Introduction to Cryptography
Lecture 12

Monika K. Polak

March 11, 2021

Encryption with Block Ciphers: Modes of Operation

- Electronic Code Book mode (ECB)
- Cipher Block Chaining mode (CBC)
- Output Feedback mode (OFB)
- Cipher Feedback mode (CFB)
- Counter mode (CTR)

Block Ciphers

- A block cipher is much more than just an encryption algorithm, it can be used ...
  - to build different types of block-based encryption schemes
  - to realize stream ciphers
  - to construct hash functions
  - to make message authentication codes
  - to build key establishment protocols
  - to make a pseudo-random number generator
  - ...

Encryption with Block Ciphers

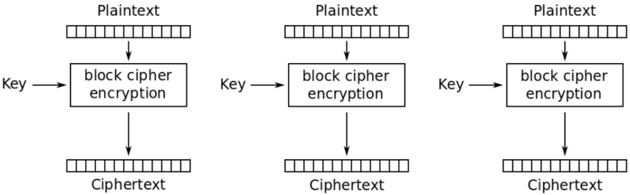
- There are several ways of encrypting long plaintexts, e.g., an e-mail or a computer file, with a block cipher ("modes of operation")
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - Output Feedback mode (OFB)
  - Cipher Feedback mode (CFB)
  - Counter mode (CTR)
  - Galois Counter Mode (GCM)

Electronic Code Book mode (ECB)

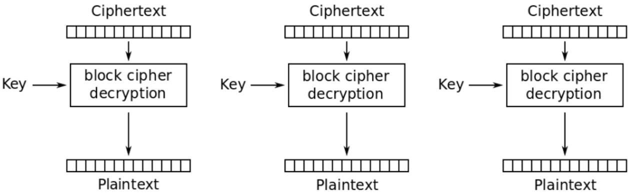
- The simplest of the encryption modes
- Messages which exceed *b* bits are partitioned into *b*-bit blocks
- Each Block is encrypted `separately`

In case the plaintext message's length is not a multiple of the block size we add `padding` (extra padding bits after the last plaintext bit).

Electronic Code Book mode (ECB)



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

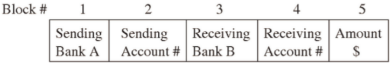
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Electronic Code Book mode (ECB)

- Advantages
  - no block synchronization between sender and receiver is required
  - bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Block cipher operating can be parallelized
  - advantage for high-speed implementations
- Disadvantages
  - ECB encrypts highly deterministically
  - identical plaintexts result in identical ciphertexts
  - an attacker recognizes if the same message has been sent twice
  - plaintext blocks are encrypted independently of previous blocks
  - an attacker may reorder ciphertext blocks which results in valid plaintext

Substitution Attack on ECB

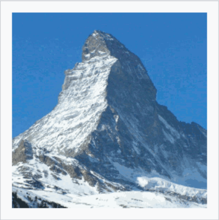
- Once a particular plaintext to ciphertext block mapping $x_i \rightarrow y_i$ is known, a sequence of ciphertext blocks can easily be manipulated
- Consider an electronic bank transfer

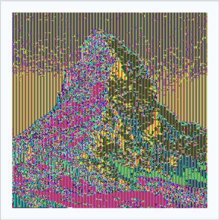


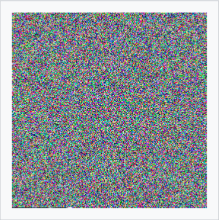
Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

  - the encryption key between the two banks does not change too frequently
  - The attacker sends $1.00 transfers from his account at bank A to his account at bank B repeatedly
    - He can check for ciphertext blocks that repeat, and he stores blocks 1,3 and 4 of these transfers
  - He now simply replaces block 4 of other transfers with the block 4 that he stored before
    - all transfers from some account of bank A to some account of bank B are redirected to go into the attacker's B account!

- Identical plaintexts are mapped to identical ciphertexts
- Statistical properties in the plaintext are preserved in the ciphertext:


Original picture

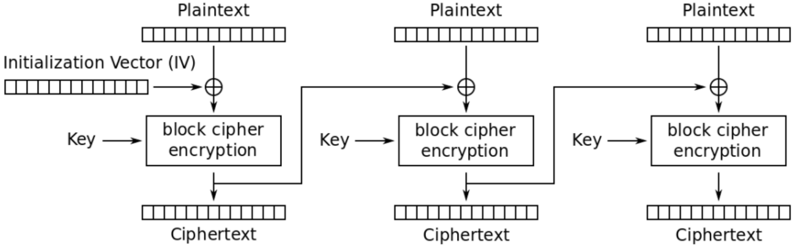

With ECB Block Mode


With any other Block Mode

Cipher Block Chaining mode (CBC)

