National Institute of Technology Mizoram

Mid – Semester Examination, Even Semester – (2022-2023)

Network Security and Cryptography (CSL 1802)

B.Tech. 8th Semester **Full Marks: 30 marks** **Duration: 1 hour 30 mins**

Answer all 3 (Three) Questions. All Questions carry same Marks

(3 * 10 = 30 Marks)

27/30

Question 1

(a) What are the basic assumptions of Kerckhoff's Principle? [2]

(b) What are the different kinds of Ciphertext-Only attack? [2]

(c) Explain why modern block ciphers are designed as substitution ciphers instead of transposition ciphers. [2]

(d) Differentiate between diffusion and confusion. [2]

(e) Differentiate between differential and linear cryptanalysis. [2]

Question 2

(a) Compute the modular inverse of the follow matrix in Z_{10} [5]

$$\begin{bmatrix} 6 & 5 & 7 \\ -3 & 2 & -5 \\ 4 & 6 & 9 \end{bmatrix}$$

(b) In each of the following ciphers, what is the maximum number of characters that will be changed in the ciphertext if only one character is changed in plaintext and why? [1+1]

a. Single transposition
b. Double transposition

(c) Eve secretly gets access to Alice's computer and using her cipher types "abcdefghij". The screen shows "CABDEHFGIJ". If Eve knows that Alice is using a 'keyed transposition cipher', answer the following questions: [1+2]

a. What type of attack is Eve launching?
b. What is the size (or possible sizes) of the permutation key?

Question 3

(a) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key. [2]

(b) For the group G = $<Z_6^*, \times>$: (note: operator '×' here is multiplication) [1+1+1]

a. Is G an abelian group?
b. Show the result of 5×1 and $1 \div 5$.
c. Show that why we should not worry about division by zero in this group

(c) A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks. [2]

(d) The input/output relation in a 2 × 2 S-box is shown by the following table. Show the table for the inverse S-box. [2]

Input: left bit	Input: right bit 0	Input: right bit 1
0	01	11
1	10	00

(e) Determine whether the P-box with the following permutation table is a straight P-box, a compression P-box, or an expansion P-box. [1]

1	1	2	3	4	4

National Institute of Technology Mizoram

End – Semester Examination, Even Semester – (2022-2023)

Network Security and Cryptography (CSL 1802)

B.Tech. 8th Semester **Full Marks: 50 marks** **Duration: 2:30 hours**

Answer all 5 (Five) Questions. All Questions carry same Marks
(5 * 10 = 50 Marks)

Question 1

(a) Differentiate between RSA digital signature scheme and RSA cryptosystem. [2]

(b) Determine the following: $\phi(231)$, $\phi(440)$ [3]

(c) Determine the following: $5^{15} \bmod 13$, $15^{18} \bmod 17$ (use the appropriate theorem) [3]

(d) Determine x:

$x \equiv 7 \bmod 13$, and $x \equiv 11 \bmod 12$ [2]

Question 2

(a) What is the one-way function in (a) RSA cryptosystem, (b) ElGamal cryptosystem [2]

(b) What is the trapdoor in (a) RSA cryptosystem, (b) ElGamal cryptosystem [2]

(c) In RSA:

i. Given n = 221 and e (public key) = 5, find d (private key). [2]

ii. Given n = 3937 and e (public key) =17, find d (private key). [2]

(d) In PGP, explain how Bob and Alice exchange the secret key for encrypting messages. [2]

Question 3

(a) Briefly explain Diffie-Hellman key exchange. [3]

(b) Users A and B use the Diffie-Hellman key exchange technique with a common prime p = 71 and a primitive root (generator) g = 7. [3]

i. If user A has private key $X_A = 5$, what is A's public key Y_A?

ii. If user B has private key $X_B = 12$, what is B's public key Y_B?

iii. What is the shared secret key?

(c) Differentiate between Modification detection code (MDC) and Message authentication code (MAC). [2]

(d) Explain why private-public keys cannot be used in creating a MAC. [2]

$12^{-1} \bmod 156$

$13^{-1} \bmod 156$

Question 4

(a) Define:

i. cryptographic hash function [1]

ii. iterated cryptographic hash function [1]

(b) What is the padding for SHA-512 if the length of the message is:

i. 5120 bits [1]

ii. 5121 bits [1]

(c) Write a routine/function (in pseudocode) for the [6]

i. Conditional function in SHA-512. Assume that words x, y, z are represented as arrays of 64 elements.

ii. Majority function in SHA-512. Assume that words x, y, z are represented as arrays of 64 elements.

Question 5

(a) In the RSA scheme (digital signature), find the relationship between the size of S and the size of n. Also, in the DSS scheme, find the size of S1 and S2 in relation to the size of p and q. (Note: In RSA, S – signature and n – modulus. In DSS, S1 and S2 are signatures, p and q are moduli) [2]

(b) Show an example of the vulnerability of RSA to selective forgery when the values of p and q are small. Use p = 19 and q = 3 for example. [2]

(c) Write the two algorithms (pseudocode) for the RSA scheme (digital signature): one for the signing process and one for the verifying process. Clearly specify the inputs and the return values of the algorithms. [4]

(d) Define a session key. Show how a KDC can create a session key between Alice and Bob. [2]

$\phi(70$

$7^{20} \bmod 21$