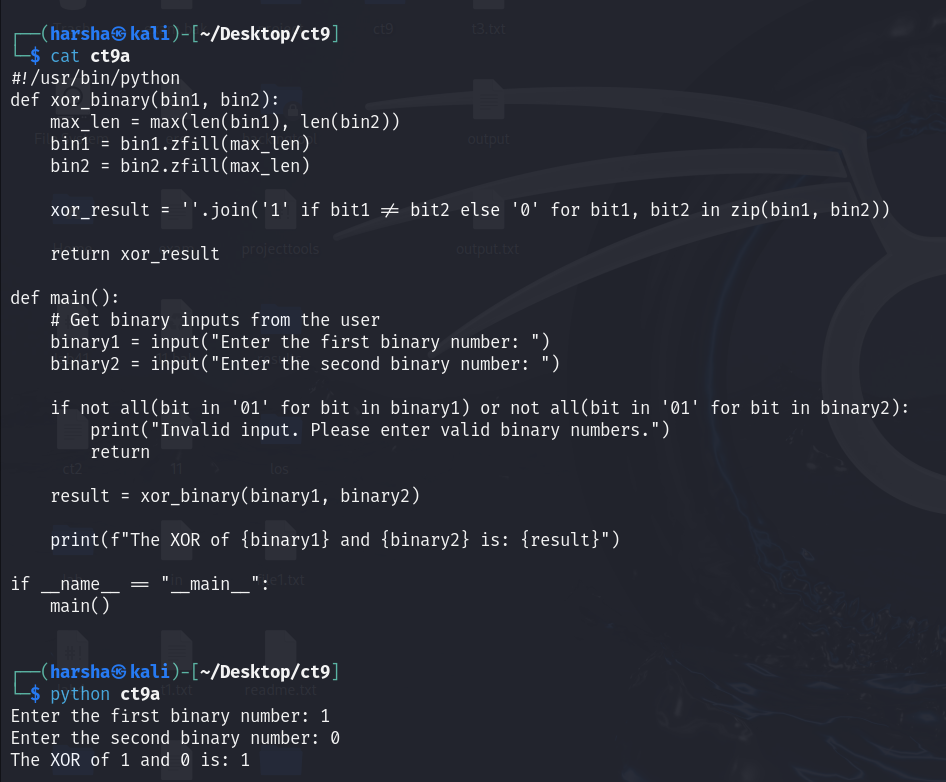
1. Write a python script to get the binary values from the user and perform XOR operation.



1. Write a Python script that implements a simple 4-bit LFSR. The initial state of the register and the tap positions should be user inputs.

Simulate 10 steps of the LFSR, displaying the state of the register at each step.

1. Write a report on attacks on LFSR. Explain any one attack in detail.

**Attacks on LFSRs**

1. **Berlekamp-Massey Algorithm:** This algorithm is used to find the shortest linear feedback shift register (LFSR) that can generate a given sequence of bits. It is efficient and can recover the secret key from a limited number of output bits.
2. **Cryptanalysis by Correlation:** Attackers can analyze the output of an LFSR to find correlations between input and output sequences, potentially leading to key recovery.
3. **Brute Force Attacks:** Although computationally intensive, brute force methods can be employed to try all possible keys until the correct one is found.
4. **Differential Cryptanalysis:** This method analyzes the difference between pairs of plaintexts and how they affect the ciphertext, potentially revealing information about the LFSR's internal state.
5. **Known-Plaintext Attacks:** If an attacker has access to both the plaintext and the corresponding ciphertext, they may be able to derive the state of the LFSR and subsequently its initial conditions.