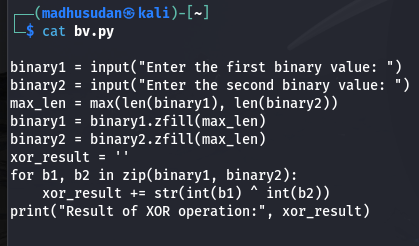
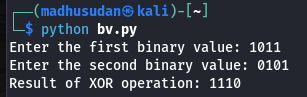
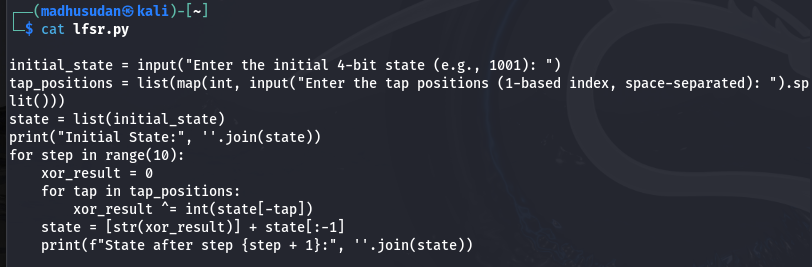
1. **Write a python script to get the binary values from the user and perform XOR operation.**

****

**Output**

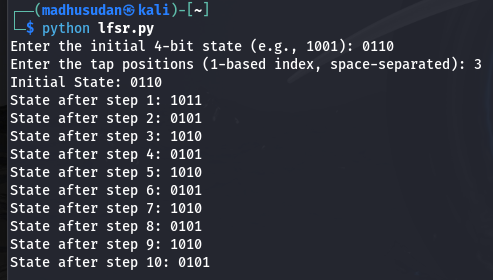
****

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.**

**Output**

****

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

Linear Feedback Shift Registers (LFSRs) are a simple, hardware-efficient way of generating pseudo-random sequences. However, they can be vulnerable to various cryptographic attacks due to their linear structure.

-Berlekamp-Massey Algorithm

**BONUS POINT:**

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

**Known Plaintext: "MEET"**

**Corresponding Ciphertext: "URRG"**

**Output**