MATH 314 Fall 2023 - Class Notes

10/12/2023

Scribe:John Roell

Summary: Other Forms Of Multi-Block SAES Encryption.

$\oplus$

Notes: Symbols used

- C_i = blocks of encrypted/Cipher text
- X_i = blocks of plain text
- IV = Initial Value
- $E_k(X_i)$ = the encryption of X_i
- $D_k(C_i)$ = the decryption of Cipher text

I. Modes of Opertation

1. Electronic Code Book (ECB)
   A. Encryption
   Formula: $C_1 = E_k(X_1)$
   B. Dencryption
   Formula: $X_1 = D_k(C_1)$

2. Cipher Block Chaining (CBC)
   A. Encryption
   Formulas:
   $IV = C_0$
   $C_i = E_k(X_i \oplus \mathrm{C}_{i-1}) \rightarrow C_1 = E_k(X_1 \oplus \mathrm{C}_0) \rightarrow C_2 = E_k(X_2 \oplus \mathrm{C}_1)...$
   B. Dencryption
   Formula:
   $D_k(C_1) = X_1 \oplus \mathrm{C}_0 \rightarrow X_1 = D_k(C_1) \oplus \mathrm{C}_0 \rightarrow X_i = D_k(C_i) \oplus \mathrm{C}_{i-1}$

3. Cipher Feed Back(CFB)
   A. Encryption
   Formulas:
   $IV = C_0$
   $C_i = E_k(C_{i-1}) \oplus \mathrm{X}_i \rightarrow C_1 = E_k(C_0) \oplus \mathrm{X}_1$
   B. Dencryption
   Formula:
   $X_i = E_k(C_{i-1}) \oplus \mathrm{C}_i$

4. Output Feed Back(OFB)
   A. Encryption
   Formulas:
   $IV = O_0$
   $O_i = E_k(O_{i-1})$
   $C_i = X_i \oplus \mathrm{O}_i$
   B. Dencryption
   Formula:
   $X_i = C_{i-1} \oplus \mathrm{O}_i$

5. Counter (CTR)
   A. Encryption
   Formulas:
   $IV = CTR_0$
   $CTR_i = CTR_{i-1} + 1 \mod 2$

   1 increases by 1 for every subsequent blocks encrypted IE block 26 would make 1 increase to 26

   $CTR_i = CTR_{i-1} + i$

   $+i$ is added as a binary number with normal binary addition rules 5 becomes 0101 so on

   $C_i = E_k(CTR_i) \oplus \mathrm{X}_i$
   B. Dencryption
   Formula:
   $X_i = E_k(CTR_i) \oplus \mathrm{C}_i$