

Student Name: Naif Almudarra
Student ID: 2536324

Task 1 :

1. Caesar Cipher (Shift = 3)

THERE IS SOMETHING GOOD IN ALL SEEMING FAILURES YOU ARE NOT TO SEE THAT NOW
TIME WILL REVEAL IT BE PATIENT

Method used : the Caesar Cipher shifts each letter by a fixed number. Since the shift is 3, each letter in the ciphertext was moved 3 positions backward in the alphabet to recover the original plaintext

2. Vigenère Cipher (Key = HELLO)

THERE IS SOMETHING GOOD IN ALL SEEMING FAILURES. YOU ARE NOT TO SEE
THAT NOW. TIME WILL REVEAL IT. BE PATIENT.

Method used :For this one, I used the key HELLO. I repeated the key over the ciphertext, then shifted each letter back based on the letter from the key. After decrypting it, I got the same message as the Caesar cipher. The ciphertext seems to be missing the last letter, but the sentence clearly ends with "BE PATIENT."

3. Playfair Cipher (Key = PLAY)

EXACT PHRASING OF THE PLAYFAIR CIPHER TEXT

Method used :For the Playfair cipher, I made the 5 by 5 table using the key PLAY. Then I split the ciphertext into pairs of letters and decrypted each pair using the Playfair rules. After going through all the pairs, the plaintext message was recovered.

Task 2 DES Decryption

Plaintext:

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Method used: For the DES part, I used the key given in the assignment: A1 B1 C1 11 11 11 11 FF

I set the tool to DES, ECB mode, and decrypt. I entered the key and ciphertext in hexadecimal format, then changed the output to text/ASCII. After decrypting, the message above appeared

