Homework 6 – Problem 1

S-box 4 is observed to have the indicated output xor when presented with the indicated inputs

```
In1: 0x22, In2: 0x16,  Output xor: 0x0c
In1: 0x12, In2: 0x0c , Output xor: 0x05
```

Perform a differential cryptanalysis and produce the possible candidate key(s). You may find the tables provided in “DC.txt” helpful.

Homework 6, problem 2 (omit)

Consider the 2 round iterative differential characteristic for DES
0x19600000000000→0x19600000000000, p=1/234

Suppose for the following questions we can always find chosen plaintext with S/N ratio high enough to require only 10 “right pairs” for a successful differential cryptanalysis (“DC”).

a. On average, how many chosen plain ciphertext pairs are required for a successful DC on two rounds?
b. On average, how many chosen plain ciphertext pairs are required for a successful DC on ten rounds?
c. After how many rounds is DC impossible because there cannot possibly be enough plain ciphertext pairs to succeed?

Homework 6 – Problem 3

A certain cipher X with 6 bit key $k_1, k_2, k_3, k_4, k_5, k_6$ has 4 linear constraints.

Given the corresponding plaintext, ciphertext pairs and substituting the equations become:

$$0 = k_1 \oplus k_3 \oplus k_4$$
$$0 = k_4 \oplus k_5$$
$$0 = k_1 \oplus k_2$$
$$1 = k_1 \oplus k_6$$

Guessing k_1 and k_3 calculate k_2, k_4, k_5, k_6. How many encryptions are needed to discover the correct key with exhaustive search in the worst case?

How many are needed with these constraints?

Homework 6, problem 4

(A) Suppose the cipher X has a linear constraint (Equation 1) that holds with probability p=.75 where the input to X is plaintext bits $i_1||i_2||\ldots||i_6$; the output is the ciphertext bits $o_1||o_2||\ldots||o_6$ under key bits $k_1||k_2||\ldots||k_6$. The constants $a_1, a_2, \ldots, a_6, b_1, b_2, \ldots, b_6, c_1, c_2, \ldots, c_6, d$ are all known.

Equation 1: $a_1i_1 \oplus a_2i_2 \oplus a_3i_3 \oplus a_4i_4 \oplus a_5i_5 \oplus a_6i_6 \oplus$
$b_1o_1 \oplus b_2o_2 \oplus b_3o_3 \oplus b_4o_4 \oplus b_5o_5 \oplus b_6o_6 =$
$c_1k_1 \oplus c_2k_2 \oplus c_3k_3 \oplus c_4k_4 \oplus c_5k_5 \oplus c_6k_6 \oplus d$

Finally, suppose upon substituting values from 3 plaintext/ciphertext pairs the left hand side of equation 1 has values 1,1,0, respectively.

What are the odds that $c_1k_1 \oplus c_2k_2 \oplus c_3k_3 \oplus c_4k_4 \oplus c_5k_5 \oplus c_6k_6 \oplus d=1$ rather than 0?

(B) Suppose the same setup as in A but 3 out of 4 plaintext/ciphertext pairs "vote" that $c_1k_1 \oplus c_2k_2 \oplus c_3k_3 \oplus c_4k_4 \oplus c_5k_5 \oplus c_6k_6 \oplus d=1$.

What are the odds that $c_1k_1 \oplus c_2k_2 \oplus c_3k_3 \oplus c_4k_4 \oplus c_5k_5 \oplus c_6k_6 \oplus d=1$ rather than 0?

Homework 6, problem 4

(C) Constructing a multi-round constraint

Suppose X is a four round iterative cipher with plaintext input, P and ciphertext output C where each round has 6 bit input I and 6 bit output O and per round keys $K^{(1)}, K^{(2)}, \ldots K^{(6)}$. Using Matsui's notation suppose the contraints:

$I[1,2] \oplus O[3,4]= K^{(1)}[1,3]$ R1

$I[3,4] \oplus O[1,5]= K^{(2)}[4,6]$ R2

$I[1,5] \oplus O[1,6]= K^{(3)}[1,5]$ R3

$I[1,6] \oplus O[2,5]= K^{(4)}[2]$ R4

hold with probabilities $p_1= .8$, $p_2= .9$, $p_3= .8$, $p_4= .9$, respectively.

What is the probability that

$P[1,2] \oplus C[2,5]= K^{(1)}[1,3] \oplus K^{(2)}[4,6] \oplus K^{(3)}[1,5] \oplus K^{(4)}[2]$?

Homework 6, problem 4

(D) Suppose X is a multi round iterative cipher with 40 bit plaintext input, P, and ciphertext output, C, and 40 bit key. Suppose, using Matsui's notation, that the following four linearly independent constraints:

i. $P[a_1^{(1)}, a_2^{(1)},\ldots, a_{40}^{(1)}] \oplus C[b_1^{(1)}, b_2^{(1)},\ldots, b_{40}^{(1)}]= K[c_1^{(1)}, c_2^{(1)},\ldots, c_{40}^{(1)}]$

ii. $P[a_1^{(2)}, a_2^{(2)},\ldots, a_{40}^{(2)}] \oplus C[b_1^{(2)}, b_2^{(2)},\ldots, b_{40}^{(2)}]= K[c_1^{(2)}, c_2^{(2)},\ldots, c_{40}^{(2)}]$

iii. $P[a_1^{(3)}, a_2^{(3)},\ldots, a_{40}^{(3)}] \oplus C[b_1^{(3)}, b_2^{(3)},\ldots, b_{40}^{(3)}]= K[c_1^{(3)}, c_2^{(3)},\ldots, c_{40}^{(3)}]$

iv. $P[a_1^{(4)}, a_2^{(4)},\ldots, a_{40}^{(4)}] \oplus C[b_1^{(4)}, b_2^{(4)},\ldots, b_{40}^{(4)}]= K[c_1^{(4)}, c_2^{(4)},\ldots, c_{40}^{(4)}]$

hold with probabilities p_1= .75, p_2= .7, p_3= .8, p_4= .9, respectively.

Suppose that on 10 plaintext/ciphertext pairs the LHS of i, ii, iii and iv "vote" that the RHS of the equations are 0 with tallies (2,8,2,8)

What is the probabilities that each of the most popular choices for the resulting constraints is correct? What is the probability that all 4 are correct? If all 4 are correct, and assuming X takes 1 microsecond/encrypt, what is the time to break X by exhaustive search (assuming a serial processor)? How about by applying the 4 constraints and searching for the remaining key bits (assuming a serial processor)?

PS: Key search is a "trivially parallelizable" operation.

Homework 6, problem 4

(E) In the lecture we noted that there was a linear attack that worked on 16 round DES with 2^{43} plaintext/ciphertext pairs where the basic constraint held with probability $p = \frac{1}{2} + \epsilon$ where $\epsilon = 1.19 \times 2^{-21}$ is the “bias”. Using this fact, estimate for what p, there are not enough corresponding plain/cipher texts to enable applying the Linear cryptanalysis to reduce the search keyspace.