MATH 314 Fall 2018 - Class Notes

10/15/2018

Scribe: Sasha Ashtiani

Summary: Basic strategy to decrypt SDES.

Differential Cryptanalysis: Released in late 80's, but was known to NSA much earlier.

- Chosen Plaintext attack:

Goal: Recover k_3

Recall S-DES:

Start with $\mathbf{L_0}$, $\mathbf{R_0}$ (Plaintext)

Step 1) $\mathbf{L_1} = \mathbf{R_0}$ and $R_1 = f(R_0, k_1) \oplus L_0$

Step 2) $L_2 = R_1$ and $\mathbf{R_2} = f(R_1, k_2) \oplus L_1$

Step 3) $\mathbf{L_3} = R_2$ and $\mathbf{R_3} = f(R_2, k_3) \oplus L_2$

NOTE: Eve already knows the highlighted ones

L_0 and R_0 are from chosen plaintext
L_3 and R_3 are from ciphertext
Because $L_3 = R_2$, Eve knows R_2

Eve wants to try and use this info to find k_3
We want to work backwards

$R_3 = f(R_2, k_3) \oplus L_2 = f(R_2, k_3) \oplus (f(R_0, k_1) \oplus L_0)$

Eve now encrypts a new plaintext: L_0^*, R_0^*

She keeps the right half the same: $R_0 = R_0^*$
But changes the left half

Out of the encryption comes a new ciphertext: L_3^* and R_3^*

$R_3^* = f(R_2^*, k_3) \oplus \mathbf{f(R_0^*, k_1)} \oplus L_0^*$

NOTE: $f(R_0^*, k_1)$ is same as $f(R_0, k_1)$

$R_3 = f(R_2, k_3) \oplus f(R_0, k_1) \oplus L_0$
$R_3^* = f(R_2^*, k_3) \oplus \underline{\mathbf{f(R_0, k_1)}} \oplus L_0^*$
$\oplus$ Both sides:

NOTE: $f(R_0^*, k_1)$ was replaced by $f(R_0, k_1)$ b/c they are same

$R_3 \oplus R_3^* = f(R_2, k_3) \oplus f(R_2^*, k_3) \oplus f(R_0, k_1) \oplus f(R_0, k_1) \oplus L_0 \oplus L_0^*$
$R_3 \oplus R_3^* = f(\cancel{R_2}, k_3) \oplus f(\cancel{R_2^*}, k_3) \oplus \cancel{f(R_0, k_1)} \oplus \cancel{f(R_0, k_1)} \oplus L_0 \oplus L_0^*$

R_2 becomes L_3 and R_2^* becomes L_3^*

Add $(L_0 \oplus L_0^*)$ to both sides:

$$\mathbf{(R_3 \oplus R_3^*) \oplus (L_0 \oplus L_0^*) = f(L_3, k_3) \oplus f(L_3^*, k_3)}$$

Eve now has an equation where she knows everything but $\underline{\mathbf{k_3}}$

However, S-Boxes were designed to make this equation hard to solve

It would be great for Eve if she knew the value of output $= f(L_3, k_3)$

Unfortunately for her, she doesn't know the output

But she does know output $\oplus$ output* $= (R_3 \oplus R_3^*) \oplus (L_0 \oplus L_0^*)$

Try to extract k_3 from the f function

Recall SDES f-function:
R_2 (is = to L_3) $\rightarrow$ Expander $\rightarrow \mathbf{E(L_3)} \oplus \mathbf{k_3} \rightarrow S_1$ and $S_2 \rightarrow$ output

input $= E(L_3) \oplus k_3$
Eve doesn't know input because she doesnt know k_3

Her goal is to find input

input $= E(L_3) \oplus k_3$
input* $= E(L_3^*) \oplus k_3$

input $\oplus$ input* $= \mathbf{E(L_3)} \oplus \mathbf{E(L_3^*)}$

Eve knows all that

Now Eve exploits the fact that she knows input $\oplus$ input* and output $\oplus$ output* :
To restrict the number of things she has to check in the S-Boxes

Example: Eve has done all this and has found that:

$L_3 = 1011\ 10$ and $L_3^* = 0000\ 10$
$E(L_3) = 1011\ 1110$ and $E(L_3^*) = 0000\ 0010$
input $\oplus$ input* $= E(L_3) \oplus E(L_3^*) = 1011\ 1100$

She also computes:

$(R_3 \oplus R_3^*) \oplus (L_0 \oplus L_0^*) = 1000\ 01 =$ output $\oplus$ output*

1st 4 bits of input get fed into S-Box 1
Sum of the outputs is 100
Suppose the 1st four bits of input were 0000
Then the 1st four bits of input* are 1011

$S_1(0000) \oplus S_1(1011)$
$001 \oplus 010 = 011 \neq 100$

So the 1st four bits of input were not 0000

Try all 16 1st four bits of input:
Lets try 0001 is input, 1010 is input*

$S_1(0001) \oplus S_1(1010) = 010 \oplus 110 = 100$ ✓

Both 0001 and 1010 work as the 1st 4 bits of input

CoCalc in class
Sage code for SDES Differential Cryptanalysis