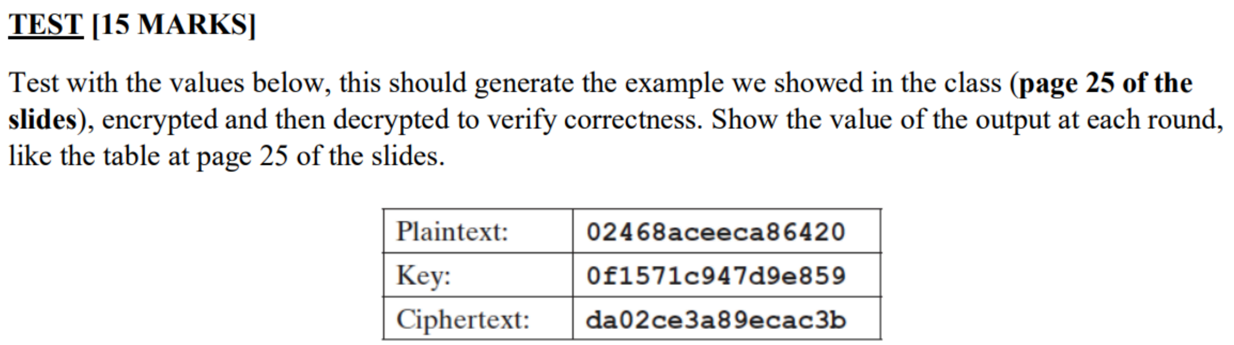
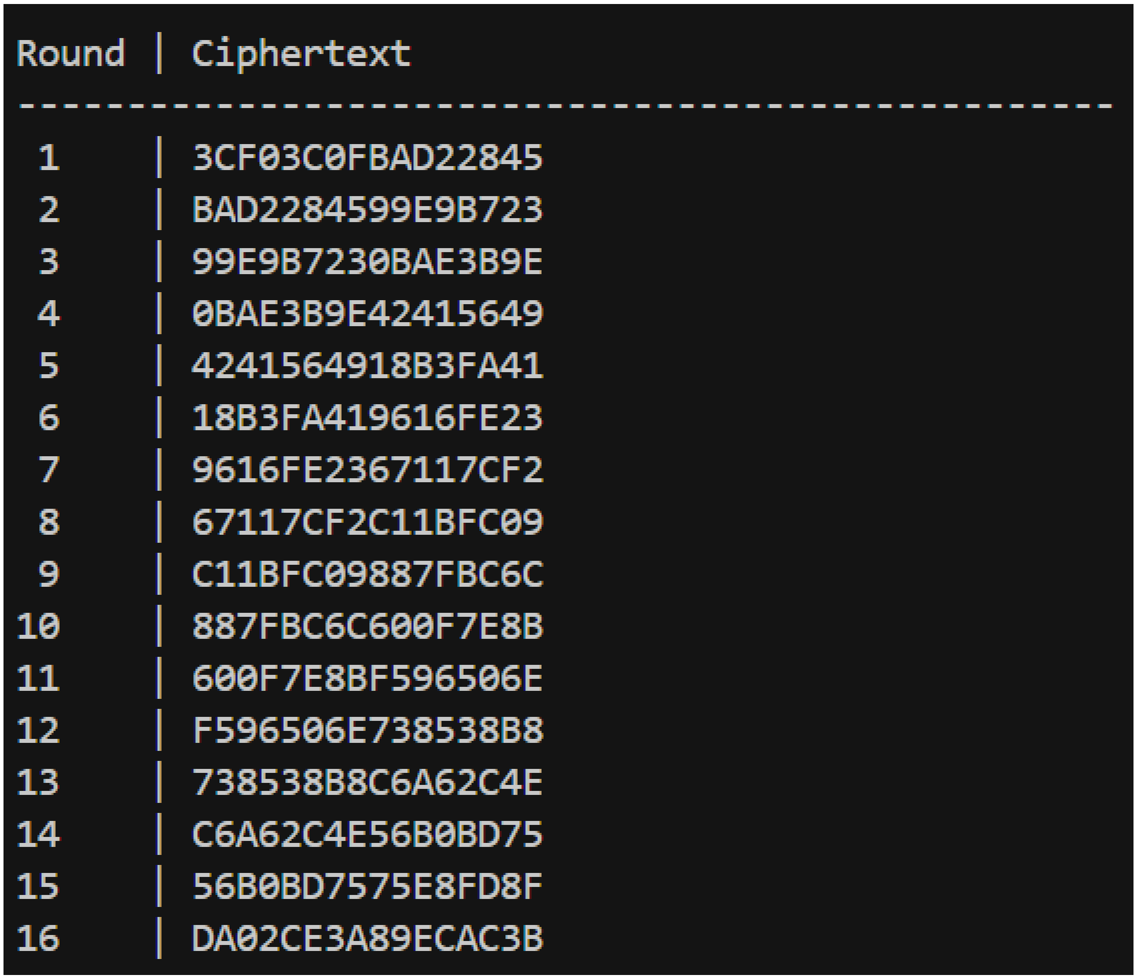
# TASK 1: FEISTEL STRUCTURE CIPHER DESIGN – DES [40 MARKS]



