Encryption Modes of Operation

COMP620

Difficulties with Block Encryption

• Two identical blocks of plaintext will be encrypted to two identical blocks of ciphertext.

original image  encrypted with ECB

Electronic codebook (ECB) Mode

• Data are divided into blocks which are encrypted separately.

Cipher-block Chaining (CBC) Mode

• Each block of ciphertext is XOR with the next block of plaintext before encryption.
• Note that a one-bit change in a plaintext block affects all following ciphertext blocks.

Cipher Block Chaining (CBC) mode encryption
Cipher-block Chaining Decryption

Decryption requires only the previous block of ciphertext, so it can be parallelized

Initialization Vector

- The initialization vector (IV) is like dummy ciphertext to start the process
- The IV does not have to be secret
- The IV should be a random value
- By using a different IV every time you encrypt a message, identical messages will encrypt to different ciphertext
- The IV should be protected with a MAC to maintain message integrity

Cipher Feedback (CFB) Mode

- The IV is encrypted to create a “random” stream of bits that are XOR with the plaintext

Cipher Feedback Decryption

- CFB decryption uses the encryption algorithm, not the decryption algorithm
And More

- There are several other encryption modes that are used.
- The initialization vector needs to be kept with the ciphertext.
- Adding the IV makes the ciphertext a little larger than the plaintext. This could be a problem in some situations.