ADMISSION NUMBER

School of Computing Science and Engineering

B.SC CS with specialization in Cyber Security
Mid Term Examination - Nov 2023

Duration : 90 Minutes
Max Marks : 50

Sem III - E1UL301B - Cryptography and Network Security

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1) List and briefly define categories of security services K2 (2)

2) What are the design parameters of Feistel cipher network K1 (3)

3) A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C: C = E([a, b], p) = (ap + b) mod 26 A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p not equal to q, then E(k, p) not equal to E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3. a. Are there any limitations on the value of b? Explain why or why not. b. Determine which values of a are not allowed. c. Provide a general statement of which values of a are and are not allowed. Justify your statement. K2 (4)

4) Suppose you are to encrypt the text “The examnation is over”. You and the receiver are agreed on the common secret key “EXAM”. Find the encrypted message and aslo decryt the message into original using the Hill Cipher. K2 (6)

5) Write a program that can encrypt and decrypt using the general Caesar cipher, also known as an additive cipher. K3 (6)

6) Use the Vigenere ciher with the keyword ABCD to decrypt the ciphertext CSASTPKVSIQUTGQUCSASTPIUAQJB K3 (9)

7) Can you suggest a security improvement to either One-loop CBC or Three-loop CBC option, using only three DES chips and some number of XOR functions? Assume you are still limited to two keys. Explain your answer. K4 (8)

8) Demonstrate encryption and decryption process in hill cipher. Consider m = “sh” and key = hill”. K4 (12)

OR

Encrypt the message "Chineese army is moving towards west, be carefull" using the key "Hill" using Hill cipher. Also recover the original message from the encrypted message. K4 (12)