**TEST** **[15 MARKS]**

Test with the values below, this should generate the example we showed in the class (**page 25 of the slides**), encrypted and then decrypted to verify correctness. Show the value of the output at each round, like the table at page 25 of the slides.

| | |
|---|---|
| Plaintext: | 02468aceeca86420 |
| Key: | 0f1571c947d9e859 |
| Ciphertext: | da02ce3a89ecac3b |

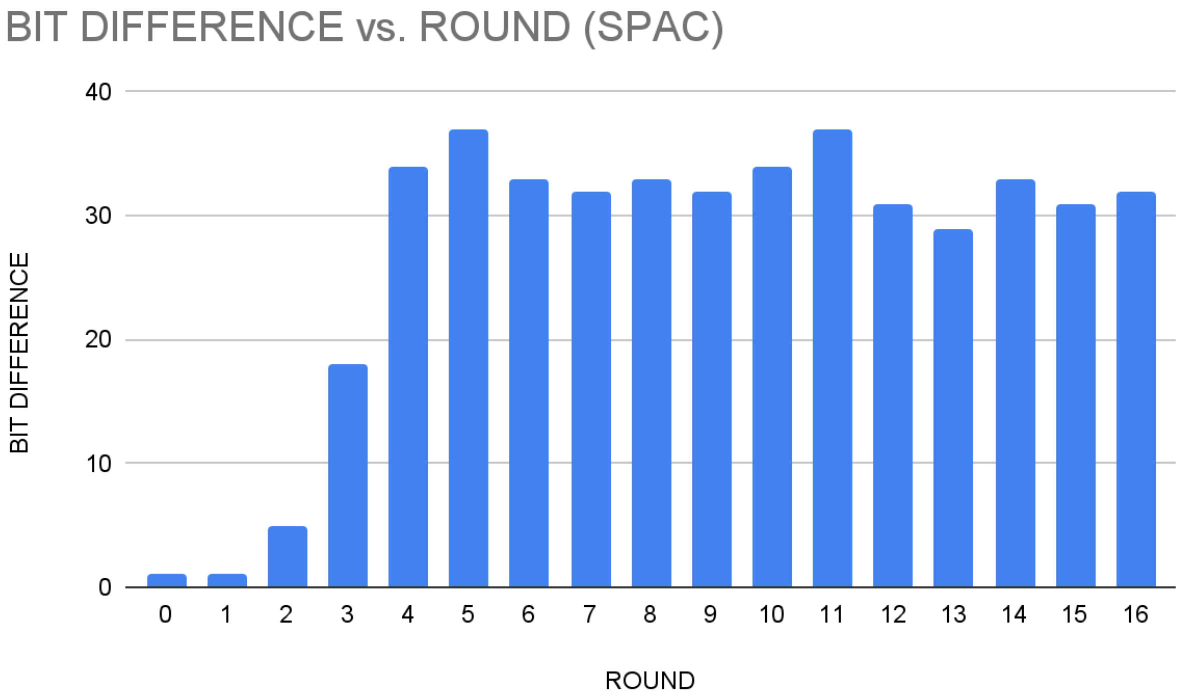


```
Round | Ciphertext
------------------------------------------------------
 1    | 3CF03C0FBAD22845
 2    | BAD2284599E9B723
 3    | 99E9B7230BAE3B9E
 4    | 0BAE3B9E42415649
 5    | 4241564918B3FA41
 6    | 18B3FA419616FE23
 7    | 9616FE2367117CF2
 8    | 67117CF2C11BFC09
 9    | C11BFC09887FBC6C
10    | 887FBC6C600F7E8B
11    | 600F7E8BF596506E
12    | F596506E738538B8
13    | 738538B8C6A62C4E
14    | C6A62C4E56B0BD75
15    | 56B0BD7575E8FD8F
16    | DA02CE3A89ECAC3B
```

