COMP3260 Assignment 2

By Kyle Dryden & Josh O'Brien

Encryption Output

First Set

```
Avalanche Demonstration
Plaintext P:
0110001101101111011011010111000000110011001100100011011000110000
Plaintext P':
0110001101101111011011010111000000110011001100100011011000110001
Key K:
0111010001100101011100110111010001101001011011100110011101110010
Key K':
0111010001100101011100110111010001101001011011100110011101110010
Total running time: 0.069592 seconds

P and P' under K
Ciphertext C DES0:
0110111110000110000100010111100000110011100110101100010110110010
Ciphertext C' DES0:
0111001000000011111111110111100100001001110011000000101010000100

Ciphertext C DES1:
0101000111110110000100000101110101001010010111010001101110001011
Ciphertext C' DES1:
0010000111100000011101101011111111010111101011011100001111011100

Ciphertext C DES2:
1111100100100101011111011101111100000111111011011110101010000101
Ciphertext C' DES2:
1111100100100101011111011101011101000111111011011110101000000101

Ciphertext C DES3:
0111111100011000111010010110100001010101010001110001111100011111
Ciphertext C' DES3:
0111110110110010001101011010101100111000110001101101011101101011
```

Round	DES0	DES1	DES2	DES3
0	1	1	1	1
1	6	5	2	6
2	24	13	3	9
3	35	23	3	7
4	29	26	4	10
5	32	28	5	19
6	33	32	5	20
7	32	30	4	25
8	32	34	5	36
9	27	35	7	37
10	29	31	8	35
11	33	25	7	32
12	29	29	5	32
13	28	39	4	37
14	31	33	3	35
15	32	32	3	28
16	32	32	3	28

Second Set

P under K and K’
Ciphertext C DES0:
0110111110000110000100010111100000110011100110101100010110110010
Ciphertext C’ DES0:
1000000101110010001111011110011010011100000000011101101110110111

Ciphertext C DES1:
0101000111110110000100000101110101001010010111010001101110001011
Ciphertext C’ DES1:
0101000111110110000100000101110101001010010111010001101110001011

Ciphertext C DES2:
1111100100100101011111011101111100000111111011011110101010000101
Ciphertext C’ DES2:
1011001001001011110100110101100110110100011011111111100000000110

Ciphertext C DES3:
0111111100011000111010010110100001010101010001110001111100011111
Ciphertext C’ DES3:
1001111110111001101001010110000110000011011100010001100011111011

Round	DES0	DES1	DES2	DES3
0	2	0	0	2
1	13	0	1	12
2	25	0	3	22
3	28	0	5	26
4	31	0	7	30
5	29	0	10	37
6	31	0	15	40
7	38	0	17	35
8	41	0	18	32
9	36	0	21	35
10	29	0	24	40
11	31	0	25	42
12	32	0	24	40
13	35	0	25	40
14	39	0	32	34
15	37	0	29	27
16	37	0	29	27

Decryption Output

```
DECRYPTION
Ciphertext C:
0110001101101111011011010111000000110011001100100011011000110000
Key K:
0111010001100101011100110111010001101001011011100110011101110011

Plaintext P DESO:
1101001111100001011101101011100100111111011000000100011101111110
Plaintext P DES1:
0101000111110110000100000101110101001010010111010001101110001011
Plaintext P DES2:
1111111100111011101101001010101111010011001101100010100101010110
Plaintext P DES3:
0111110100001011110011011100100100111011010011010011100001100110
```