Assignment 05

Cryptology – B Keerthana

AMRUTHESH

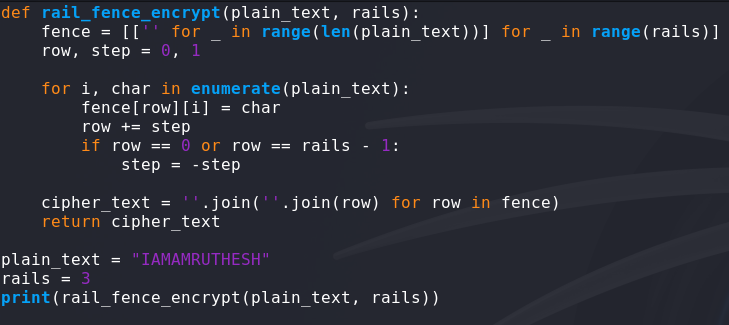
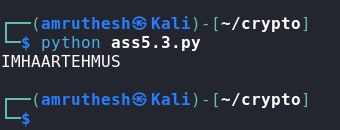
241059041

M.E – Cyber Security

MSIS, MANIPAL

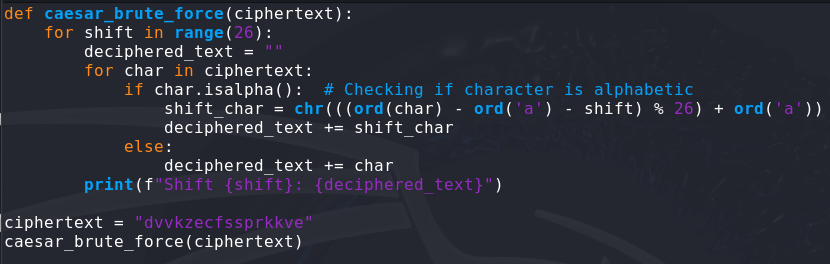
### 1. Encrypt Plain Text Using Rail Fence Cipher

In a Rail Fence cipher with 2 or more rails, the text is written in a zigzag pattern and then read horizontally. Here's an example for encrypting a plaintext using 3 rails.



**2. Brute Force Attack on a Caesar Cipher (Shifting Cipher)**

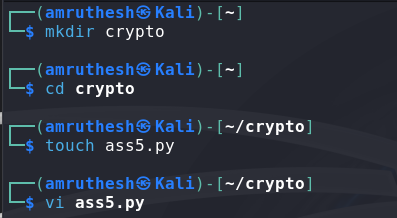
In this task, we'll attempt to decipher the given ciphertext "dvvkzecfssprkkve" by trying all possible shifts (0–25). This will give us each possible plaintext until we find a readable output.



This code will output all possible decrypted texts, helping you to identify the correct shift by finding the one that makes the most sense in English.

We've successfully run a brute-force attack on the Caesar cipher with the output above. You can see that **Shift 17** produces a meaningful plaintext: "meet in lobby at ten".

So, the original message appears to be: **"Meet in lobby at ten"**

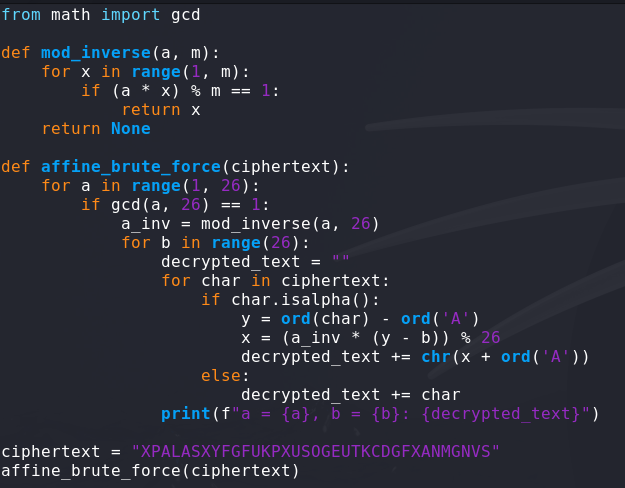


### 3. Brute Force Attack on Affine Cipher

Given that the Affine cipher equation is:  
E(x)=(ax+b)mod  26E(x) = (ax + b) \mod 26E(x)=(ax+b)mod26  
We need to find values of aaa and bbb that make "ab" encrypt to "GL".

