

1. a) Answer the following questions. (5x3)
- i) Distinguish between a modern and a traditional symmetric-key cipher. (CO3)
 - ii) "A modern block cipher can be designed to act as a substitution cipher or a transposition cipher" – Justify this statement. (PO1, PO2)
 - iii) Define a P-Box and list its three variations. Which variation is invertible?
 - iv) A transpositional block has 10 inputs and 10 outputs. What is the order of the permutation? What is the key size?
 - v) Demonstrate the simplest design of Feistel cipher and show that the plaintext maintains its integrity on both the sender and receiver's end.