BLOCK CIPHER TECHNIQUE

Kriptografi - Week 9

Aisyatul Karima, 2012
1. Block Cipher Technique
2. Mode Electronic Code Book (ECB)
3. Cipher Block Chaining (CBC)
A block cipher algorithm is a basic building block for providing data security.

Plaintext bits divided by bit block with the same length.

Use the block cipher, the same plaintext block will encrypt become the same ciphertext block if use the same key.

Block cipher algorithm combine some classic cryptography on encryption process.
Teknik Block Cipher

- Classic cryptography technique that used are:
  - Substitution
  - Transposition
  - Expansion
  - Compresion
Teknik Block Cipher

- Cipher Blok operation mode:
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFC)
  - Output Feedback (OFB)
Electronic Code Book (ECB)

- In this technique, each plaintext block will be encrypted individually and independently.
- In mathematics, **ECB** encryption is:
  \[ C_i = E_K(P_i) \]
- Decryption process
  \[ P_i = D_K(C_i) \]
Electronic Code Book (ECB)

- Encryption and decryption schema with ECB:
Example:

The plaintext on biner is

- 10100010001110101001

Divide the plaintext into the blocks size 4 bit:

- 1010 0010 0011 1010 1001

On hexa = .... ?
Electronic Code Book (ECB)

- For the example the **Key (K)** that used is has the length 4 bit
  - 1011 = on hexadecimal is... ??
- For the example the simple encryption E is XOR process between plaintext $P_i$ with $K$,
- Then wrapping the bit from $P_i \oplus K$ one position to the left.
**Electronic Code Book (ECB)**

- **Encryption process**:  
  
  \[
  \begin{align*}
  1010 & \ 0010 \ 0011 \ 1010 \ 1001 \\
  1011 & \ 1011 \ 1011 \ 1011 \ \oplus \\
  \end{align*}
  \]

  **Result XOR**

  \[
  \begin{align*}
  \text{...} & \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \\
  \end{align*}
  \]

  **wrap 1 bit to the left**

  \[
  \begin{align*}
  \text{...} & \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \\
  \end{align*}
  \]

  **on hexadecimal**

  \[
  \begin{align*}
  \text{...} & \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \ \text{...} \\
  \end{align*}
  \]

  **encryption result = .... ???**
Electronic Code Book (ECB)

- **Note:**
  - The *same plaintext* block always encrypted become the *same ciphertext* block.
  - Based on the example, block 1010 appear twice and always encrypted into 0010.
The word “code book” on ECB appear from the fact which the same block plaintext always encrypted into the same block ciphertext.

Theoretically, it cause make the plaintext code book and cipher text which correspondently.
Electronic Code Book (ECB)

- However, higher the block size is higher the code book size.
- For the example if the block has 64 bit, then the code book consist of $2^{64} - 1$ code. It means so many large to save.
Electronic Code Book (ECB)

- The **advantages** of ECB:
  - We do not need encrypt the file linearly because each block plaintext **encrypted independently**.
  - If one or more the bit on block ciphertext is failed, then the fault only influence the ciphertext on decryption process.
The weaknesses of ECB:

- The result of encryption process produce the **same block ciphertext** because the plaintext is often repeat.
- The opposite site can **manipulate** the ciphertext to lie the recipient message.
Cipher Block Chaining (CBC)

- This technique implements the feedback mechanism on a block.
- The result in previous encryption will feed back into the current block encryption.
- The way is current block plaintext is XOR with the result of the previous encryption block ciphertext.
- Then the XOR result is entry into the encryption function.
with CBC, each block ciphertext depend on all of previous block plaintext.

Decryption process with insert the current block ciphertext into the decryption function, then the result is XOR with the previous block ciphertext.

In this case, the previous block ciphertext as the feed forward at the end of decryption process.
Cipher Block Chaining (CBC)

- Encryption & decryption schema with CBC
Mathematically, the **CBC** encryption mode as

\[ C_i = E_K(P_i \oplus C_{i-1}) \]

And decryption as

\[ P_i = D_K(C_i) \oplus C_{i-1} \]

The first block plaintext use \( C_0 \) as the first vektor (*initialization vector* or IV).

IV does not need to be secret.
Cipher Block Chaining (CBC)

- Identical block plaintext is encrypted into different block ciphertext only if the previous block plaintext is different.
- If there is same the previous block plaintext, then there is possible the same ciphertext.
- To prevent this case, then used IV which random data as first block. IV is does not the meaning, it just used to make the block ciphertext is unique.
Cipher Block Chaining (CBC)

- **Plaintext**: 10100010001110101001
- **Divided** the plaintext into the 4 bit block:
  - 1010 0010 0011 1010 1001
  - hexadecimal = ?
- For the example the **Key (K)** that used is 4 bit
  - 1011 = hexadecimal... ?
- **IV** that used is all bit 0 (So, \( C_0 = 0000 \))
Cipher Block Chaining (CBC)

- For the example the simple encryption $E$ is XOR between the plaintext $P_i$ with $K$,

- Then slide it use the wrapping bits of $P_i \oplus K$ one position to the left.
Cipher Block Chaining (CBC)

- $C_1$ is obtains as follows:
  - $P_1 \oplus C_0 = 1010 \oplus 0000 = 1010$
  - Encrypt this result with the E function:
    \[
    1010 \oplus K = 1010 \oplus 1011 = 0001
    \]
  - wrapping this result one bit to the left: 0010
  - So, $C_1 = 0010$ in hexadecimal is .... ?

- $C_2 = ...??$
- $C_3 = ...??$
And so on, so the result of plaintext and ciphertext are:

- Plaintext: A23A9
- Ciphertext (mode ECB): 23124
- Ciphertext (mode CBC): 27FDF
Cipher Block Chaining (CBC)

- **Error propagation:**
  - A single bit error in a block of plaintext will propagate the corresponding ciphertext blocks.
  - However, this is contrary to the decryption process. A single bit error in the ciphertext block affects only the corresponding plaintext block and a bit on the next plaintext block.
  - Ciphertext bit error usually occurs due to interference (noise) data communications channel during a malfunction in the transmission or storage media.
Cipher Block Chaining (CBC)

- **Security issues on CBC**
  - Because the ciphertext block affects the next blocks, the opponent can add extra ciphertext block at the end of the encrypted message without being detected.
  - Opposing party can change the ciphertext, such as changing a bit in a block of ciphertext. But this only affects the result of the decryption plaintext block and a bit keslahan the next plaintext position.