Report

Harsh Anand (B18CSE016)

Question 1:
Part a) Find code in zip file

Lets take an example: Here I changed the SHIFT_TABLE to :

```
[1, 1, 2, 2, 2, 2, 1, 2, 1, 2, 2, 2, 2, 1, 2, 2]
```

I encrypted the following message: ABCD1234 with the following key: hello123

Cipher with original DES:
1000001010010001100000111110111000111011001001000100111001111000

Cipher with modified DES:
1000001010100001100000110011101100111000000101001001100011111000

We can similarly change other parameters to modify the cipher more.

Part b)
The primary issue is that DES can be broken using brute-force search. DES is insecure due to the relatively short 56-bit key size.
Despite the vulnerabilities, It is not useless, it is still useful in cases where it doesn't matter if an attacker cracks the code after some time (where the relevance period of the data is small) It is often used in embedded systems, smaller less powerful computers etc.