Title: Enigma Machine Encryption
Name: Chengkai Lin
SBU ID: 113499548
Assignment #1: Enigma Machine Project

The Enigma Machine was a cipher device used during World War II to encrypt and decrypt messages. This project involves creating a simulation of the machine's encryption process using bash scripting. The program mimics the functionality of rotors, reflectors, plugboards, and encryption cycles to encode plaintext.

1. Functions:

Initialization(): This function initializes all components of the Enigma Machine, including reflectors, rotors, and the alphabet array.

rotors_set_up(): This function sets up the rotors and their starting positions based on user input.

plugboard_set_up(): Here, the user input for the plugboard connections is processed and stored.

key_clicked(): This simulates the key press, rotating the rotors accordingly before encryption begins.

is_alphabet(): This function check whether the input is a valid alphabet, since Enigma Machine only encrypt 26 alphabet.

find_index(): This function finds the index of a given letter in the alphabet array, necessary for rotor transformations.

first_pass() and **second_pass()**: These functions handle the encryption process as the input signal passes through the rotors, reflector, and back through the rotors.

encrypt(): The main function that combines the operations of the plugboard, rotors, and reflector to encrypt each letter.

enigma_Machine(): This function takes a plaintext input and encrypts it using the configured Enigma Machine.

2. Encryption Process

1. The input character is passed through the plugboard to check for pair substitutions.
2. The rotors rotate, simulating a key press, and the signal passes through each rotor (right to left).
3. The signal is reflected and passes back through the rotors (left to right).
4. The output character is then modified by the plugboard again, completing the encryption cycle.

Encryption Setup:

- Reflector: B
- Rotors: 1, 2, 3
- Starting Positions: A, B, C
- Plugboard: (A, Z), (B, X)

Plaintext: "HELLO"

After encryption, you might get a ciphertext like: **"MTXOI"**.

Then you might use the same configuration setup, to decrypt a ciphertext **"MTXOI"** to **"HELLO".**

3. User Inputs

First prompt (first line input):
Selection of the reflector (A, B, or C) and configuration of the rotors (three rotors left to right and their initial positions).
EX: B123AAA indicates reflector B, and from left to right, using rotor 1, rotor 2, and rotor 3 as rotors configuration, and their initial positions of A, A, A in respective rotor.

Second prompt (second line input):
Plugboard settings (comma-separated character pairs).
EX: AD,BC indicates plugboard between A and D, B and C.

Third promp (third line input)t:
The plaintext that needs to be encrypted.