Encrypting a large message

Cipher Block Chaining (CBC)  IV is a random number

Block Cipher

message

m1  m2  m3  m4  m5  m6

c1  c2  c3  c4  c5  c6

IV ⊕ Secret E E E E E E
Block Cipher

Decrypting a large message

Cipher Block Chaining (CBC)  IV is a random number

\[ \text{message} \]

\[ \begin{align*}
    m_1 & \quad m_2 & \quad m_3 & \quad m_4 & \quad m_5 & \quad m_6 \\
    c_1 & \quad c_2 & \quad c_3 & \quad c_4 & \quad c_5 & \quad c_6 \\
\end{align*} \]

IV \rightarrow \oplus \quad m_1 \quad \oplus \quad m_2 \quad \oplus \quad m_3 \quad \oplus \quad m_4 \quad \oplus \quad m_5 \quad \oplus \quad m_6

Secret \rightarrow D \quad m_1 \quad D \quad m_2 \quad D \quad m_3 \quad D \quad m_4 \quad D \quad m_5 \quad D \quad m_6

\[ \text{D} \]

\[ \text{D} \]

\[ \text{D} \]

\[ \text{D} \]

\[ \text{D} \]

\[ \text{D} \]
Block Cipher

En/Decrypting a large message

Cipher Block Chaining (CBC)

**Discussion:**

1. Must use random IV – guarantees that same plaintext causes different ciphertext
   If IV is not random, information is revealed even if message not decrypted

**Examples:**
   Commander orders troops to hold several times then attack
   If salary fields are known, can determine whose salary has changed

**Benefit:**
   attackers cannot supply chosen plaintext to the encryption algorithm itself, even if chosen plaintext can be supplied to the CBC
Block Cipher

En/Decrypting a large message

Cipher Block Chaining (CBC)

Discussion:

1. Must use random IV – guarantees that same plaintext causes different ciphertext
   If IV is not random, information is revealed even if message not decrypted

   Examples:
   Commander orders troops to hold several times then attack
   If salary fields are known, can determine whose salary has changed

   Benefit:
   attackers cannot supply chosen plaintext to the encryption algorithm itself, even if chosen plaintext can be supplied to the CBC

2. Attacker can rearrange blocks with predictable effect on resulting plaintext.
   Changing \( c_i \) has a predictable effect on \( m_{i+1} \). Might decrypt to this:

   | Hello | 7834 | → | &8*# | 7835 |
Block Cipher

En/Decryption of a large message

Cipher Block Chaining (CBC)

Discussion:

1. Must use random IV – guarantees that same plaintext causes different ciphertext.
   If IV is not random, information is revealed even if message not decrypted.

   Examples:
   - Commander orders troops to hold several times then attack.
   - If salary fields are known, can determine whose salary has changed.

   Benefit:
   - Attackers cannot supply chosen plaintext to the encryption algorithm itself, even if chosen plaintext can be supplied to the CBC.

2. Attacker can rearrange blocks with predictable effect on resulting plaintext.
   Changing $c_i$ has a predictable effect on $m_{i+1}$. Might decrypt to this:

   \[
   \begin{array}{cc}
   \text{Hello} & 7834 \\
   \rightarrow & \text{&8*#} & 7835
   \end{array}
   \]

3. If $m_1...m_n$ and $c_1...c_n$ and IV are known, all decryptions of $c_i$ are known.
   If enough of these are obtained, a new ciphertext can be constructed and the decrypt would be known.
Generating Message Integrity Check (MIC)

Suppose message is sent in the clear

Only send the residue as the check on the ciphertext and the plaintext message (no confidentiality)
Generating Message Integrity Check (MIC)

Integrity plus confidentiality

Huh? Send last block twice? Tamperer merely sends tampered message and just repeats its last block!!
Generating Message Integrity Check (MIC)

To use CBC for both message integrity and encryption, use different keys for the residue and ciphertext!