the Random Oracle model and how it relates to the cryptography hash functions.
6. Explain Elliptic Curve based Discrete Logarithm Problem (ECDLP)? List two cryptographic algorithms whose security is based on hardness of ECDLP.

****

Question to Course Outcome (CO) Mapping (in form of H (High), M (Medium), L (Low) :

	CO1 (Understand)	CO2 (Apply)	CO3 (Analyze)	CO4 (Evaluate)	CO5 (Create)
Q-1	H	H	H	H	-
Q-2	H	-	-	H	-
Q-3	H	H	H	M	M
Q-4	H	H	-	-	-