Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Synoptic- Mid Semester Examination

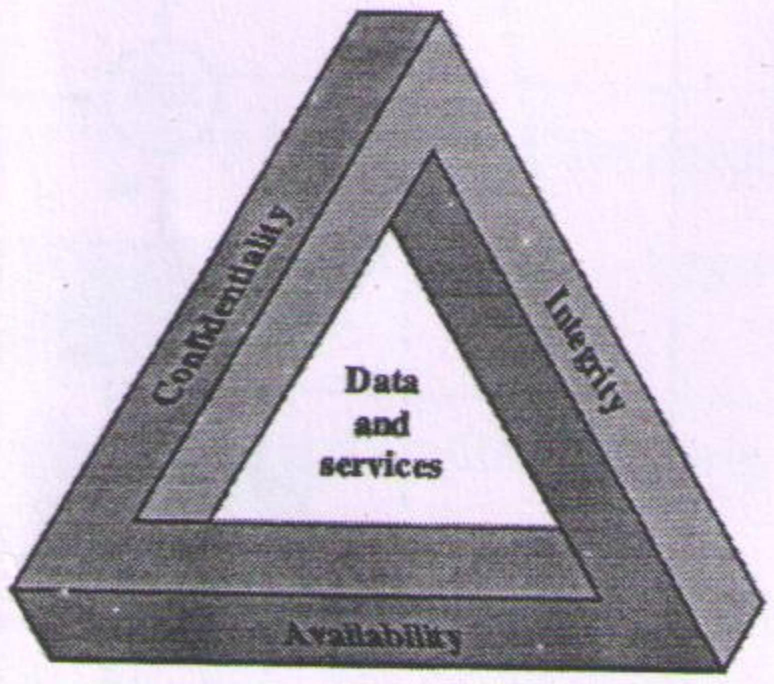
March 2020

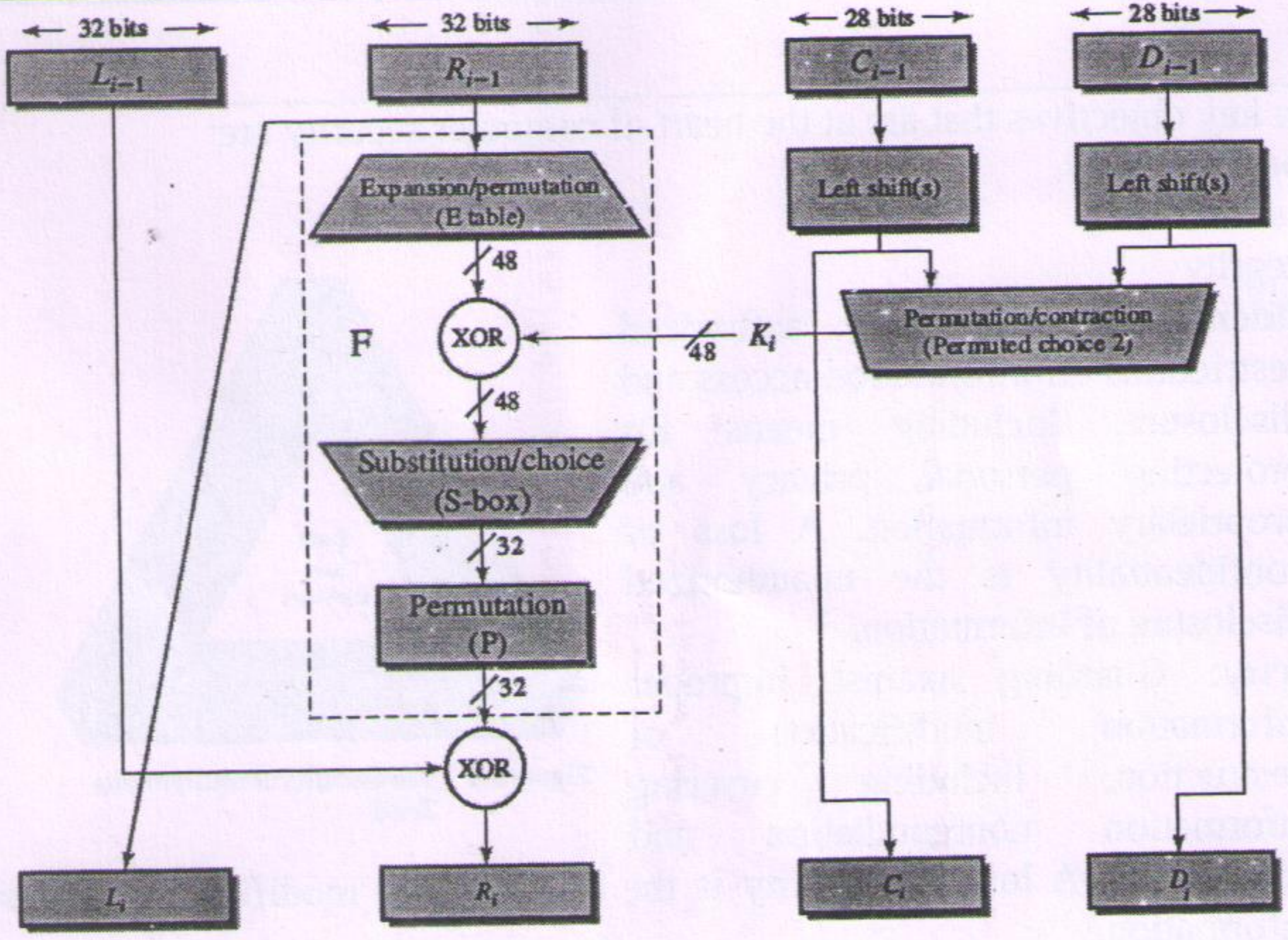
Max. Marks: 20
Class: T.E.
Course Code: CE62
Name of the Course:Cryptography and System Security

