MATH 314 Fall 2023 - Mode of Operation Class Notes

10/10/2023

Scribe: Oreoluwa Williams

Summary: In today's class we covered the five(5) Modes of Operation and how we encrypt and decrypt each.

Notes: We encrypt multiple blocks with a block cipher by using Modes of Operation.

- $BlocksofPlaintext X_1, x_2, ...$
- $EncrpytionFunctionandakey E_K(X)$
- $DecrpytionFunctionis D_K(Y)$

1. **Electronic Codebook (ECB)**

   Each block is encrypted or decrypted separately using the encryption and decryption functions.

   $C_1 = E_K(X_1)$

   $C_2 = E_K(X_2)$

   Encryption Function: $C_i = E_K(X_i)$

   Decryption Function: $X_i = D_K(C_i)$

2. **Cipher Block Chaining (CBC)**

   Pick an initial value IV

   $C_0 = IV$

   $C_1 = E_K(X \oplus C_0)$

   $C_2 = E_K(X \oplus C_1)$

   Encryption Function: $C_i = E_K(Xi \oplus C_{i-1})$

   How to decrypt CBC?

   Bob knows $C_0, C_1, C_2 and K$

   $D_K(C_1) = X_1 \oplus C_0$

   $X_1(D_K) = C_1 \oplus C_0$

   $X_2(D_K) = C_2 \oplus C_0$

   Decryption Function: $X_i = D_K(C_i) \oplus C_{i-1}$

Other modes of operation use the encryption function as a random number generator.

Xor with the plaintext to get the ciphertext.

Never use the decryption function.

3. **Cipher Feedback (CFB)**

   $C_0 = IV$

   $C_1 = E_K(C_0) \oplus X_1$

   $C_2 = E_K(C_2) \oplus X_2$

   Encryption Function: $C_i = E_K(C_{i-1}) \oplus X_i$

   Decryption Function: $X_i = E_K(C_{I-1}) \oplus C_1$

4. **Output Feedback (OFB)**

   $O_0 = IV$

   $O_1 = E_K(O_0)$

   $C_1 = X_1 \oplus O_1$

   $O_2 = E_K(O_1)$

   $C_2 = X_1 \oplus O_2$

   $O_i = E_K(O_{i-1})$

   Encryption Function: $C_i = X_i \oplus O_i$

   Decryption Function: $X_i = C_I \oplus O_i$

5. **Counter (CTR)**

   $CTR_0 = IV$

   $CTR_1 = CTR_0 + 1 \pmod 2^{blocksize}$

   $CTR_i = CTR_{i-1} + 1 \pmod 2^{blocksize}$

   $= CTR_0 + i \pmod 2^{blocksize}$

   Encryption Function: $C_i = E_K(CTR_i) \oplus X_i$

   Decryption Function: $X_i = E_k(CTR_i) \oplus C_i$