MATH 314 Spring 2019 - Class Notes

3/28/2019

Scribe: Megan McCulley

Summary: In today's class we covered several types of modern day encryption systems such as the Electric Code Book, Cipherblock Chaining, Cipher Feedback, Output Feedback, Counter, and DES in the modern era.

0.1 How do you send very large messages in DES?

- Break the plaintext up into blocks
- Encrypt each block one at a time

Different ways to do this called Modes of Operation

0.2 Electronic Code Book (ECB)

Plaintext Blocks $P_1, P_2, P_3 \ldots$
Ciphertext $C_1 = E_k(P_1)$ and $C_2 = E_k(P_2)$

0.3 Cipherblock Chaining (CBC)

- Start with some initial block C_0 (random) sent in cleartext
- Encryption $C_1 = E_k(C_0 \oplus P_1)$ and $C_2 = E_k(C_1 \oplus P_2)$

How do we recover the plaintext?

- $D_k(c_1) \oplus C_0 = P_1$
- $D_k(c_2) \oplus C_1 = P_2$

0.4 Bitwise Addition $\oplus$

M $\oplus$ M = 0000000.....
$\oplus$ undoes itself when you add the same thing twice
$1011 \oplus 1001 = 0010$
$0010 \oplus 1001 = 1011$
We get back to the originial

0.5 Recall: One Time Pad

- key k same length as plaintext
- k- completely random string of 1's and 0's, only used one time
- Encryption: $C = P \oplus K)$ $E_k(P) = P \oplus K$
- Decryption: $P = C \oplus K)$ $D_k(C) = C \oplus K$

0.6 New Idea

Use our encryption algorithm as a way to produce a string of 1's and 0's to encrypt the plaintext int eh same way

0.7 Cipher Feedback (CFB)

- Intial C_0- sent in the clear
- $C_1 = E_k(C_0) \oplus P_1$
- $C_2 = E_k(C_1) \oplus P_2$

Notice that the plaintext isn't encrypted useing our encryption fucntion E_k, instead it is xored with the string of bits produced by it.

0.8 Output Feedback (OFB)

- $O_0 =$ intial string sent in cleartext
- $O_1 = E_k(O_0)$ $C_1 = P_1 \oplus O_1$
- $O_2 = E_k(O_1)$ $C_2 = P_2 \oplus O_2$

Benefit: O_k blocks can be precomputed without knowing the plaintext

0.9 Counter (CTR)

- $O_0 =$ 0000000.... All O's
- $C_i = E_k(O_i) \oplus P_i$
- $O_{i+1} = O_i + 1$ (increment as a number by 1)

0.10 Why isn't DES used today?

- 56 bit keys were secure in 1970, not so much in the late 90's
- Mid 90's, the Electroinic Frontier Foundation (EFF) built a super comupter specifically designed to attack DES (Could brute force a key in a few days)
- DES is not secure, but there is a need to still use it (example: embedded systems)

0.11 Idea: Double Encrypt

- Unlike other ciphers, encrypting twice is not the same as single encryption with a different key
- DES 2x
- two keys (k_1, k_2)
- $C = E_{k_2}[E_{k_1}(P)]$
- $P = D_{k_1}[D_{k_2}(C)]$

0.12 Disadvantages of Double Encrypt

- Double encryption is vulnerable to meet-in-the-middle-attack
- because $C = E_{k_2}[E_{k_1}(P)]$ and $P = D_{k_1}[D_{k_2}(C)]$
- To be continues next class....