Duration: 1 hr
Semester: VI
Branch: Computer

Instructions:

(1) All Questions are Compulsory
(2) Draw neat diagrams
(3) Assume suitable data if necessary

Question No.		**Max. Mks**
Q1	Three key objectives that are at the heart of computer security are: 1. Confidentiality 2. Availability 3. Integrity **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. **Integrity**: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.\\  Confidentiality Integrity Availability Data and services **Figure 1.1 The Security Requirements Triad** **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. **Marks Distribution:** only stated the three key objectives / goals of computer security-------- 01mks Explained all three goals properly with diagram------------------------ 04mks Explained all three goals properly without diagram------------------------ 03mks	**04**
Q2	**The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique:** • Plaintext is encrypted two letters at a time. • If a pair is a repeated letter, insert filler like 'X'.	**05**

	• If both letters fall in the same row, replace each with the letter to its right (circularly). • If both letters fall in the same column, replace each with the the letter below it (circularly). • Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair. **Marks Distribution:** The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique--- **02mks** Problem solved correctly with all steps/calculations shown-------------------- **03 mks**	
Q3	 32 bits 32 bits 28 bits 28 bits L_{i-1} R_{i-1} C_{i-1} D_{i-1} Expansion/permutation (E table) 48 F XOR 48 K_i 48 Substitution/choice (S-box) 32 Permutation (P) 32 XOR Left shift(s) Left shift(s) Permutation/contraction (Permuted choice 2) L_i R_i C_i D_i **Figure 3.6 Single Round of DES Algorithm** **Marks Distribution:** Explained properly Single Round of DES Encryption algorithm with diagram------06 mks Explained properly Single Round of DES Encryption algorithm w/o diagram --03 mks	**06**
Q4	P=17, Q= 11, Phi(n) = 160, e=7 , d= 23 CT=11 [solved correctly with all steps/calculations shown] **OR** Ra= 4 Rb=10 Sa=18 Sb=18	**05**