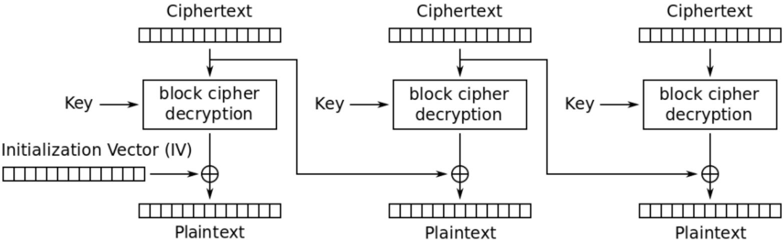
There are two main ideas behind the CBC mode:

- The encryption of all blocks are "chained together" (ciphertext y_i depends not only on block x_i but on all previous plaintext blocks as well)
- The encryption is randomized by using an initialization vector (IV)



Cipher Block Chaining mode (CBC)

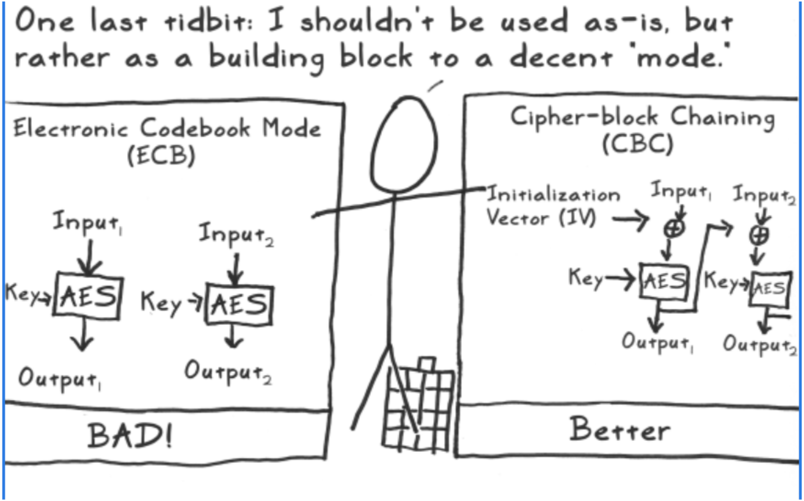
- Requires padding (same as ECB)
- Messages longer than $2^{n/2}$ blocks, where n is the block size in bits shouldn't be encrypted with this mode
- Encryption cannot be parallelizabled but dencryption can be



Substitution Attack on CBC

- Suppose the last example (electronic bank transfer)
- If the IV is properly chosen for every wire transfer, the attack will not work at all
- If the IV is kept the same for several transfers, the attacker would recognize the transfers from his account at bank A to back B
- If we choose a new IV every time we encrypt, the CBC mode becomes a probabilistic encryption scheme, i.e., two encryptions of the same plaintext look entirely different
- It is not needed to keep the IV secret!
- Typically, the IV should be a non-secret nonce (value used only once)

AES and CBC

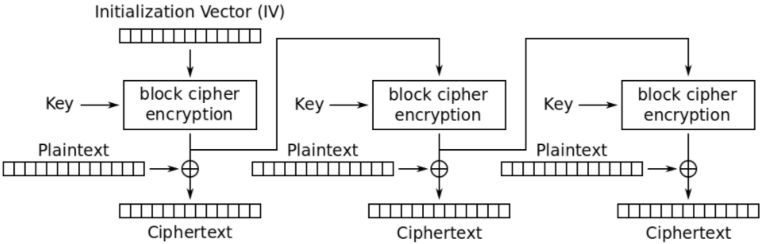

One last tidbit: I shouldn't be used as-is, but rather as a building block to a decent "mode."
Electronic Codebook Mode (ECB)
Input1
Input2
Key
AES
Key
AES
Output1
Output2
BAD!
Cipher-block Chaining (CBC)
Initialization Vector (IV)
Input1
Input2
Key
AES
Key
AES
Output1
Output2
Better

http://www.moserware.com

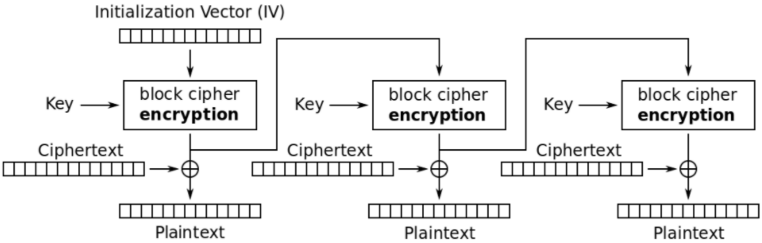
Output Feedback mode (OFB)

- It is used to build a `synchronous stream cipher from a block cipher`
- The key stream is not generated bitwise but instead in a blockwise fashion
- The output of the cipher gives us key stream bits with which we can encrypt plaintext bits using the XOR operation
- `Does not require` using the decryption algorithm
- Requires an initialization vector IV
- Each new messages shall use a new IV (nonce)

Output Feedback mode (OFB)



Output Feedback (OFB) mode encryption


Initialization Vector (IV)
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext

