Block Cipher Modes
ECB Mode

- Electronic Code Book
- Divide the plaintext into fixed-size blocks
- Encrypt/Decrypt each block independently
- There is a weakness with this approach
Electronic Codebook (ECB) mode encryption

Electronic Codebook (ECB) mode decryption
CBC Mode

- Cipher Block Chaining
- Overcomes the problem with ECB
- XOR the plaintext with the prior ciphertext block
- What about the first block?
Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption
Figure 2.7 Cipher Block Chaining (CBC) Mode
Initialization Vector (IV)

- Must be known to both the sender and recipient
- Ideally both IV and key should be protected, but the IV may be public
- Common approach: encrypt IV using ECB and send it with the encrypted data
- Most importantly, an IV should never be reused with the same key. Why?
  - What happens if we have two plaintext message with the same prefix? How will the ciphertexts compare?
Block Cipher as a Stream Cipher

- The following modes create a stream cipher from a block cipher. How is it done?
- Three modes
  - Counter Mode (CTR)
  - Cipher Feedback Mode (CFB)
  - Output Feedback Mode (OFB)
Counter (CTR) mode encryption

Counter (CTR) mode decryption
Cipher Feedback (CFB) mode encryption

Cipher Feedback (CFB) mode decryption
Output Feedback (OFB) mode encryption

Output Feedback (OFB) mode decryption
Homework 3

• Comparison of these modes
• Summative – we will grade for correctness
• Contrived scenario to illustrate why the IV should not be reused
Summary

- **ECB**
  - Simple
  - Don’t have to create/manage an IV
  - Parallel encryption/decryption
  - Reveals patterns in the plaintext – should not use

- **CBC**
  - Conceals plaintext patterns
  - Requires sequential encryption
  - Parallel decryption
Summary

• Block cipher as stream cipher
  o No need for padding
  o Only have to implement encrypt function

• CTR
  o Parallel encryption/decryption
  o Preprocessing able to generate the keystream in advance

• CFB
  o Parallel decryption

• OFB
  o Preprocessing able to generate the keystream in advance
Authenticated Encryption Modes
• Symmetric encryption offers confidentiality, but not integrity and authenticity
  o HW 3 – bit flipping attacks
• More recent block cipher modes offer both
• Authenticated Encryption with Associated Data (AEAD)
  o EAX Mode
    https://en.wikipedia.org/wiki/EAX_mode
  o GCM (Galois Counter Mode)
    https://en.wikipedia.org/wiki/Galois/Counter_Mode
Encrypt-then-MAC (EtM)

- IPSec
- TLS/DTLS
- SSHv2
Encrypt-and-MAC (E&M)

- SSH
MAC-then-Encrypt (MtE)

- SSL/TLS
EAX Mode

Algorithm EAX.Encrypt_{K}^{N,H} (M)
10 \( N \leftarrow \text{OMAC}_{K}^{N,H}(N) \)
11 \( \mathcal{K} \leftarrow \text{OMAC}_{K}^{N,H}(H) \)
12 \( C \leftarrow \text{CTR}_{K}^{N,H}(M) \)
13 \( \mathcal{E} \leftarrow \text{OMAC}_{K}^{C,H}(C) \)
14 \( \text{Tag} \leftarrow N \oplus \mathcal{E} \oplus \mathcal{K} \)
15 \( T \leftarrow \text{Tag} \) [first \( \tau \) bits]
16 return \( CT \leftarrow C \parallel T \)

Algorithm EAX.Decrypt_{K}^{N,H} (CT)
20 if \( |CT| < \tau \) then return INVALID
21 Let \( C \parallel T \leftarrow CT \) where \( |T| = \tau \)
22 \( N \leftarrow \text{OMAC}_{K}^{N,H}(N) \)
23 \( \mathcal{K} \leftarrow \text{OMAC}_{K}^{N,H}(H) \)
24 \( \mathcal{E} \leftarrow \text{OMAC}_{K}^{C,H}(C) \)
25 \( \text{Tag'} \leftarrow N \oplus \mathcal{E} \oplus \mathcal{K} \)
26 \( T' \leftarrow \text{Tag'} \) [first \( \tau \) bits]
27 if \( T \neq T' \) then return INVALID
28 \( M \leftarrow \text{CTR}_{K}^{N,H}(C) \)
29 return \( M \)
GCM Mode

- TLS
- SSH
- IPSec
- OpenVPN
Padding
Block Ciphers & Padding

• Block ciphers require that the plaintext be a multiple of the block size (ECB and CBC modes)

• Padding is used to make sure that all blocks are “full”

• Both sides need to know the padding scheme
Padding Schemes

- Pad with bytes all of the same value as the number of padding bytes
- Pad with 0x80 followed by 0x00 characters
- Pad with 0x00 characters
  - Last byte is equal to the number of padding bytes
  - Pad with spaces
- Pad with 0x00 characters or spaces
  - Assuming these values don’t appear at the end of the actual data
- Short one-block messages in ECB mode will all encrypt the same with the same key – use random padding

Other Uses for Padding?

- **Disguise identical messages**
  - Identical messages encrypted with the same key will always produce the same ciphertext (assumes no IV, such as ECB mode)

- **Disguise message length**
  - Pad the message with a random number of bytes to create a random-sized messages
  - All messages are padded to a preset length

- **When is padding not required?**
  - When the plaintext is always a multiple of the block size and both sides agree not to include padding