Homework 6

John Manferdelli
jlm@cs.washington.edu
jmanfer@microsoft.com

This material is provided without warranty of any kind including, without limitation, warranty of non-infringement or suitability for any purpose. This material is not guaranteed to be error free and is intended for instructional use only.

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, answer 1

```
D4(34, 0c): (0c,38)(0d,39)(18,2c)(19,2d)(2c,18)
            (2d,19)(38,0c)(39,0d)         8 found


                  22
0c  00 1100 ^ 01 0110 = 01 1010 = 1a
38  11 1000 ^ 01 0110 = 10 1110 = 2e
0d  00 1101 ^ 01 0110 = 01 1011 = 1b
39  11 1001 ^ 01 0110 = 10 1110 = 2e
18  01 1000 ^ 01 0110 = 00 1110 = 0e
2c  01 1100 ^ 01 0110 = 00 1010 = 0a
19  01 1001 ^ 01 0110 = 00 1110 = 1e
2d  10 1101 ^ 01 0110 = 11 1011 = 3d
```

Homework 6, answer 1

```
D4(1e, 05): (08,16)(16,08)(26,38)(38,26)    4 found


                        0c
08   00 1000 ^ 00 1100 = 00 0100 = 04
16   01 0110 ^ 00 1100 = 01 1010 = 1a
26   10 0110 ^ 00 1100 = 10 1010 = 2a
38   11 1000 ^ 00 1100 = 11 0100 = 34
```

Homework 6, problem 2

Consider the 2 round iterative differential characteristic for DES
0x196000000000000→0x196000000000000, 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, answer 2

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

Suppose the S/N is 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?

Let m be the number of chosen plain ciphertext pairs. $1/234\ m \geqq 10$, so $m \geqq 2340$

b. On average, how many chosen plain ciphertext pairs are required for a successful DC on ten rounds?

$(1/234)^5\ m \geqq 10$, so $m \geqq 10(234^5) \approx 7 \times 10^{12}$

c. After how many rounds is DC impossible because there cannot possibly be enough plain ciphertext pairs to succeed?

$(1/234)^5\ 2^{64} \leqq 10$, $(234)^{n/2} \geqq (.10)2^{64}$, $n/2 \geqq (\log(1.6)+17)/\log(234)$. $n \geqq 7.26$. So 16 rounds is impossible.

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, answer 3

$0= k_1 \oplus k_3 \oplus k_4 \rightarrow k_4 = k_1 \oplus k_3$

$0= k_4 \oplus k_5 \rightarrow k_5 = k_4$

$0= k_1 \oplus k_2 \rightarrow k_2 = k_1$

$1= k_1 \oplus k_6 \rightarrow k_6 = k_1 \oplus 1$

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?

2^6=64

How many are needed with these constraints?

4

Homework 6, problem 4 (A, B)

(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 $c_1k_1 \oplus c_2k_2 \oplus c_3k_3 \oplus c_4k_5 \oplus c_5k_5 \oplus c_6k_6 \oplus d=1$ 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, answer 4 (A, B)

(A) Let the three equations be E_1, E_2 and E_3 and $q=1-p$. Suppose 1 is the correct value then the probability that E_1 and E_2 are correct and E_3 is incorrect is p^2q; if 0 is the correct value the probability that E_1 and E_2 are incorrect and E_3 is correct is q^2p. So the odds that 1 is correct are $(p^2q)/(q^2p)= p:q=3:1$. The probability it's correct is ¾.

(B) $(p^3q)/(q^3p)=(p/q)^2=9:1$. The probability it's correct is 9/10.

Note: This is all I expected but for an explanation see the next page.

Homework 6, problem 4 (A, B Supplement)

Let $P(110|1)$ be the probability that 110 as the outcome of the “event’ if 1 is correct (i.e.- if the constraint equation is correct). Define $P(110|0)$ similarly.

Let $P(1|110)$ be the probability that 1 is correct given the 110 outcome of the event. Define $P(1|110)$ similarly.

Let $P(1, 110)$ be the joint probability. Let $P(1)$ be the a priori probability that 1 is the outcome and $P(0)$ be the a priori probability that 0 is the outcome.

