

Lab assignment 4:

1. Alice needs to send the message "Enemy attacks tonight" to Bob. They agreed to use keyed transposition cipher with key value: 31452. Implement double transposition cipher over it and generate the ciphertext.
2. Create a key stream with linear feedback shift register with 4 cells in which $b_4 = b_1 \oplus b_0$. Show the value of output for 20 transitions (if the seed is 0001).
3. Write a code to encrypt a message A Midsummer Night's Dream, which is a comedy written by Shakespeare. You have to use key: SWINDON and keyed transposition cipher row-column.
4. Find the result of multiplying $P_1=000100110$ and $P_2=10011110$ with irreducible polynomial 100011010 (nine bits).