Encrypting with Block Ciphers

BİL 448/548
Internet Security Protocols
Ali Aydın Selçuk
How to Encrypt with a Block Cipher?

Electronic Codebook (ECB) Mode:

• The naive way.

• The plaintext is divided into blocks $P_i$ , each block is encrypted independently:
  
  $$C_i = E(P_i)$$
  $$P_i = D(C_i)$$

• Problem: Leaks information about identical blocks
An Illustration – The Plaintext
An Illustration – ECB Encrypted
Cipher Block Chaining (CBC)

• Add randomization to the plaintext by mixing with the previous ciphertext:
  \[ C_i = E(P_i \oplus C_{i-1}) \]
  \[ P_i = D(C_i) \oplus C_{i-1} \]

• Initialization Vector (IV): used instead of \( C_0 \) when encrypting/decrypting the first block.
  (not a secret)

• Most common mode in practice

• Features:
  – Error propagation: 1 wrong bit corrupts 1 block + 1 bit
  – Allows random access to the ciphertext
  – Decryption is parallelizable
An Illustration – CBC Encrypted
Output Feedback (OFB) Mode

• Block cipher is used as the PRNG in a stream cipher.
• A key stream is generated from the output:
  \[ O_i = E(O_{i-1}) \]
  \[ C_i = P_i \oplus O_i \]
  \[ P_i = C_i \oplus O_i \]
• IV used for \( O_0 \)
• Features:
  – Error propagation minimal (bit for bit)
  – Preprocessing possible (may be good for multimedia)
  – Doesn’t allow random access; not parallelizable
Cipher Feedback (CFB) Mode

• A key stream is generated from the ciphertext:
  \[ O_i = E(C_{i-1}) \]
  \[ C_i = P_i \oplus O_i \]
  \[ P_i = C_i \oplus O_i \]

• IV used for \( C_0 \)

• Features:
  – Error propagation: 1 bit + 1 block
  – Allows random access
  – Decryption is parallelizable
Counter (CTR) Mode

- A key stream is generated by encrypting a counter:
  \[ C_i = P_i \oplus E(IV + i - 1) \]
  \[ P_i = C_i \oplus E(IV + i - 1) \]

- Features:
  - Error propagation minimal (bit for bit)
  - Preprocessing possible
  - Allows random access
  - Both encryption and decryption are parallelizable