Intro:

Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present. While today, the cryptographic techniques available relies on complex mathematical concepts like factorization of large numbers, cryptography initially started with more simple concepts like the Vigenère cipher, the Hill cipher…

This project implements 6 classical encryption techniques in one platform:

* Affine Cipher
* Mono-Alphabetic Cipher
* Vigenère Cipher
* Playfair Cipher
* Hill Cipher
* Extended Euclid Algorithm

Implementation:

The WebApp is build using the Flask framework: the front end is implemented with HTML, while the back end is programed using python. The interface is very user friendly: for each cipher you will find a box to input the ciphertext, and a box to input the key. The output of the cypher will show next to the submit button.

Affine Cipher: Given a and b, the code allows the user to encrypt or decrypt a message using the formula C = aP + b.

Mono-Alphabetic Cipher: Given a key consisting of 26 letters, the code allows the user to encrypt or decrypt a message using the key to map the letters.

Vigenère Cipher: Given a key that consists of a word or a sentence, the code allows the user to encrypt or decrypt a message using a Caesar cypher for each letter of the message with each letter of the key.

Playfair Cipher: Given a key that consists of a word or a sentence, the code displays the Playfair Matrix and allows the user to then encrypt the message given.

Hill Cipher: This code supports a matrix size of 2x2 or 3x3 (or more accidentally implemented to support any size of matrix). Given a key, the code displays the Matrix and allows the user to encrypt the message.

Extended Euclid Algorithm: This code finds the inverse of an integer modulo another integer.