Security of Information Systems
Bezpieczeństwo systemów informacyjnych

Piotr Pacyna
pacyna@kt.agh.edu.pl
Lecture
Modes of operation for block ciphers

Piotr Pacyna
pacyna@kt.agh.edu.pl
Encrypting large volume of data
Mode of operation

- A block cipher works on data units of some fixed size (known as a *block size*).
- A block cipher by itself allows encryption of a single data block only.
  - Key replacement should take place after encryption of a single data block.
- In a block cipher, the length of the data block must match the length of the cipher's block.
  - Long messages must be segmented into blocks.

*Mode of operation* is the procedure of enabling the repeated and secure use of a block cipher under a single key.
A mode of operation:

- describes the process of encrypting multiple data blocks,
- uses additional input for randomization to encrypt safely.
- The extra input value is an initialization vector

See also:
• An initialization vector (IV) is a block of bits used by some ‘modes’ to randomize the encryption

• Initialization vector allows to produce distinct ciphertexts, even if the same plaintext is encrypted multiple times

☞ There is no need for a key replacement (no re-keying)
☞ IV is sometimes called a starting variable
The message is divided into blocks.
Each block is encrypted separately.

**Disadvantage:**
- identical plaintext blocks are encrypted into identical ciphertext blocks
- doesn't provide serious message confidentiality,
- not recommended for use in cryptographic protocols at all.
Cipher Block Chaining mode (CBC)

CBC is one of the many modes of operation that can be applied to a general block cipher,

It is not tied specifically to DES or AES.

In CBC mode, each block of plaintext is XOR with the previous ciphertext block before being encrypted.

**Advantage:**
- Each ciphertext block depends on all plaintext blocks processed up to that point.
- To make each message unique, an initialization vector must be used in the first block.
Comments on Cipher Block Chaining

Its main drawbacks are:

- encryption is sequential (i.e., it cannot be parallelized),
- message must be padded to a multiple of the cipher block size.

Note well that:

- a one-bit change in a plaintext or IV affects all following ciphertext blocks.
- one-bit change to the ciphertext causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact.
- decrypting with the incorrect IV causes the first block of plaintext to be corrupt but subsequent plaintext blocks will be correct (this is because a plaintext block can be recovered from two adjacent blocks of ciphertext). As a consequence, decryption can be parallelized.
**Cipher Feedback mode (CFB)**

The *cipher feedback* (CFB) mode, makes a block cipher into a self-synchronizing stream cipher.

- Operation is similar to CBC
The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. OFB generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.
Output Feedback (OFB)

OFB generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher.

Advantage:
End of lecture