Roll No. | | | | | | | | | | |

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)

B.E. /B. Tech / B. Arch (Full Time) - END SEMESTER EXAMINATIONS, APR / MAY 2024

COMPUTER SCIENCE AND ENGINEERING

Semester - VI

CSM506 CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2019)

Time: 3 hrs

Max. Marks: 100

CO1	Discuss various exploitations present in the security.
CO2	Illustrate the basic concepts of encryption and decryption for secure data transmission.
CO3	Develop solutions for security problems
CO4	Analyze various cryptography techniques and their applications
CO5	Learn the various network security techniques and their characteristics.

BL – Bloom's Taxonomy Levels

(L1-Remembering, L2-Understanding, L3-Applying, L4-Analysing, L5-Evaluating, L6-Creating)

PART- A (10x2=20Marks)

(Answer all Questions)

Q. No.	Questions	Marks	CO	BL
1	Define Security.	2	1	1
2	State Fermat's theorem and using it find Find 128^{129} mod 17.	2	1	2
3	Find f(x) * g(x) (mod m(x)) over GF(2), given, $f(x) = X^2+X+1$, $g(x) = X^7+X+1$ and $m(x) = X^8+X^4+X^3+X+1$.	2	2	3
4	Differentiate DES Vs AES	2	2	2
5	Name two user application software that has/uses Digital Signatures	2	3	2
6	Draw a diagram to show authentication in public key cryptography	2	3	2
7	What are the requirements for cryptographic hash?	2	4	2
8	What is preimage in hashing?	2	4	2
9	How VPNs provide an added layer of defense against cyber threats?	2	5	2
10	Write 4 attacks targeted on web security.	2	5	2

PART- B (5x 13=65Marks)

(Restrict to a maximum of 2 subdivisions)

Q. No.	Questions	Marks	CO	BL
11 (a)	i) Write the Fast Exponentiation Algorithm ii)Find the Inverse of 550 in GF(1759)	8 5	1	3
	OR			
11 (b)	Bobby has a certain number of pencils in his backpack. If Bobby were to pull out pencils in groups of 4, he would eventually end up with 1 pencil in his backpack. Similarly, if Bobby were to pull out pencils in groups of 5, he would end up with 2 pencils left in his backpack. Finally, we know that if Bobby pulls out pencils in groups of 7, he would end up with up 4 pencils left. How many pencils does Bobby have in his backpack?	13	1	3
12 (a)	i) Draw and explain AES in detail. ii) Describe how substitution, transposition, confusion and diffusion constitute to a good encryption algorithm? Explain how it is applicable to AES.	8 5	2	4
	OR			

12 (b)	Draw and explain S-DES and If the input Plain text to the S-DES is 00101001 and the key used is 1100011100 find the Cipher text. (Show the Algorithm steps clearly) $s0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}; s1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$ P10: 3 5 2 7 4 10 1 9 8 6; P8: 6 3 7 4 8 5 10 9; IP: 2 6 3 1 4 8 5 7; IP^{-1}: 4 1 3 5 7 2 8 6; E/P: 4 1 2 3 2 3 4 1; P4: 2 4 3 1;	13	2	4
13 (a)	Write the Diffie Hellman key exchange algorithm and explain the working of it to share key between Alice and Bob. Provide numerical example for the same.	13	3	4
	OR			
13 (b)	Brian uses an RSA system with public keys n (the modulus) and e1 (public exponent) with a matching private key d1. Brian creates RSA keys for his friend Meg using the same public key n, but a different public exponent e2 and matching private exponent d2. While Brian was being careless, you discover the values of d1 and d2. Though you do not wish to read message intended for Brian or Meg, you do wish to read messages directed towards Sarah, who also uses the public modulus n with the public exponent e3. Outline a strategy that may help uncover Sarah's private exponent, d3.	13	3	5
14 (a)	Explain the following concepts related to hash function: i)one-way property, ii) weak collision free, iii) strong collision free, iv) birthday attack. Understand the implication of birthday attack. v) Explain how block chaining techniques can be used to build hash function and why it is insufficient.	8(2+2 +2+2) 5	4	3
	OR			
14 (b)	Explain the working of Kerberos V5 in detail with neat representation of all the dialogues involved.	13	4	3
15 (a)	i) Draw and explain the traffic flow management by Firewalls ii) Draw and explain the IP Security Architecture	8 5	5	4
	OR			
15 (b)	i) Explain SSL in detail. What protocols comprise SSL? ii) Explain how VPN operates in detail	8 5	5	3

PART- C (1x 15=15Marks)

(Q.No.16 is compulsory)

Q. No.	Questions	Marks	CO	BL
16.	i) Identify and explain the type of attack Priya could pose on the following Public Key Protocol from the given flow diagram. ii)How could this attack be rectified? Explain the algorithm.	10 5	5	6