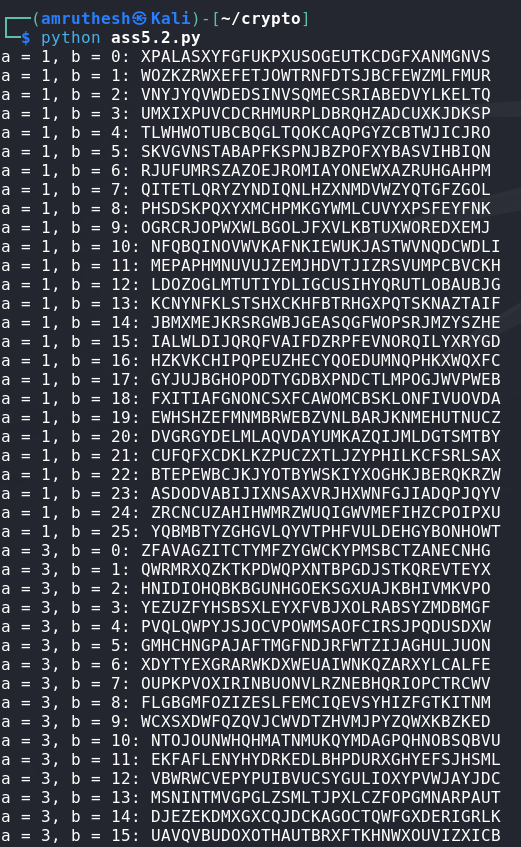
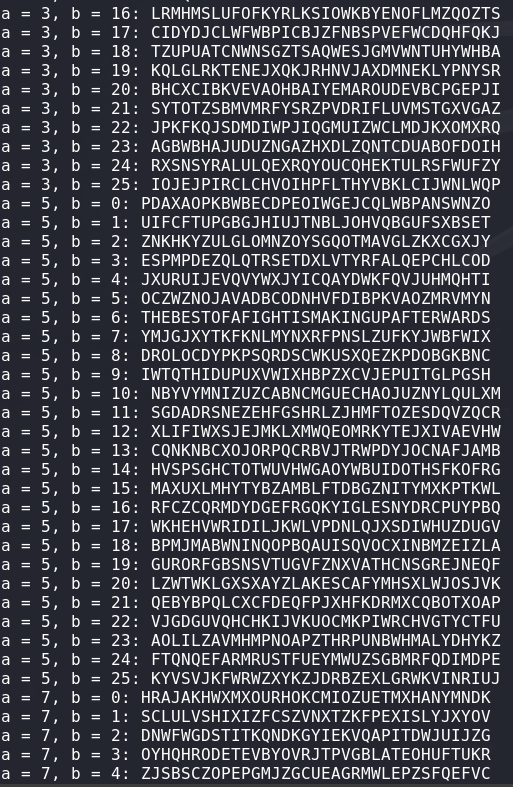
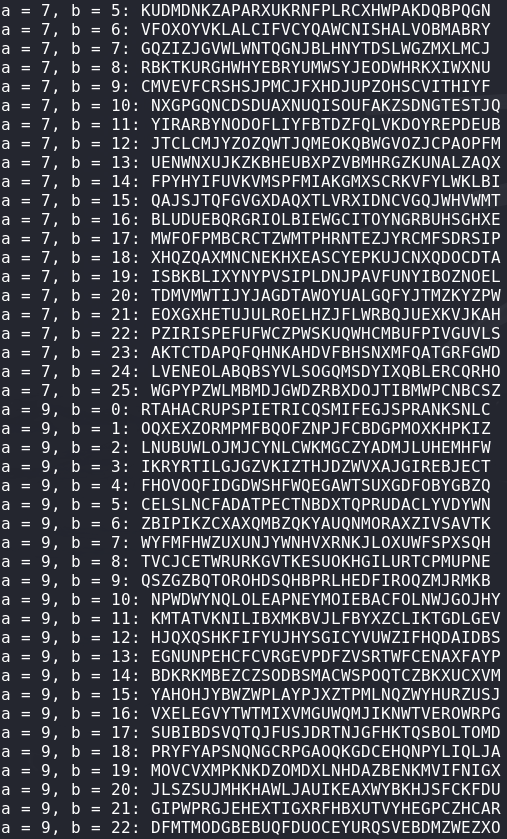
Affine cipher decryption uses the formula: D(y)=a−1×(y−b)mod  26D(y) = a^{-1} \times (y - b) \mod 26D(y)=a−1×(y−b)mod26 Here, a must be coprime with 26 for it to have a modular inverse.

Let's brute-force the Affine cipher keys aaa and bbb:



This code will iterate over all possible values of aaa (coprime with 26) and bbb (0–25) and print each decrypted message.

We successfully generated encrypted text outputs for various affine cipher values of a and b. Each combination yields a different ciphertext, as expected. The interesting part is seeing a = 5 and b = 6 producing the message "THEBESTOFAFIGHTISMAKINGUPAFTERWARDS," which suggests it’s a meaningful plaintext rather than random letters.

The Decryption starts from a = 1 , b = 0 and continues till a = 25 , b = 25

