Block cipher and modes of encryptions
Block cipher

• Other name for fixed-length encryption scheme
Problem with just encrypting each block of the message using a randomized encryption scheme

• Each block uses $k$ bits of randomness
  • If we have $d$ blocks, it requires $dk$ bits of randomness.

• Randomness is expensive
Solution to minimize randomness

- Create an initial state
  - May use some randomness (called Nonce or IV).

- Encrypt the current block using the current state

- Update the state after each use of the block cipher
Goals (block cipher)

• Security
  • Is it secure?
  • What level of security does it have?

• Parallelizable: Can we encrypt/decrypt each block in parallel
  • We don’t need to wait for the previous part to encrypt the next part.

• Forward: Do we need to use decryption operation
  • Better if we don’t

• Error-resilient: If one block of the ciphertext becomes corrupted
ECB mode

- \textit{Init}()
  - \( S_1 \leftarrow 0 \)

- \textit{Output}(m_i, S_i)
  - \( c_i \leftarrow Enc_k(m_i) \)

- \textit{Update}(m_i, s_i)
  - \( S_{i+1} \leftarrow S_i \)
Electronic codebook mode (ECB)
Electronic codebook mode (ECB)

Electronic Codebook (ECB) mode encryption

<table>
<thead>
<tr>
<th>Secure?</th>
<th>Parallelizable</th>
<th>Forward</th>
<th>Error-resilient</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Unless the plaintext has high entropy.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Problem with ECB mode
Counter mode (CM)

• *Init*()
  • \(\text{nonce} \in_R \{0,1\}^{s/2}\)
  • \(S_1 \leftarrow (\text{nonce}, \{0\}^{s/2})\)

• *Output*(\(m_i, S_i\))
  • \(c_i \leftarrow \text{Enc}_k(S_i) \oplus m_i\)

• *Update*(\(m_i, s_i\))
  • \(s_{i+1} \leftarrow s_i + 1\)
Counter mode (CM)
Counter mode

Counter (CTR) mode encryption

<table>
<thead>
<tr>
<th>Secure?</th>
<th>Parallelizable</th>
<th>Forward</th>
<th>Error-resilient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes but</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>IV security reduced by half</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cipher block chaining

• *Init*()
  • $IV \in \mathbb{R} \{0,1\}^s$
  • $S_1 \leftarrow IV$

• *Output*$(m_i, S_i)$
  • $c_i \leftarrow Enc_k(m_i \oplus S_i)$

• *Update*$(m_i, s_i)$
  • $s_{i+1} \leftarrow c_i$
Cipher block chaining (CBC)
Cipher block chaining

Cipher Block Chaining (CBC) mode encryption

<table>
<thead>
<tr>
<th>Secure?</th>
<th>Parallelizable</th>
<th>Forward</th>
<th>Error-resilient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>