CS 153 Problem Set 1 Documentation

Mark Daniel Asiddao & Jacob Villanueva

Plaintext(in hex): 0123456789abcdef
Key(in hex): 0101010101010101

**********Encrypting string: 0123456789abcdef**********

Original Bits: 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
Key(in Binary): 00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001

Initial Permutation: 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

------------------------------ Round 0 ------------------------------

PC: 0000000 0000000 0000000 0000000 0000000 0000000 0000000 0000000
C: 0000000 0000000 0000000 0000000
D: 0000000 0000000 0000000 0000000
L: 1100 1100 0000 0000 1100 1100 1111 1111
R: 1111 0000 1010 1010 1111 0000 1010 1010

------------------------------ Round 1 ------------------------------

ROUNDKEY(2): 000000 000000 000000 000000 000000 000000 000000 000000

ROUNDKEY(16): 000000000000

…
<results of the succeeding rounds have been omitted because of repetition>

Final Permutation(2):
0110000101111011001110100000110011101000111100000111000100000000
Final Permutation(16): 617b3a0ce8f07100
Ciphertext(2):
0110000101111011001110100000110011101000111100000111000100000000
Ciphertext(16):
617b3a0ce8f07100

Analysis of the given output:

Key (in hexadecimal to binary) : 0000 0001. Every eighth bit of the key is used as the parity bit, reducing the key to 56 bits of only zeros, and the parity bitstring is composed of ones. We have noticed that, after each iteration, the key rotates only zeros. The 56 bit string remains the same after 16 rounds. The successive iterations for rotating the key have been cut from this sample because the key after each round does not change. We have also noticed that, compared to the key (in hexadecimal) 0000000000000000 (a semi-weak key), DES gives the same encryption as the example. This is due to the fact that every eighth binary bit is omitted resulting in some keys having the same encryption (without making use of the parity bits). In addition, when "encrypting" the resulting ciphertext in DES using this same key, the resultant ciphertext is the same as the initial plaintext:

Plaintext(in hex): 617b3a0ce8f07100
Key(in hex): 0101010101010101

*********Encrypting string: 617b3a0ce8f07100*********
Original Bits: 0110 0001 0111 1011 0011 1010 0000 1100 1110 1000 1111 0000 0111 0001 0000 0000
Key(in Binary): 00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001
Initial Permutation: 0111 0011 0110 0110 0000 1000 0100 0011 0011 0000 0111 0111 0001 1110 0000 0110

Final Permutation(2):
0000000100100011010001010110011111000100110101011110011011101111
Final Permutation(16): 0123456789abcdef
Ciphertext(2):
0000000100100011010001010110011111000100110101011110011011101111
Ciphertext(16):
123456789abcdef

Plaintext(in hex): 0123456789abcdef
Key(in hex): fefefefefefefefe

**********Encrypting string: 0123456789abcdef**********

Original Bits: 0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111
Key(in Binary): 11111110 11111110 11111110 11111110
11111110 11111110 11111110 11111110

Initial Permutation: 1100 1100 0000 0000 1100 1100 1111
1111 1111 0000 1010 1010 1111 0000 1010 1010

------------------------------ Round 0 ------------------------------

PC: 1111111 1111111 1111111 1111111 1111111
1111111 1111111 1111111
C: 1111111 1111111 1111111 1111111
D: 1111111 1111111 1111111 1111111
L: 1100 1100 0000 0000 1100 1100 1111 1111
R: 1111 0000 1010 1010 1111 0000 1010 1010

------------------------------ Round 1 ------------------------------

ROUNDKEY(2): 111111 111111 111111 111111 111111
111111 111111 111111

ROUNDKEY(16): ffffffffffff

…
<results of the succeeding rounds have been omitted because of repetition>

Final Permutation(2):
0110110111001110000011011100100100000000011001010
101011010100011
Final Permutation(16): 6dce0dc9006556a3
Ciphertext(2):
0110110111001110000011011100100100000000011001010
101011010100011
Ciphertext(16):
6dce0dc9006556a3

Analysis of the given output:

The key in the second example is the inversion of the previous key. Instead of 0000 0001, the inverted binary bitstring becomes 1111 1110. Every eighth bit is removed, the key of 56 bits is composed of only ones, while the parity bitstring is composed of zeros. Like the previous key (repeated 01s) after each iteration, the 56 bit string remains the same after 16 rounds, and was cut from this sample because it remains the same. Like the previous example, this key also decrypts the ciphertext identically by encrypting the ciphertext again using the same key. In DES, this key is coined as a Weak Key.

