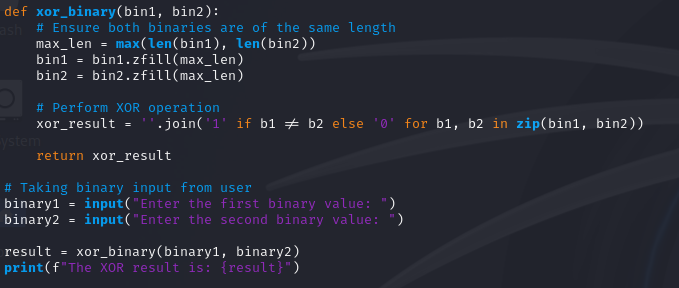
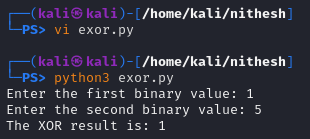
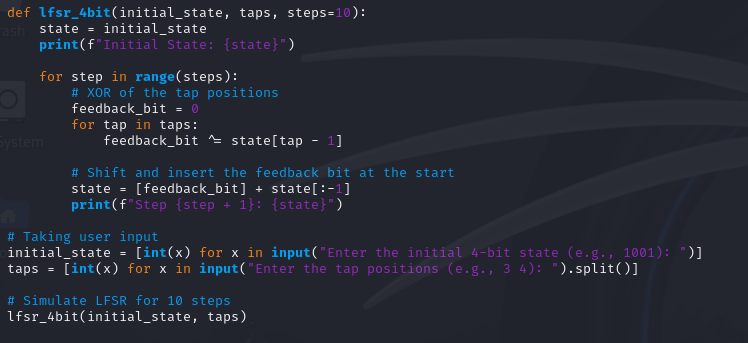
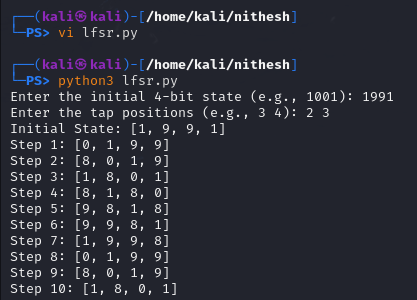
1. Write a python script to get the binary values from the user and perform XOR operation.





2. 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.





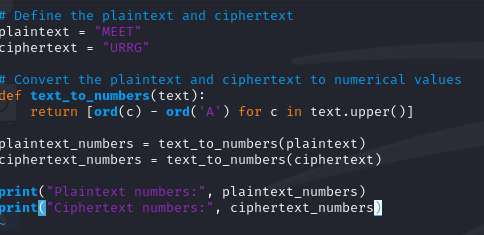
3.Write a report on attacks on LFSR. Explain any one attack in detail.

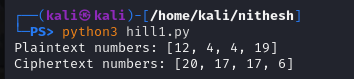
Linear Feedback Shift Registers (LFSRs) are cryptographic primitives often used in stream ciphers. One common attack is the BerlekampMassey Algorithm, which can be used to reconstruct the LFSR from its output sequence.

The Berlekamp-Massey algorithm is used to find the shortest LFSR that generates a given binary sequence. It's efficient and widely used in cryptanalysis of LFSRs. The algorithm iteratively improves an estimated LFSR by minimizing the discrepancy between the LFSR output and the given sequence.

BONUS POINT:

4. write a python script to break hill cipher (2X2) using known plain text attack.





Known Plaintext: "MEET"

Corresponding Ciphertext: "URRG"