# MATH 314 Spring 2018 - Class Notes

03/26/2018

Scribe:Wei Zhang

**Summary:** Various ways of attacking SDES through Chosen Plaintext Attack.

**Notes:** Differential Cryptanalysis of SDES: is a sort of reverse engineering of the cryptosystem to try to recover the key.

1. Eve is trying to recover $K_3$ -Picks $L_0$ and $R_0$ encrypts then gets $L_3$ and $R_3$
2. Now she picks a new plaintext $L_0^*$ , $R_0^*$,$L_0^*$ can be anything(different from $L_0$), $R_0^* = R_0$(she picks the same right half as the first time)
3. $R_3 = L_2 \oplus f(R_2,K_2)$
4. $R_3 =(L_0 \oplus f(R_0,K_1))+f(R_2,K_3)$
5. $R_3^* = (L_0^* \oplus f(R_0^*,K_1))\oplus f(R_2^*,K_3)$
6. Add together:
   (a) $R_3 \oplus R_3^* = (L_0 \oplus L_0^*) \oplus f(R_2,K_3)\oplus f(R_2^*,K_3)$
7. Eve knows everything is this equation except for $K_3$
8. $(R_3\oplus R_3^*)\oplus(L_0\oplus L_0^*)=f(L_3,K_3)\oplus f(L_3^*,K_3)$
9. Eve does not know what output or output* from number 8. However,Eve does know what output $\oplus$ $ouput^*$ is because it is equal to $(R_3+R_3^*)\oplus(L_0+L_0^*)$
10. $Input = \mathrm{E}(L_3)\oplus K_3$
11. $Input^* = \mathrm{E}(L_3^*)\oplus K_3$
12. $Input\oplus Input^* = \mathrm{E}(L_3)\oplus\mathrm{E}(L_3^*)+(K_3\oplus K_3)$
13. $Input\oplus Input^* = \mathrm{E}(L_3)\oplus\mathrm{E}(L_3^*)$
14. $(K_3\oplus K_3)$ Goes away because of the 'xor' operator which cancels out the same value.
15. Eve knows $Input\oplus Input^*$ and $Output\oplus Output^*$
16. Eve can try possible paris for $Input\oplus Input^*$ that sum to be the right value and see if they give the right $Output\oplus Output^*$

**Example:**

Lets say:

- $L_3 = 101110$
- $(L_3^*) = 000010$
- $(R_3 \oplus R_3) \oplus (L_0 \oplus L_0^*) = 100001$ $(Output \oplus Output^*)$

- $\mathrm{E}(L_3) = 1011110$
- $\mathrm{E}(L_3^*) = 00000010$
- $\mathrm{E}(L_3) \oplus \mathrm{E}(L_3^*) = 101111000$ $(Input \oplus Input^*)$

Try input = 0000

Then $input^* = 1011$

- $001 \oplus 010 = 010 \; ! = 100$

Try input = 0001

Then $input^* = 1010$

- $010 \oplus 110 = 100 = 100$