MATH 314 - Class Notes

03/30/2017

Scribe: Cyrus Buckman

Summary: Today in class we covered attacking and encrypting DES.

0.1 Attacking DES

I. Chosen Plaintext attack.
Goal:Recover Key
Pick any plaintext $P = (L0, R0)$
2. Encrypt P using an Unknown Key K1,K2,K3
L0 R0
$L1 = R0$ —- $R1 = f(R0, K1) \oplus L0$
$L2 = f(R0, K1) \oplus L1$ — $R2 = f(R1, K2) \oplus L2$
$L3 = f(R1, K2) \oplus L2$ — $R3 = f(R2, K3) \oplus L3$
Recall that $x \oplus y \oplus y = x$
Output is $L3, R3 = f(L3, K3) \oplus f(R0, K1) \oplus L0$ know L0,R0,L3,R3.
3.Encrypt a new plaintext $P* = (L0*, R0*)$ with R0=R0* and $L0! = L0*$ Give us a new L3* and R3*
$R3 = f(L3, K3) \oplus f(R0, K1) \oplus L0$
$R3* = f(L3*, K3) \oplus f(R0*, K1) \oplus L0*$
$R3 \oplus R3* = f(L3, K3) \oplus f(L3*, K3) \oplus L0 + L0*$
At this point we know L0,L0*.R3,R3* and the function F but we still dont know k3
$f(L3, K3)\ f(L3*, K3)$
$E(L3) \oplus K3 \Rightarrow$ input (which splits) S1 and S2 to get an output
$E(L3*) \oplus K3 \Rightarrow$ input* (which splits) S1 and S2 to get an output*.
Dont know input.
If we did then we could solve for K3.
$K3 = input \oplus E(L3)$
input $\oplus$ input* = $(E(L3) \oplus K3) \oplus (E(L3*) \oplus K3) = E(L3) \oplus E(L3*)$ (we know this)
Focus on the first 4 bits know $E(L3) \oplus E(L3*)$ 16 possible bits that could be set to S1(first 4 bits of input). Only 16 pairs of 4 bits that could be the first 4 bits of input and input* for a fixed $E(L3) \oplus E(L3*)$ search over all 16 pairs see if the output of the S-boxes corresponds to the right value of the output