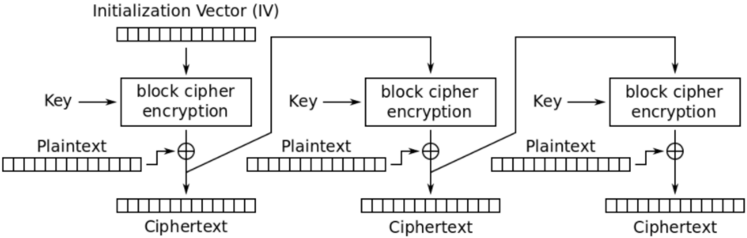
Output Feedback (OFB) mode decryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

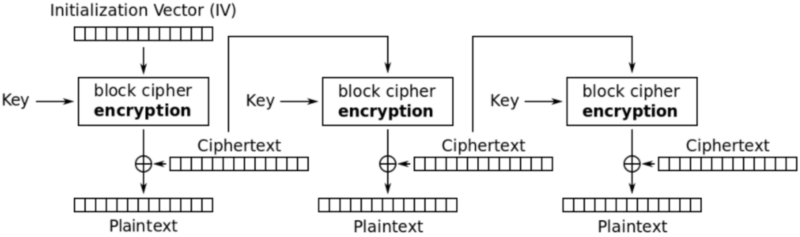
Cipher Feedback mode (CFB)

- It `uses a block cipher as a building block for an asynchronous stream cipher` (similar to the OFB mode)
- The key stream Si is generated in a blockwise fashion and is also a function of the ciphertext
- As a result of the use of an IV, the CFB encryption is also nondeterministic
- It can be used in situations where short plaintext blocks are to be encrypted
- No real advantage over OFB mode

Cipher Feedback mode (CFB)



Cipher Feedback (CFB) mode encryption

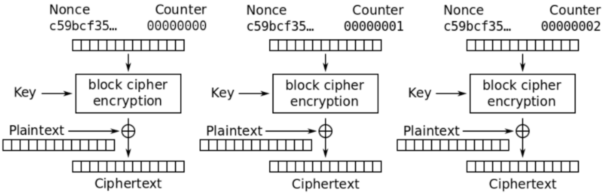

Initialization Vector (IV)
Key
block cipher **encryption**
Key
block cipher **encryption**
Key
block cipher **encryption**
Ciphertext
Ciphertext
Ciphertext
Plaintext
Plaintext
Plaintext

Cipher Feedback (CFB) mode decryption

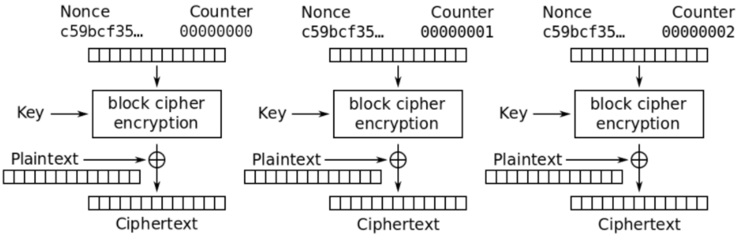
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Counter mode (CTR)

- Counter mode turns a block cipher into a stream cipher (like the OFB and CFB modes)
- The key stream is computed in a blockwise fashion
- The input to the block cipher is a counter which assumes a different value every time the block cipher computes a new key stream block
- Unlike CFB and OFB modes, the CTR mode can be parallelized (desirable for high-speed implementations, e.g., in network routers)
- Does not require padding; just discard unneeded portion of last key block



Counter mode (CTR)



Nonce c59bcf35... Counter 00000000

Key → block cipher encryption

Plaintext → ⊕ → Ciphertext

Nonce c59bcf35... Counter 00000001

Key → block cipher encryption

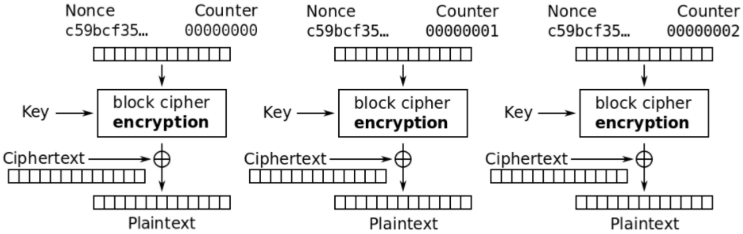
Plaintext → ⊕ → Ciphertext

Nonce c59bcf35... Counter 00000002

Key → block cipher encryption

Plaintext → ⊕ → Ciphertext

Counter (CTR) mode encryption



Nonce c59bcf35... Counter 00000000

Key → block cipher **encryption**

Ciphertext → ⊕ → Plaintext

Nonce c59bcf35... Counter 00000001

Key → block cipher **encryption**

Ciphertext → ⊕ → Plaintext

Nonce c59bcf35... Counter 00000002

Key → block cipher **encryption**

Ciphertext → ⊕ → Plaintext

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Thanks for Your attention.