Plaintext(in hex): 0000000000000000
Key(in hex): 1f1f1f1f1f1f1f1f

*********Encrypting string: 0000000000000000*********

Original Bits: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
Key(in Binary): 00011111 00011111 00011111 00011111 00011111 00011111 00011111 00011111
Initial Permutation: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
---------- Round 0 ----------
PC: 0000000 0000000 0000000 0001111 1111111 1111111 1111111 1111111
---------- Round 1 ----------
ROUNDKEY(2): 000100 000000 000010 001000 111111 111111 111111 111111
ROUNDKEY(16): 100088ffffff
---------- Round 2 ----------
ROUNDKEY(2): 000100 000000 100010 000000 111111 111111 111111 111111
ROUNDKEY(16): 100880ffffff
---------- Round 3 ----------
ROUNDKEY(2): 000100 000010 100000 000000 111111 111111 111111 111111
ROUNDKEY(16): 102800ffffff
---------- Round 4 ----------
ROUNDKEY(2): 000000 000010 010000 000100 111111 111111 111111 111111
ROUNDKEY(16): 002404ffffff
---------- Round 5 ----------
ROUNDKEY(2): 010000 000000 010000 000100 111111 111111 111111 111111
ROUNDKEY(16): 400404ffffff
---------- Round 6 ----------
ROUNDKEY(2): 010000 001000 000000 100000 111111 111111 111111 111111
ROUNDKEY(16): 408020ffffff
---------- Round 7 ----------
ROUNDKEY(2): 100000 001000 000000 100010 111111 111111 111111 111111
ROUNDKEY(16): 808022ffffff
---------- Round 8 ----------
ROUNDKEY(2): 101000 000000 001000 000010 111111 111111 111111 111111
ROUNDKEY(16): a00202ffffff
---------- Round 9 ----------
ROUNDKEY(2): 001000 000001 001000 000010 111111 111111 111111 111111
ROUNDKEY(16): 201202ffffff
---------- Round 10 ----------
ROUNDKEY(2): 001000 000001 000001 000000 111111 111111 111111 111111
ROUNDKEY(16): 201040ffffff
---------- Round 11 ----------
ROUNDKEY(2): 000000 000100 000001 010000 111111 111111 111111 111111
ROUNDKEY(16): 004050ffffff
---------- Round 12 ----------
ROUNDKEY(2): 000001 000100 000100 010000 111111 111111 111111 111111
ROUNDKEY(16): 044110ffffff
---------- Round 13 ----------
ROUNDKEY(2): 000001 100000 000100 000001 111111 111111 111111 111111
ROUNDKEY(16): 060101ffffff
---------- Round 14 ----------
ROUNDKEY(2): 000010 110000 000000 000001 111111 111111 111111 111111
ROUNDKEY(16): 0b0001ffffff
---------- Round 15 ----------
ROUNDKEY(2): 000010 010000 000010 001000 111111 111111 111111 111111
ROUNDKEY(16): 090088ffffff
---------- Round 16 ----------
ROUNDKEY(2): 000000 010000 000010 001000 111111 111111 111111 111111
ROUNDKEY(16): 010088ffffff

Final Permutation(2): 0100101110110000110010000010001101010100000010110110010101001100
Final Permutation(16): 4bb0c823540b654c
Ciphertext(2): 0100101110110000110010000010001101010100000010110110010101001100
Ciphertext(16): 4bb0c823540b654c

Analysis of the given output:

In the 3rd example, the key given by the hex string 1f1f1f1f1f1f1f1f shows that after the main key is processed by PC-1, the bit key generated becomes a series of twenty-four zeroes and a series of ones. Evidently, in the successive rounds until round 16, the key consistently outputs six f's on the second half (D_0) while the first half (C_0) is altered after each iteration. Looking closely at each half, the bitstring is simply a permutation of the previous round's half, which explains why half of the key consistently outputs f's.

