

Roll. No.

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)
B.E. Full Time - END SEMESTER EXAMINATIONS, DEC 2024

ELECTRONICS AND COMMUNICATION ENGINEERING
EC5072 & CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation2019)

Time:3hrs

Max.Marks: 100

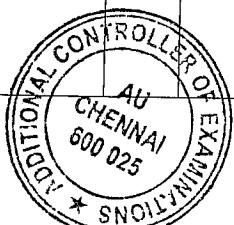
PART- A(10x2=20Marks)

(Answer all Questions)

Q.No	Questions	Marks	CO	BL
1	Suppose "C" is the cipher text in Affine cipher then what is the plain text? Assume Multiplicative Key $K_1=5$ and Additive key $K_2=7$.	2	1	2
2	Determine the solution to the following linear equation: $5x + 6 \equiv 24 \pmod{37}$.	2	1	2
3	What is Avalanche Effect in cryptography?	2	2	2
4	Enumerate the advantages and disadvantages of Electronic Code Book (ECB) mode.	2	2	2
5	State Euler's theorem. Using Euler's theorem, determine $12^{-1} \pmod{77}$.	2	3	2
6	Find out if 3 is a QRs in \mathbb{Z}_{23}^* . Solve the following quadratic equation: $x^2 \equiv 3 \pmod{23}$.	2	3	2
7	What is the number of padding bits required if the length of the original message is 2967 bits in Whirlpool?	2	4	2
8	In SHA 512, the E, F, G buffers are processed using conditional function and majority function. If E is 22_{16} , F is 88_{16} , and G is 55_{16} , what is the result of conditional function?	2	4	2
9	What is digital certificate and digital envelop? Highlight its applications.	2	5	2
10	What is S-MIME? Highlight its merits over PGP protocol.	2	5	2

PART- B(5x 13=65Marks)

Q.No	Questions	Marks	CO	BL
11 (a)	Encrypt the message "authentication" using Playfair cipher with the key "good" and transposition cipher with the key $K=[3 \ 2 \ 4 \ 1]$.	6	1	3
(ii)	Determine the multiplicative inverse of $(x^4+1) \bmod (x^8 + x^4 + x^3 + x + 1)$.	7	1	4
OR				
11 (b)	Explain the following security services: Nonrepudiation, Authentication and Availability.	6	1	3
(ii)	Encrypt the message "DIVIDE" using the Hill cipher with the key $\begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$. Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext.	7	1	4
12 (a)	With neat block diagram, explain the AES key expansion algorithm.	6	2	3
(i)				
(ii)	Explain the key stream generation and encryption algorithm for RC4	7	2	3
OR				
12 (b)	Illustrate and explain the following modes of operation: CBC, CFB and OFB.	13	2	3
13 (a)	Explain how Miller-Rabin algorithm is used to determine the primality.	6	3	4
(i)	Prove that the given number 73 is prime using Miller-Rabin algorithm.			
(ii)	State and explain Chinese Remainder Theorem(CRT). Determine the value of X for the following set of congruence using the CRT: $X \equiv 4 \pmod{13}$, $X \equiv 2 \pmod{17}$ and $X \equiv 7 \pmod{19}$.	7	3	4
OR				
13 (b)	Encrypt the plain text $M = 20$ with prime numbers $p = 7$ and $q = 19$ using RSA algorithm with public key $e = 25$. Also perform the decryption and determine the original plain text.	5	3	4
(i)				
(ii)	Encrypt the plain text $M = 20$ with prime numbers $p = 7$ and $q = 19$ using Rabin algorithm. Also perform the decryption and determine the original plain text.	8	3	4



14 (a)	With neat block diagram explain the compression function and structure of each round in SHA 512.	13	4	3
--------	--	----	---	---

OR

14 (b) (i)	Explain the key generation, signing and verification of Digital Signature Standard (DSS).	8	4	3
(ii)	Explain the Diffie-Hellman key exchange technique. Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 37$ and a primitive root $a = 5$. If user A has private key $X_A = 11$ and user B has private key $X_B = 16$, determine the A's public key Y_A , B's public key Y_B and shared secret key.	5	4	4
15 (a)	Explain the functions of SSL record and SSL Handshake protocols.	13	5	3

OR

15 (b)	Explain the process of the Authentication Header and Encapsulating Security Payload Protocols of IP Security.	13	5	3
--------	---	----	---	---

PART- C(1x 15=15Marks)

(Q.No.16 is compulsory)

Q.No	Questions	Marks	CO	BL
16.	(i) Consider Advanced Encryption Standard with $GF(2^8)$ and Determine the substitution byte value for given byte '94'. (ii) Encrypt the plain text $M = 10$ using ElGamal algorithm with the following parameters: Prime $p = 17$, primitive root $e_1 = 5$, private key $d = 7$ and random number $r = 3$. Also perform the decryption and determine the original plain text.	8 7	2 3	5 5

