MATH 314 Spring 2018 - Class Notes

3/29/18

Scribe: Tyler Smith

Summary: Today's class covered the history of DES, including different ways to approach attacking a DES system such as brute forcing and Man in the Middle attacks.

Notes:

DES:

- Plaintext is 64 bits
- Masterkeys are 56 bits
- 16 Rounds
- 8 Sboxes
- Initial permutation (mixes up the order of the bits once right at the beginning)

  This initial permutation made implementation faster on old hardware and serves no cryptographic purpose.

Differential Cyptanalysis was first published in the 80's. This method of attacking DES would only be faster than a brute force attack if DES had 15 or fewer rounds.

Brute force is the only known way to attack DES.

DES is no longer considered secure because 56 bits is not enough security for today's technology.

In the mid 90's, EFF designed a supercomputer just for brute forcing DES. The computer was able to brute force a key in approximately 24 hours.

One solution to this problem was to double encrypt plaintexts using DES since double encrypting with DES is **not** the same as single encrypting with a different key (DES is not a group).

2DES:

Pick two different keys: *k1*, *k2*.

$2DES(P) = E_{k_2}$

Meet in the Middle Attack:

Used against any sort of double encryption.

Encryption is $C = E_{k_2}(E_{k_1}(P))$

Decrypt both sides using k_2

$E_{k_1}(P) = D_{k_2}(C)$

Example: If Eve wants to attack 2DES (known plaintext attack), she knows that:

$$C = 2DES(P)$$

She wants to recover the two keys: k_1 and k_2.

She creates two tables with 2^{56} rows.

All 2^{56} possible encryptions of P	All 2^{56} possible decryptions of C
$E_{k_1}(P)$	$D_{k_2}(C)$

Same entries in each table indicate possible k_1, k_2

She gets a list of possible k_1, k_2 pairs.

Repeat a second time and take the pairs that are valid both times.

If we assume that every encryption or decryption produces approximately a random string of bits then there is a $2^{1/64}$ that any two random binary strings of length 64 are the same.

Since there are total 2^{112} rows, multiplying these things together we expect 2^{48} possible pairs of the first round.

Once Eve does this attack a second time, the probability that any two random strings are the same $2^{1/16}$.

Almost always after performing this twice, Eve will only be left with one possible key pair.

Let's check how much work this is:

She performs 2^{56} operations (Encryptions/Decryptions) to create each table. She creates these tables 4 times.

We must take into account that searching the tables increases her time by another factor of 4.

In total, this requires 2^{60} operations.

Conclusion: 2DES has 60 effective bits of security.