MATH 314 Spring 2018 - Class Notes

3/29/2018

Scribe: Kyle Harris

Summary: In this class we covered the differences between SDES and DES as well as 2DES and Meet-in-The-Middle Attacks. We also touched briefly on 3DES.

Notes:

SDES v.s. DES

DES

- 64-bit plaintexts
- 16 rounds
- 56-bit master keys
- 8 S-Boxes
- Prior to the first round, there is an initial permutation (scrambling of the bits).

SDES

- 12-bit messages
- 3 rounds
- 9 bit master key
- 2 S-Boxes

The initial permutation found in DES doesn't have any cryptographic benefit. It was added by the NSA to increase efficiency on really old machines with only 8-bit registers.

2DES

As we've seen with the SDES system, applying differential cryptanalysis techniques is a viable way of cracking the system. This is not the case with DES. With each round of SDES and DES, the complexity of differential cryptanalysis is almost doubled. The efficiency of differential cryptanalysis would have been faster than brute force techniques if DES only had 15 rounds, but after 16 rounds it became more efficient to brute force the system.

Since DES has 56-bit master keys, there are 2^{56} possible keys. Computing power has advanced to the point where the correct key could be found out of the the 2^{56} possible keys in just a matter of hours via a brute force attack on our most advanced computers. The short key length of DES has made it vulnerable - therefore it is no longer secure.

With the hill cipher we saw that double encrypting a plaintext message didn't increase the security of the system. This is because double encrypting a hill cipher is the same as encrypting it once with a different key! However, these properties of the hill cipher do not apply to DES. Double encryption with DES (2DES) **is not** the same as single encryption with a different key. It actually increases the security of the system to the point where there are 2^{112} possible keys.

Given two keys, (K_1, K_2) and a plaintext, P, 2DES is encrypted as follows:

2DES = $E_{K_2}(E_{K_1}(P))$, where E_{K_n} is a regular DES encryption function.

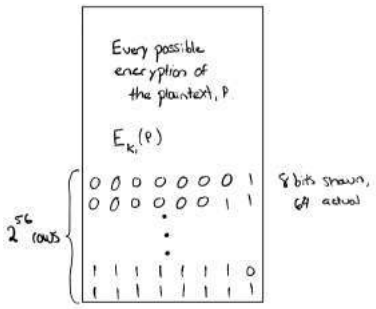
While 2DES dramatically improves the security of DES, it's still insecure. This is because of the "Meet in The Middle" attack.

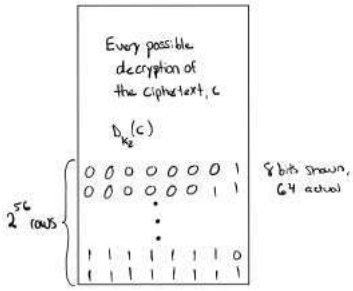
Meet in The Middle Attack

- Useful anytime there is double encryption
- known plaintext attack
- C = $E_{K_2}(E_{K_1}(P))$ (ciphertext double encryption formula)
- attacker knows both C and P and wants to get K_1 and K_2

  In double encryption systems like 2DES the attacker, Eve, knows that $D_{K_2} = E_{K_1}(P)$ - this is sort of the half-way point in double encryption and it's exploited in the attack.

  To conduct the Meet in the Middle attack, eve will produce two big tables. One will contain every possible encryption of the plaintext and the other will contain all the possible decryptions of the ciphertext.





  Eve now will look for all the row that are in both tables. This forms all the possibilities for (K_1, K_2)

  How many pairs would Eve expect?
  Since each row has 64 bits, then there is a $\frac{1}{2^{64}}$ chance that they're the same, given the assumption that each row is a string of random bits. Among the two tables, there are a total of 2^{112} possible rows. The expected number of identical rows is $\frac{1}{2^{64}} * 2^{112} = 2^{48}$. That's a lot of rows, rather than brute forcing this, Eve keeps track of the 2^{48} matching pairs and simply chooses a different plaintext and ciphertext and perform the same

process again. Again she generates large tables of very possible encryption and decryption of the plaintext and ciphertext and keeps track of the matching keys. Eve then checks which of the matching keys from the first set generated tables are contained in the second set of matching keys from the second set of matching tables. If there is a pair in common, there is a good chance it's the key! In fact, there is a $\frac{1}{2^{16}}$ chance that there are matching pairs in the first place. A matching pair occurs because the string of bits in the table are not actually random! They're dependent on the encryption keys.

How much work was the "Meet in the Middle Attack"?

Eve had to create each table which required 2^{56} encryptions/decryptions. She has to create 4 tables which changes the efficiency to 2^{58}. Eve, however still has to search through the tables and find matches, which increases the complexity to 2^{60}. A brute force attack on 2DES required 2^1112 operations, which is not realistic. The meet in the middle attack reduces this to 2^{60} operations, which is doable on modern equipment. This means that 2DES has 60-bits of effective security, which is not much better than 56-bits provided by DES. Triple DES is DES which is encrpyted 3 times and it's not susceptible to meet in the middle attacks. It has an effective security of 112 bits. It's still used sparingly around the web today.