23 11.30 to 12.30

Bharatiya Vidya Bhavan's

SARDAR PATEL INSTITUTE OF TECHNOLOGY

(Autonomous Institute Affiliated to University of Mumbai)

Munshi Nagar, Andheri (W), Mumbai – 400 058.

MSE

(Sep. 2024)

Max. Marks: 30 | **Duration: 60 Min.**

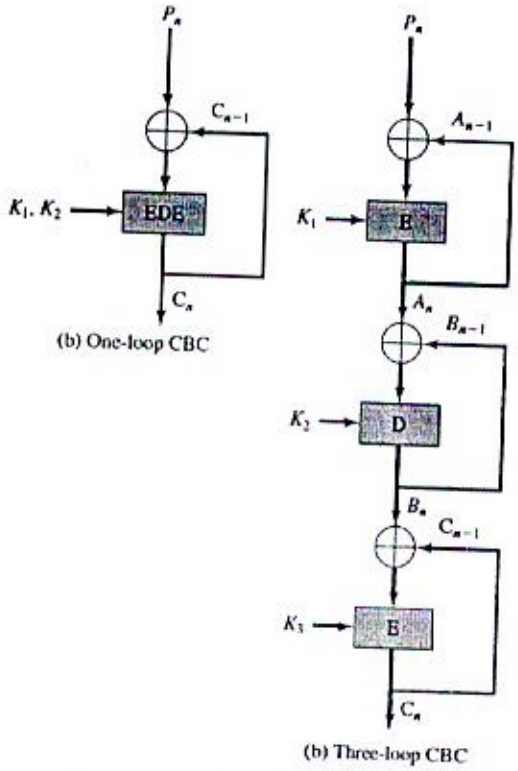
Class: BTech(CE) | **Semester: VII**

Name of the Course: Cryptography and System Security | **Course Code: CS401**

Instruction:

1) **All questions are compulsory.**
2) **Draw neat diagrams.**
3) **Assume suitable data if necessary but justify the same.**

Q. No.	Question	Max. Marks	CO-BL
Q. 1	Exemplify the working principles of any of four cipher/cryptography methods: a) Caesar Cipher b) Monoalphabetic Cipher c) Playfair Cipher d) Hill Cipher e) Polyalphabetic Cipher f) Row-Column Rail-fence Cipher g) Public Key cryptography using RSA h) Diffie–Hellman (DH) Key Distribution Algorithm	8	CO1,2-2
Q. 2	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 $p \neq q$, then $E(k,p) \neq E(k,q)$. 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. d) How many one-to-one affine Caesar ciphers are there?	7	CO1,2-5
Q. 3	In each of the following ciphers, what is the maximum number of characters that will be changed in the ciphertext if only a single character is changed in the plaintext? Justify each of them mathematically in terms of encryption, decryption and keys etc. used in the ciphers. a) Caesar cipher b) Affine cipher c) Vigenere cipher d) One-time pad cipher	8	CO1,2-3

Q. 4	You want to build a hardware device to do block encryption in the ***Cipher Block Chaining (CBC)*** mode using an algorithm stronger than DES. The ***3DES*** is a good candidate. Following figure shows two possibilities [a) One-loop CBC, b)Three-loop CBC], both of which follow from the definition of CBC. Which of the two [a) One-loop CBC, b)Three-loop CBC] would you choose for: i. For security? ii. For performance? Justify your answers for both (i and ii).  (b) One-loop CBC (b) Three-loop CBC Note – Notations in figure are self explanatory e.g. Keys = K_1, K_2, K_3. E=Encryption, D=Decryption, P_n=Plaintext, C_n= Ciphertext, Partial outputs are A_n, B_n etc.	7	CO1,2-5