MATH 314 - Spring 2018 - Class Notes
Alexander Stoyanov
03/27/2018

Recall SDES Feistel Cipher (3 rounds)

Round 1:	$L_1 = R_0$	$R_1 = L_0 \oplus f(R_0, K_1)$
Round 2:	$L_2 = R_1$	$R_2 = L_1 \oplus f(R_1, K_2)$
Round 3:	$L_3 = R_2$	$R_3 = L_2 \oplus f(R_2, K_3)$

Differential Cryptanalysis:

- Sort of like reverse engineering the system to recover the

Use Differential Cryptanalysis to attack SDES:

- Chosen Plaintext Attack
- Eve's goal is to recover K_3

Eve starts off with any plaintext L_0, R_0. She encrypts this and gets L_3, R_3.
She knows $R_3 = L_2 \oplus f(R_2, K_3) = L_2 \oplus f(L_3, K_3) \rightarrow R_3 = (L_0 \oplus f(R_0, K_1)) \oplus f(L_3, K_3)$

Now Eve picks a new plaintext L_0* and R_0* where L_0* can be anything (different from L_0).
But R_0* $= R_0$ (only change left half of the plaintext).
She encrypts this plaintext and gets L_3*, R_3*.

R_3* $= L_0$* $\oplus f(R_0$*$,K_1) \oplus f(L_3$*$,K_3)$ $\oplus$ $R_3 = L_0 \oplus f(R_0,K_1) \oplus f(L_3,K_3)$

$R_3 \oplus R_3$* $= (L_0 \oplus L_0$*$) \oplus f(L_3$*$,K_3) \oplus f(L_3, K_3)$

$(R_3 \oplus R_3$*$) \oplus (L_0 \oplus L_0$*$) = f(L_3, K_3) \oplus f(L_3$*$,K_3)$

F-function:

$L_3 \rightarrow [Expander] \rightarrow [E(L_3) \oplus K_3] \rightarrow [S_1, S_2] \rightarrow [Output]$

Eve doesn't know output but she does know

$output \oplus output$* $= (R_3 \oplus R_3$*$) \oplus (L_0 \oplus L_0$*$)$

She also doesn't know input, but

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

Ex: Suppose Eve is performing differential cryptanalysis and she ends up finding that
$L_3 = 101110, L_3{}^* = 000010$
She also computes that $(R_3 \oplus R_3{}^*) \oplus (L_0 \oplus L_0{}^*) = 100001$
$(100001 = (output \oplus output^*))$
$[E(L_3) = 10111110] \quad \oplus \quad [E(L_3{}^*) = 00000010] = [10111100] \leftarrow input \oplus input^*$

first 4 bits of $input \oplus input^* = 1011$
first 3 bits of $output \oplus output^* = 100$

Suppose $input = 0000 \rightarrow [S_1] \rightarrow 001 \leftarrow [output]$
$input^* = 1011 \rightarrow [S_1] \rightarrow 010 \leftarrow [output^*]$
$[output] \oplus [output^*] = 011 \leftarrow$ (wrong value, doesn't work)

Let's try $input = 0001 \rightarrow [S_1] \rightarrow 010 \leftarrow [output]$
$input^* = 1010 \rightarrow [S_1] \rightarrow 110 \leftarrow [output^*]$
$[output] \oplus [output^*] = 100 \leftarrow$ (This is what we wanted)

Repeat this for all 16 values of input, we find that only 0001 and 1010 are allowed.