# TASK 2 : DIFFUSION AND CONFUSION – SPAC AND SKAC ANALYSIS [40 MARKS]

| ROUND | RESULT 1 | RESULT 2 | BIT DIFFERENCE |
|---|---|---|---|
| round 0 | 02468aceeca86420 | 12468aceeca86420 | 1 |
| round 1 | 3CF03C0FBAD22845 | 3CF03C0FBAD32845 | 1 |
| round 2 | BAD2284599E9B723 | BAD3284539A9B7A3 | 5 |
| round 3 | 99E9B7230BAE3B9E | 39A9B7A3171CB8B3 | 18 |
| round 4 | 0BAE3B9E42415649 | 171CB8B3CCACA55E | 34 |
| round 5 | 4241564918B3FA41 | CCACA55ED16C3653 | 37 |
| round 6 | 18B3FA419616FE23 | D16C3653CF402C68 | 33 |
| round 7 | 9616FE2367117CF2 | CF402C682B2CEFBC | 32 |
| round 8 | 67117CF2C11BFC09 | 2B2CEFBC99F91153 | 33 |
| round 9 | C11BFC09887FBC6C | 99F911532EED7D94 | 32 |
| round 10 | 887FBC6C600F7E8B | 2EED7D94D0F23094 | 34 |
| round 11 | 600F7E8BF596506E | D0F23094455DA9C4 | 37 |
| round 12 | F596506E738538B8 | 455DA9C47F6E3CF3 | 31 |
| round 13 | 738538B8C6A62C4E | 7F6E3CF34BC1A8D9 | 29 |
| round 14 | C6A62C4E56B0BD75 | 4BC1A8D91E07D409 | 33 |
| round 15 | 56B0BD7575E8FD8F | 1E07D4091CE2E6DC | 31 |
| round 16 | DA02CE3A89ECAC3B | 057CDE97D7683F2A | 32 |