Plaintext(in hex): faded09178888888
Key(in hex): e0e0e0e0e0e0e0e0

*********Encrypting string: faded09178888888*********

Original Bits: 1111 1010 1101 1110 1101 0000 1001 0001 0111 1000 1000 1000 1000 1000 1000 1000
Key(in Binary): 11100000 11100000 11100000 11100000 11100000 11100000 11100000 11100000
Initial Permutation: 0001 0111 0001 1111 0000 0010 0000 1000 1110 1111 0001 0001 1111 0011 0000 0011
---------- Round 0 ----------
PC: 1111111 1111111 1111111 1110000 0000000 0000000 0000000 0000000
---------- Round 1 ----------
ROUNDKEY(2): 111011 111111 111101 110111 000000 000000 000000 000000
ROUNDKEY(16): efff77000000
---------- Round 2 ----------
ROUNDKEY(2): 111011 111111 011101 111111 000000 000000 000000 000000
ROUNDKEY(16): eff77f000000
---------- Round 3 ----------
ROUNDKEY(2): 111011 111101 011111 111111 000000 000000 000000 000000
ROUNDKEY(16): efd7ff000000
---------- Round 4 ----------
ROUNDKEY(2): 111111 111101 101111 111011 000000 000000 000000 000000
ROUNDKEY(16): ffdbfb000000
---------- Round 5 ----------
ROUNDKEY(2): 101111 111111 101111 111011 000000 000000 000000 000000
ROUNDKEY(16): bffbfb000000
---------- Round 6 ----------
ROUNDKEY(2): 101111 110111 111111 011111 000000 000000 000000 000000
ROUNDKEY(16): bf7fdf000000
---------- Round 7 ----------
ROUNDKEY(2): 011111 110111 111111 011101 000000 000000 000000 000000
ROUNDKEY(16): 7f7fdd000000
---------- Round 8 ----------
ROUNDKEY(2): 010111 111111 110111 111101 000000 000000 000000 000000
ROUNDKEY(16): 5ffdfd000000
---------- Round 9 ----------
ROUNDKEY(2): 110111 111110 110111 111101 000000 000000 000000 000000
ROUNDKEY(16): dfedfd000000
---------- Round 10 ----------
ROUNDKEY(2): 110111 111110 111110 111111 000000 000000 000000 000000
ROUNDKEY(16): dfefbf000000
---------- Round 11 ----------
ROUNDKEY(2): 111111 111011 111110 101111 000000 000000 000000 000000
ROUNDKEY(16): ffbfaf000000
---------- Round 12 ----------
ROUNDKEY(2): 111110 111011 111011 101111 000000 000000 000000 000000
ROUNDKEY(16): fbbeef000000
---------- Round 13 ----------
ROUNDKEY(2): 111110 011111 111011 111110 000000 000000 000000 000000
ROUNDKEY(16): f9fefe000000
---------- Round 14 ----------
ROUNDKEY(2): 111101 001111 111111 111110 000000 000000 000000 000000
ROUNDKEY(16): f4fffe000000
---------- Round 15 ----------
ROUNDKEY(2): 111101 101111 111101 110111 000000 000000 000000 000000
ROUNDKEY(16): f6ff77000000
---------- Round 16 ----------
ROUNDKEY(2): 111111 101111 111101 110111 000000 000000 000000 000000
ROUNDKEY(16): feff77000000

Final Permutation(2): 1111101000100110011000111001001100010010010101110010100011110011
Final Permutation(16): fa266393125728f3
Ciphertext(2): 1111101000100110011000111001001100010010010101110010100011110011
Ciphertext(16): fa266393125728f3

Analysis of the given output:

In this 4th example, much like the 3rd sample key, the Permuted Choice(1) iterates and leaves the second half of the round key to be consistently a series of zeroes for the incoming rounds while the first half receives alterations. The output of the 3rd example also complements the 4th sample key. By adding the bits of the key for each round with each other, the bitstring would output twelve f's . This leads to the conclusion that if initially, two keys bitwise complement each other, the sum of their keys after each round of DES will be a string of ones.