Assignment 1

COMP 7402

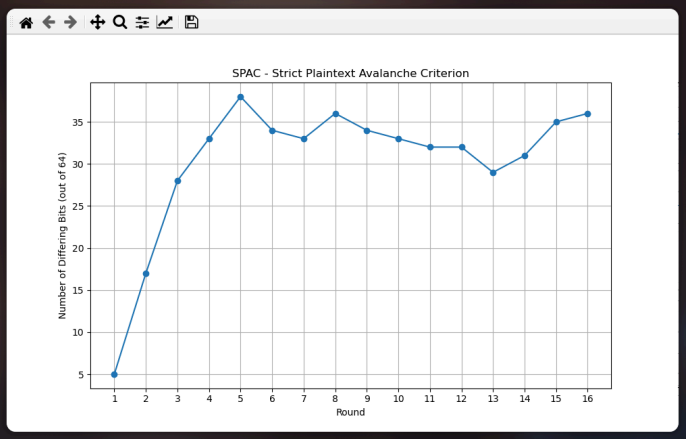
Task 1

```
7402/assign2 on  main [!?] via  v3.13.7 took 20s
❯ python task1.py
Enter the plaintext: 02468aceeca86420
Enter key: 0f1571c947d9e859

Plaintext: 02468aceeca86420
Key: 0f1571c947d9e859

Encrypted: DA02CE3A89ECAC3B
Decrypted: 02468ACEECA86420

7402/assign2 on  main [!?] via  v3.13.7 took 20s
❯
```

Task 2

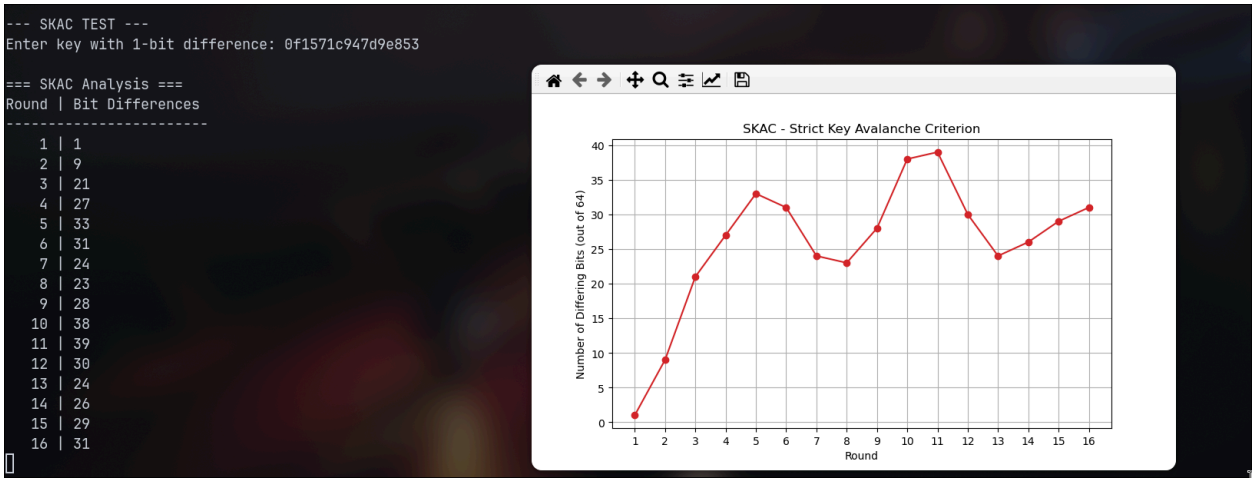
SPAC

```
7402/assign2 on  main [!?] via  v3.13.7
❯ python task2.py
Enter plaintext (16 hex chars): 02468aceeca86420
Enter key (16 hex chars): 0f1571c947d9e859

--- SPAC TEST ---
Enter plaintext with 1-bit difference: 02468aceeca86422

=== SPAC Analysis ===
Round | Bit Differences
------------------------
    1 | 5
    2 | 17
    3 | 28
    4 | 33
    5 | 38
    6 | 34
    7 | 33
    8 | 36
    9 | 34
   10 | 33
   11 | 32
   12 | 32
   13 | 29
   14 | 31
   15 | 35
   16 | 36
```



In SPAC when I changed a single bit in the plaintext in the first 3 rounds the bit differences increased slowly. From round 4 onward the bit differences hover around the 30-38 except on round 13 which drops to 29. The ideal for SPAC is a 50% target which provides good diffusion. In my output by round 4 the bit difference starts to stabilize which leads to good diffusion.

SKAC



In SKAC when I change one bit in the key the rounds 1-3 the values are low which shows bad diffusion. After round 4 the bit difference is around 21-39 which shows the stabilization although not to the point of SPAC. It's still decently good diffusion as the rounds progress.

(For this I output the round and bit differences in the terminal and save it to a CSV. I use matplotlib to create the graphs.)