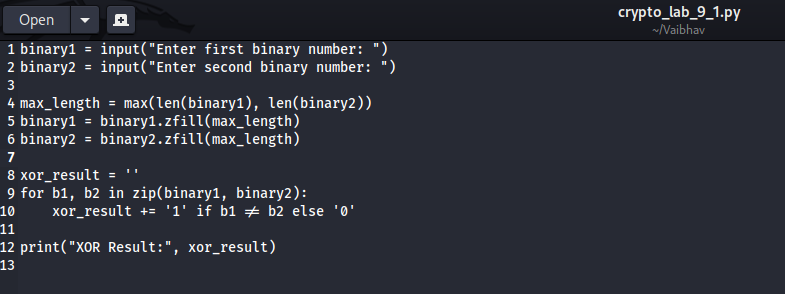
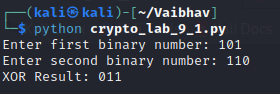
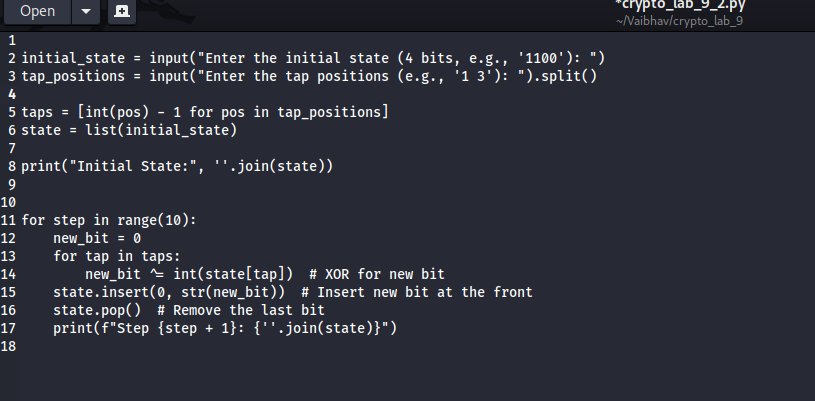
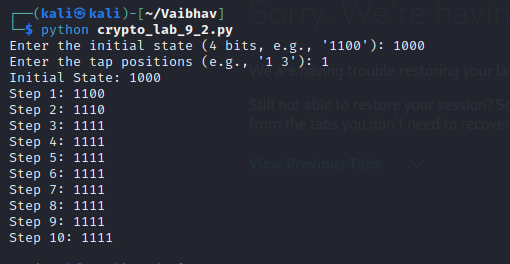
1. Write a python script to get the binary values from the user and perform XOR operation.

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.

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




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

**Title: Attacks on Linear Feedback Shift Registers (LFSRs)**

Linear Feedback Shift Registers (LFSRs) are widely used in cryptography and digital communications for pseudo-random number generation and stream cipher implementations. However, they are susceptible to various attacks due to their linear nature.

**Types of Attacks:**

1. **Berlekamp-Massey Algorithm**: This algorithm efficiently reconstructs the feedback polynomial of the LFSR from observed output bits, allowing the attacker to recover the internal state and predict future outputs.
2. **Known-Plaintext Attack**: In this attack, the attacker uses known plaintext and corresponding ciphertext to determine the LFSR parameters.
3. **Mathematical Attacks**: Given the linear properties of LFSRs, algebraic techniques can be used to find relationships between input and output bits.

**Detailed Explanation of the Berlekamp-Massey Algorithm:**

The Berlekamp-Massey algorithm is a method for finding the shortest LFSR that can produce a given output sequence. It works as follows:

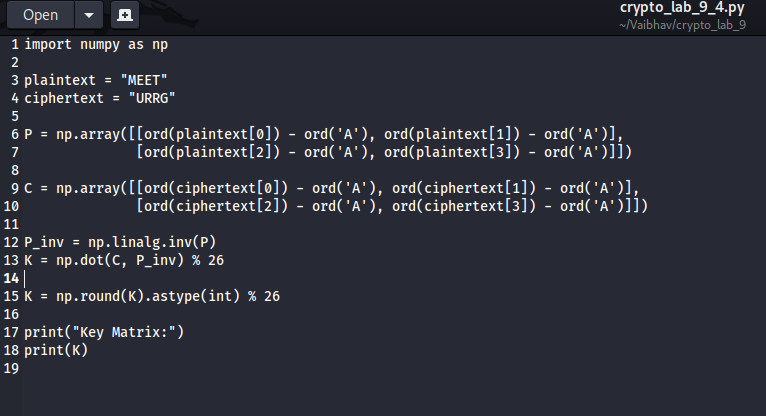
* **Input**: A sequence of bits (e.g., output of the LFSR).
* **Initialization**: Start with an LFSR of length 0 and a polynomial that corresponds to the trivial LFSR.
* **Iteration**: For each bit in the sequence, calculate the discrepancy between the expected output and the actual output. If there is a discrepancy, adjust the current polynomial using previously found polynomials and update the LFSR length.
* **Termination**: After processing all bits, the resulting polynomial represents the feedback taps of the LFSR.

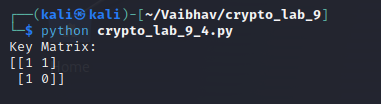
This algorithm is particularly powerful because it requires only a linear number of steps with respect to the length of the sequence, making it feasible even for longer sequences.

BONUS POINT:

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

Known Plaintext: "MEET"

Corresponding Ciphertext: "URRG"  
  




=========================================================================================================================

“Dream, Dream, Dream. Dreams transform into thoughts and thoughts result in action.” - Dr. APJ

=========================================================================================================================