COLLEGE OF ENGINEERING, PUNE

(An Autonomous Institute of Government of Maharashtra.)

END SEM - EXAM

Cryptography and Network Security

Program: **B.Tech. (Computer Engineering/Information Technology)**
Year: 2022-23 Semester: VII
Duration: 3 hr. Max. Marks: 60

Student MIS No.:

1	1	1	9	0	3	0	1	9

Instructions:

1. **Mobile phones and programmable calculators are strictly prohibited.**
2. **Writing anything on question paper is not allowed.**
3. **Exchange/Sharing of stationery, calculator etc. not allowed.**
4. **Write your MIS Number on Question Paper.**
5. **Make appropriate assumptions wherever necessary.**
6. **Give examples and draw neat diagrams wherever necessary.**

			COs	POs
Q.1.	A.	Fill in the blanks and **Re-write** the complete sentence with correct answer:	(5) CO-1, CO-3, CO-4, CO-5	a, b, h

1. The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext the scheme is known as _____.

   a) Confusion b) Diffusion

   c) Error Propagation d) Avalanche Effect

2. The problem with Diffie-Hellman Key Agreement Protocol is _____

   a. too short keys

   b. lack of security

   c. failure to agree on the key

   d. Man in the middle attack

3. If we want to ensure the principle of _____, the contents of a message must not change while in transit.
   a. Confidentiality
   b. Authentication
   c. Integrity
   d. Non–repudiation
4. Calculate the value of φ (437). It is _____
   a. 293
   b. 396
   c. 369
   d. 236
5. In DES-3, we can use ___ or ____ keys.
   a. 1 or 2
   b. 3 or more
   c. 1 or more
   d. 2 or 3

B. Use Hill cipherand decrypt the following message. **(5)**

Message: "ZSHLFGLKTVDUWAQBCG"

Encryption key: "CDPFIMBNE".

Q.2. A. List various ways of distribution of public keys. Explain each scenario by taking appropriate parameters. **(5)** CO-4, CO-5 c, d, e, h

B. Calculate the digital signature using following data: **(5)**

Global public key values are 29 and 9, h =7,

Users Private key = 5 and K =7, $K^{-1} = 5$,

Find the public key and the digital signature for the message whose message digests is 53.

OR

B. Draw a neat architecture diagram of Kerberos. List down the various steps involved during the authentication of users with respect to Kerberos, use proper conventions for the same.

Q.3. A. Explain the zero point (point at infinity) of an elliptic curve? **(5)** **CO-2, CO-4** **a, d, g**

i) Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over F_{17}?

ii) In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, What is 2P if P = (1, 3)?

iii) In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, What is P+Q if P = (2, 0) and Q = (1, 3)?

B. Answer the following: **(5)**

a) Using Fermat's little theorem find 13^{2010} mod71

b) Find the multiplicative inverse of 27 (mod 392)

c) Find the primitive root in modulo 13

d) Solve $9x \equiv 1 \pmod 7$

e) Find all solutions for $232x + 42 \equiv 248 \pmod{50}$

Q.4. A. Create the scenario for each of the following attacks and propose solution/s: **(5)** **CO-1, CO-5, CO-6** **a, e, f, h**

i) Man-in-middle attack ii) meet-in-the-middle attack

iii) Sniffing iv) Denial of Service attack

v) Repudiation of origin

B. List the popular filename extensions for X.509 certificates. Describe the X.509 Standard used in PKI. Explain its structure (various fields). **(5)**

Q.5. **A.** Perform AES mix column transformation for following and show your calculations **(5)** **CO-2, CO-3,** **a, b, d,**

	02	03	01	01		63
Rcon=	01	02	03	01	State column =	2F
	01	01	02	03		AF
	03	01	01	02		A2

B. Find the integer x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively. Using Chinese Remainder Theorem (CRT). **(5)**

Q.6. **A.** Two users A & B wish to use Diffie-Hellman algorithm. They are agreed about following parameters: n = 191 and g = 2. User A selects 42 as his private key. Also, user B selects 33 as his private key. **(5)** **CO-4, CO-6** **a, b, e**

a) What is the public key of user A?

b) What is the public key of user B?

c) What is the shared session key for their communication?

B. Compare and contrast between Intrusion Detection System and Firewall. List and explain types of firewall. **(5)**