MATH 314 Spring 2018 - Class Notes

10/22/2018

Scribe: Braeden Dorsey

Summary: Today we analyzed how a "Meet-in-the-Middle" attack would work on DES compared to how a brute force attack would, as well as what 3DES is and ideas on how we would encrypt messages longer than 64 bits.

- Meet-in-the-middle attacks work on double-encryptions
- Ciphertext = E_{k_2} (E_{k_2} (Plaintext))
- D_{k_2}(Ciphertext) = E_{k_1}(Plaintext)
- 2 tables: one of all $D_{k_2}(C)$ and one of all $E_{k_1}(P)$
- look for coincidences between these 2 tables

M-i-t-M Attack on DES

- 56 bit keys leads to 2^{56} possible keys.
- 64 bit plaintexts/ciphertexts
- Pretend that the ciphertexts are random (like you flipped a coin)
- Pick an entry from each table. The probability that all are the same is $1/2^{64}$
- There are 2^{112} possible pairs of strings
- expect to find $2^{112} * 2^{-64} = 2^{48}$ coincidences
- now Eve does the attack again w/ a new Ciphertext C' = $E_{k_2}(E_{k_1}(P))$
- Each of the 2^{48} coincidences last time again has a $1/2^{64}$ chance of being all the same
- $2^{48} * 2^{-64} = 2^{-16} = 1/(2^{16})$
- This means you should expect 1 pair to remain, with this one pair being the coincidence from the actual k_1 and k_2
- Eve has to do 2^{56} encryptions to make one of the tables

- 4 tables total makes this number go up to 2^{58} encryptions

- If Eve attempts a brute force attack on DES, she must try 2^{112} encryptions
- DES has 58 bits of "Effective Security"

- Encrypting 3 times makes Meet-in-the-Middle attacks much more difficult
- Ciphertext = $E_{k3}(E_{k2}(E_{k1}(\text{Plaintext})))$
- $D_{k3}(\text{Ciphertext}) = E_{k2}(E_{k1}(\text{Plaintext}))$
- This leads to 2^{112} possibilities
- encrypting 3 times gives 112 bits of "Effective Security"

- 3DES uses 2 keys (k_1 and k_2)
- Ciphertext = $E_{k1}(D_{k2}(E_{k1}(\text{Plaintext})))$
- Plaintext = $D_{k1}(E_{k2}(D_{k1}(\text{Ciphertext})))$
- still used today because, unlike DES it is not considered "broken", but still recommended against.
- mostly used in the financial business

How do we encrypt messages longer than 64 bits?

1. Idea 1: Electronic Codebook
   - We break the plaintext into blocks, and encrypt each block separately
   - The problem with this way is that blocks that are the same will end up as the same ciphertext, allowing Eve to still get an idea of what the message is once one of these similar blocks is cracked
2. Idea 2: Cipher Feedback
   - start with some initial C_0 (can be sent in cleartext)
   - break the message into blocks P_1, P_2, P_3, ...
   - to encrypt : $C_i = E_k(C_{i-1} \text{ XOR } P_i)$
   - to decrypt : $P_i = D(C_i) \text{ XOR } C_{i-1}$
   - unlike with Electronic Codebook, encrypting the same thing produces different ciphertexts every time