MATH 314 Fall 2019 - Class Notes

10/12/2019

Scribe: Jacob M. Smedley

Summary: Modes of Operation - Cipher Feedback, Output Feedback, and Counter; Double Encrypted DES

Notes:

- One-time-pad
  - Encryption occurs by adding the plaintext to a completely random key k
  - $C = P \oplus k$ - Encryption with one-time-pad
- Other modes of operation "mimic" the one-time-pad
  - Use Encryption function as a random number generator to produce a "key" like in the one-time-pad
- Cipher Feedback (CFB)
  - C_0 = random string sent unencrypted (cleartext)
  - Encryption (CFB)
    - $C_1 = E_k(C_0) \oplus P_1$
    - $C_2 = E_k(C_1) \oplus P_2$
    - $\underline{C_i = E_k(C_{i-1}) \oplus P_i}$
  - Decryption of CFB
    - Bob wants to decrypt messages sent using CFB
    - He knows C_0, C_1; goal: recover P_1
    - He computes $E_k(C_0)$
    - $C_1 \oplus E_k(C_0) = P_1$
    - $\underline{P_i = E_k(C_{i-1}) \oplus C_i}$
- Output Feedback (OFB)
  - Pick a random O_0 sent in cleartext
  - Encryption
    - $O_1 = E_k(O_0)$
    - $C_1 = P_1 \oplus O_1$
    - $O_2 = E_k(O_1)$

        * $C_2 = P_2 \oplus O_2$
        * $\underline{O_i = E_k(O_{i-1})}$
        * $\underline{C_i = O_i \oplus P_i}$
    - Decryption
        * $\underline{O_i = E_k(O_{i-1})}$
        * $\underline{P_i = C_i \oplus O_i}$

- Counter (CTR)
    - X_0 = All 0's (or random)
    - $X_i = X_{i-1}$ incremented by 1
    - Encryption
        * $\underline{C_i = P_i \oplus E_k(X_i)}$
    - Decryption
        * $\underline{P_i = C_i \oplus E_k(X_i)}$

- 2DES
    - By the mid-90s DES was no longer secure
    - 56-bit keys (2^{56} possible keys) were within the realm of brute force
    - Unlike previous ciphers double encryption is not the same as single encryption with a different key
    - $E_{k_2}(E_{k_1}(P)) \neq E_{k_3}(P)$
    - Double encryption is vulnerable to a meet-in-the-middle attack
        * Known Plaintext Attack
        * Alice and Bob are using double encryption with keys k_1 and k_2
        * Eve can brute force attack single encryption but not double encryption
        * She learns that $C = E_{k_2}(E_{k_1}(P))$
            · Decrypt both sides: $D_{k_2}(C) = E_{k_1}(P)$
        * (P, C) are a plaintext and corresponding ciphertext
        * Goal: Find k_1 and k_2
        * Eve creates two tables
        * Table 1:
            · All possible encryptions of P
            · $E_{k_1}(P)$ for every k_1
        * Table 2:
            · All possible decryptions of C

- $\cdot$ $D_{k_2}(C)$ for every k_2
* She finds all possible matches in both tables
* Repeats with a new P' and C'
* Checks each of the matches from (P, C)
* Odds are that only one pair k_1 and k_2 will work