$P(1|110)= P(110|1)\ P(1)/P(110)$ [Bayes]

$P(1|110)P(110)=P(1,110)$ and $P(0|110)P(110)=P(0,110)$ [Conditional prob]

$P(1|110)+P(0|110) =1$ multiplying by this $P(110)$, we get

$$P(1|110)\ P(110)+P(0|110)\ P(110) = P(110)$$

$$P(1|110)/P(0|110)= [P(1)\ P(110|1)/(P(0,110)+P(1,110))]/ [P(0)\ P(110|0)/(P(0,110)+P(1,110))]= P(110|1)/P(110|0)$$

So $P(1|110)/P(0|110)= P(110|1)/P(110|0) =p/q$.

Homework 6, problem 4 (C)

(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 $K^{(1)}$, $K^{(2)}$,…$K^{(6)}$. 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, answer 4 (C)

(C) Let $q_i=1-p_i$.

The probability that the resulting equation is correct is the probability that all 4 equations are correct plus the probability that exactly two are correct plus the probability that all 4 are wrong. So,

$$\begin{aligned}
&\text{Prob}(P[1,2] \oplus C[2,5]= K^{(1)}[1,3] \oplus K^{(2)}[4,6] \oplus K^{(3)}[1,5] \oplus K^{(4)}[2])= \\
&\quad p_1p_2p_3p_4+ p_1p_2q_3q_4+ p_1q_2p_3q_4+ p_1q_2q_3p_4+ q_1q_2p_3p_4+ \\
&\quad q_1p_2q_3p_4+ q_1p_2p_3q_4+q_1q_2q_3q_4= \\
&\quad (.8)^2(.9)^2+(.2)^2(.9)^2+(.8)^2(.1)^2+4(.9)(.1)(.8)(.2)+(.2)^2(.1)^2= \\
&\quad .5184+.0324+.0064+.0576+.0004=.6152
\end{aligned}$$

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, answer 4 (D)

(D) As in (A) and (B), the odds for each of the 4 equations and the corresponding probabilities are

$o_1= [(3/4)^8(1/4)^2]/[(3/4)^2(1/4)^8]= 3^6:1= 729:1;\quad p_1=729/730$

$o_2= [(.7)^8(.3)^2]/[(.7)^2(.3)^8]= 7^6:3^6= 161:1;\quad p_2=161/162$

$o_3= [(.8)^8(.2)^2]/[(.8)^2(.2)^8]= 4^6:1= 4096:1,\ p_3= 4096/4097$

$o_4= [(.9)^8(.1)^2]/[(.9)^2(.1)^8]= 9^6:1,\ p_4= 531441/ 531442$

So they are virtually certain.

So is the product of the resulting probabilities $p_1\ p_2\ p_3\ p_4>.99$

Worse case exhaustive search requires 2^{40} encryptions. At 1 encryption per microsecond, this takes $2^{40} \text{ x } 10^{-6} \approx 10^6$ seconds or about $10^6/86{,}400 \approx$ 11.5 days

With linear constraints $\approx 2^{36}$ encryptions are requires taking about 18 hours.

4 constraints help a lot.

Homework 6, problem 4 (E)

(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 $p= ½ + \epsilon$ 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.

Homework 6, answer 4 (E)

(E) Recall from the lecture that the best linear expression with probability $p=1/2 + \epsilon$ where $\epsilon= 1.19 \times 2^{-21}$ required 2^{43} plaintext/ciphertext pairs to solve a 16 round version of DES and the amount of corresponding plain/ciphertext required, R, was $R \approx c\epsilon^{-2}$, thus, $c\,(1.19 \times 2^{-21})^2 \approx 2^{43}$. Linear Cryptanalysis fails when fewer pairs exist than are required. In the case of DES this is 2^{64} pairs. This happens

$$(1.19 \times 2^{-21}/\epsilon))^2 \geqq (2^{64})/(2^{43})) \rightarrow (1.19/\sqrt{2}) \times 2^{-21} \times 2^{-10} \geqq \epsilon \rightarrow 8.4 \times 2^{-32} \geqq \epsilon$$

End Paper

- Done