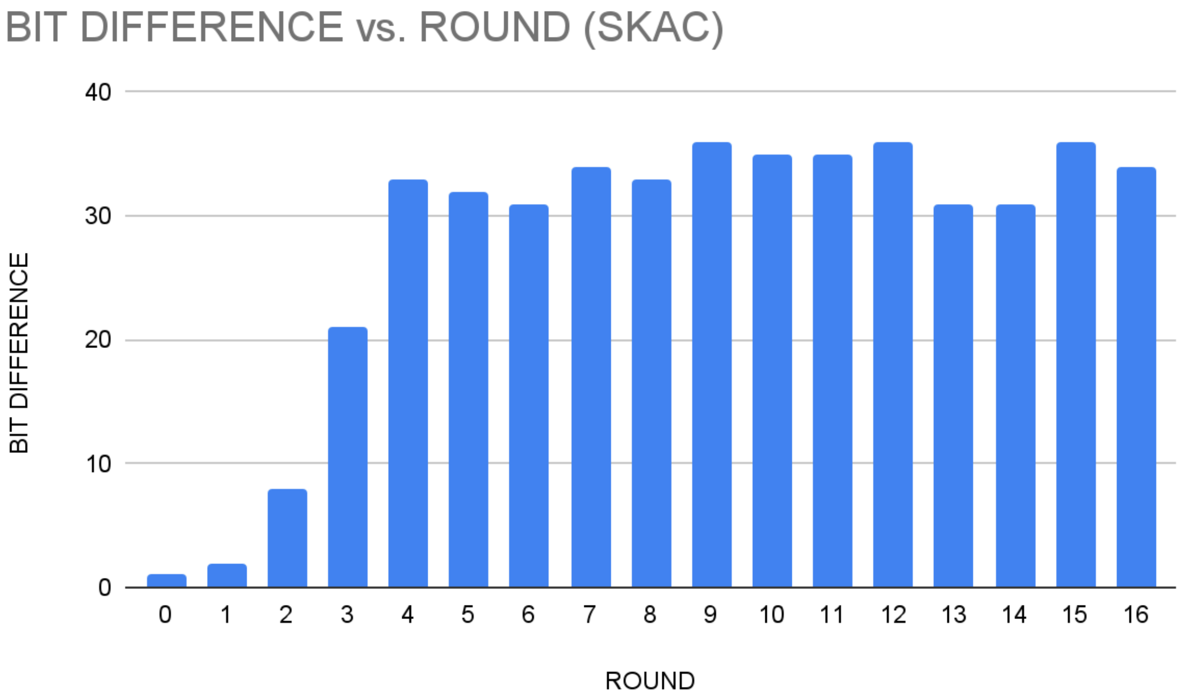
It



The plaintexts fed are 64 bits long, so the avalanche effect of flipping around 50% of bits (32) seems to kick in at around round 4. It seems like this is actually faster than average (50% at around round 5 to 6?), but it satisfies the criterion. Notably, I expected the graph to be more logarithmic in nature, and that the difference would only increase and never decrease over rounds, but that appears to not be the case.

| ROUND | RESULT 1 | RESULT 2 | BIT DIFFERENCE |
|---|---|---|---|
| 0 | 133457799BBCDFF1 | 933457799BBCDFF1 | 1 |
| 1 | 3CF03C0F86DFB8BA | 3CF03C0F869FB8FA | 2 |
| 2 | 86DFB8BA617F198E | 869FB8FA25761D8F | 8 |
| 3 | 617F198E7B12F51D | 25761D8F9ABF7DF5 | 21 |
| 4 | 7B12F51D66EC473D | 9ABF7DF51B37F27D | 33 |
| 5 | 66EC473DD09ABE4F | 1B37F27DD482E5BA | 32 |
| 6 | D09ABE4FC1B416FE | D482E5BAB94267F0 | 31 |
| 7 | C1B416FE323B3287 | B94267F09C36183C | 34 |
| 8 | 323B32877C81DE29 | 9C36183C58FC1563 | 33 |
| 9 | 7C81DE2920822D7C | 58FC1563536ECFA1 | 36 |
| 10 | 20822D7C392C5FE6 | 536ECFA17DFE0804 | 35 |

| | | | |
|---|---|---|---|
| 11 | 392C5FE6BAD15117 | 7DFE080461FA84E6 | 35 |
| 12 | BAD151174F05E89A | 61FA84E6F13D7A3C | 36 |
| 13 | 4F05E89AC5C96BCB | F13D7A3C1DA48983 | 31 |
| 14 | C5C96BCB61392A95 | 1DA48983A325E78A | 31 |
| 15 | 61392A95F03F95B0 | A325E78ABEEBE90F | 36 |
| 16 | 69703930BBE6D0CA | 2AE2C3EAC5ED2CE8 | 34 |



Similar results for the key criterion as well: we see the avalanche of 50% flip comes in at about round 4.