# MATH 314 - Class Notes

10/17/2017

Scribe: John Wiand

**Summary:** Today's class was based on various ways of attacking SDES such as Chosen Plaintext Attack or differential crytanalysis.

**Notes:** SDES can be attacked through Differential Cryptanalysis. The idea was published in 1990.

The idea:

- Pick a plaintext.
- Split the plaintext into two parts L0, R0.
- Encrypt the plaintext to find R3 and L3.
- Pick new plaintext with a new L0 but the same R0.
- Repeat the process with a new L0 called $L0^*$ and the new R0 called $R0^*$.

$R3 = f(L3, k3)xor(f(R0, k1)xorL0)$ and $R3^* = f(L3^*, k3)xor(f(R0^*, k1)xorL0^*)$. Add both equations together and the result is:

$(L0 + L0^*)xor(R3 + R3^*) = f(L3, k3)xorf(L3^*, k3)$
With the equation, everything will be known besides k3. Working backwards finds k3.

**Examples:**

Lets say:
L3 = 101110
$L3^* = 000010$
E(L3) = 1011/1110
E($L3^*$) = 0000/0010
E(L3) xor E($L3^*$) = 1011/1100
R3 xor $R3^*$ = 100/001
The input into S1 will be 1011 and the output will be 100
Check over all pairs of inputs that sum to 1011 in SBox 1 and see if the output is 100

Input—$Input^*$—S(Input)—S($Input^*$)—output+$output^*$
0000——1011——101————010————111
0001——1010——010————110————100
0010——1001
0011——1000

After finding all the pairs, pick a new value for $L0*$ and discover the new value for $L3^*$ and repeat the process. Eliminating from the pairs already recorded. Continuing to repeat the process until

only one value is left. Repeat the process but use the back half of L3 xor $L3^*$ and R3 xor $R3^*$ and using SBox 2.