

Class Notes for October 19th

Asim Shrestha

October 25, 2017

Differential Cryptanalysis

Chosen Plain Text

$$P = L_0 + R_0$$

Encrypt Get

$$c = L_3 + R_3$$

Want to find: k_3 All the important secrecy was hidden in the sboxes.

$$P^* = L_0^* + R_0^* \text{ Where } R_0^* = R_0$$

$$C^* = L_3^* + R_3^*$$

Inside the Encryption for P

$$Input \Rightarrow Sbox \Rightarrow Output$$

$$Input^* \Rightarrow Sbox \Rightarrow Output^*$$

We know:

$$input(+)input^* = E(L_3)(+)E(L_3^*)$$

$$output(+)output^* = (R_3(+)R_3^*)(+)(L_3(+)L_3^*)$$

Strateay Search are all paris of possible input/input* compute outputs see if we get the correct value of output (+) output*

$$input = k_3(+)E(L_3)$$

$$input(+)E(L_3)$$

$$L_3 - > E(L_3) - > (+)k_3 - > input$$

DES

- 16 Rounds.
- 8-Sboxes.
- Master key 56 bits (64 with 8 check bits).
- DES starts with an intitial permutation.
- Plain text is 64 bits.

At the very end swap the last L_{16}, R_{16}

Attack DES

Differential Cryptanalysis would be faster than Brute force if DES used only 15 rounds. Else Best attack is Brute force.

In 1990, the Electronic Frontier Foundation built a custom super computer to brute force DES. They could break DES in under a week. (Today: Hours)

So, DES is no longer considered secure. 2^{56} is just not enough to defend against brute force.

Patch DES

Patch DES is doing encryption multiple times. DES is not a group. (It isn't the case for DES, that means $E_{k_1}(E_{k_2}(p)) \neq E_{k_3}(p)$) So, Double encryption with different keys is not Single encryption with a different key.

2-DES is more secure than just DES.

- Pick 2 keys k_1, k_2 .
- Encryption is $E_{k_1}(E_{k_2}(p))$.
- Decryption is $D_{k_1}(D_{k_2}(c))$.

2-DES is vulnerable to meet-in-the-middle attack. Encryption in 2 DES is $C = E_{k_1}(E_{k_2}(p))$

$$D_{k_2}(c) = E_{k_1}(p)$$

Man-in-the-middle is a known plaintext attack, so Eve knows both P and C. Eve creates 2 Tables

$E_{k_1}(p)$		$D_{k_2}(c)$
Every possible k_1 a key	is equal	Every possible k_2 a key

Eve finds every row that appears in both tables.

Eve tries with a new pair p_* and c_* . On average there is 3^{48} pair the first time and the probability of more than one pair existing second time is $\frac{1}{2^{16}}$

Challenge: need to have enough memory to store 2^{56} entries.

2-DES provides 2^{50} effective bits of security.