ICT2213 Applied Cryptography

Topic 2.2: Symmetric Key Cryptography (Block Cipher Modes)

Learning outcomes

- Understand the difference between block and stream ciphers
- List the different modes of operation for block ciphers
- Understand the advantages, disadvantages, and use-cases for each block cipher mode

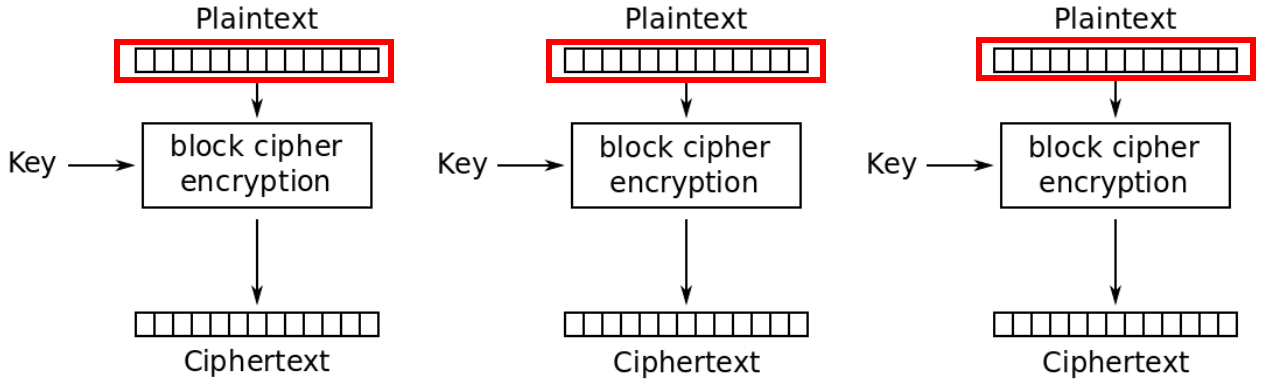
Algorithm types and modes

- There are two basic types of symmetric key algorithms: block ciphers and stream ciphers
- Block ciphers operate on blocks of plaintext and ciphertext
  - The block is typically 16 bytes (e.g., for the case of AES)
  - They are deterministic: The same plaintext will always produce the same ciphertext (using the same key)
- Stream ciphers operate on streams of plaintext and ciphertext
  - One byte at a time
  - They are randomized: The same byte will produce a different byte every time it is encrypted (similar to OTP cipher)
- A cryptographic mode usually combines the basic cipher, some sort of feedback, and some simple operations

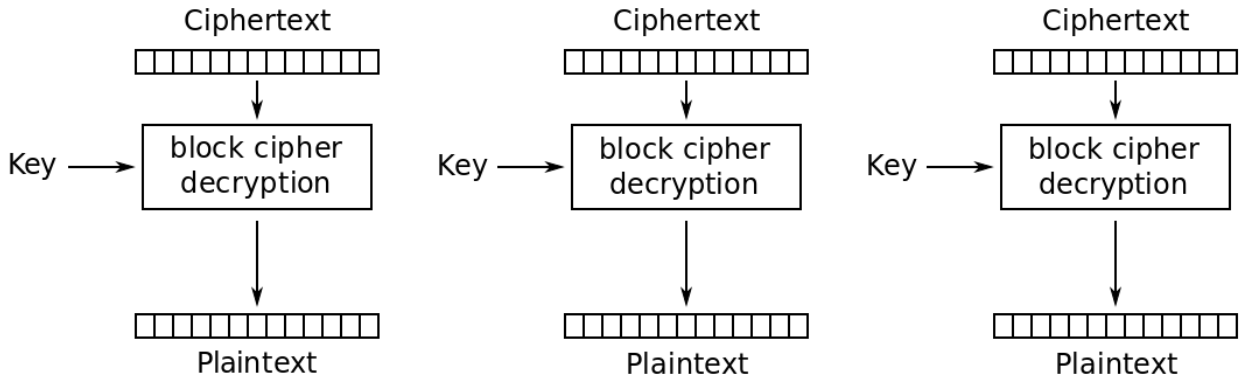
Cipher mode considerations

- NIST has defined 5 modes of operation in special publication SP 800-38A
- The operations in each mode are simple, because the security is a function of the underlying cipher and not the mode
- Some security considerations:
  - Patterns in the plaintext should be concealed
  - Input to the cipher should be randomized
  - Manipulation of the plaintext by introducing errors in the ciphertext should be difficult
- Other considerations:
  - Speed, efficiency
  - Error recovery

Electronic codebook (ECB) mode



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

ECB mode properties

SINGAPORE INSTITUTE OF TECHNOLOGY

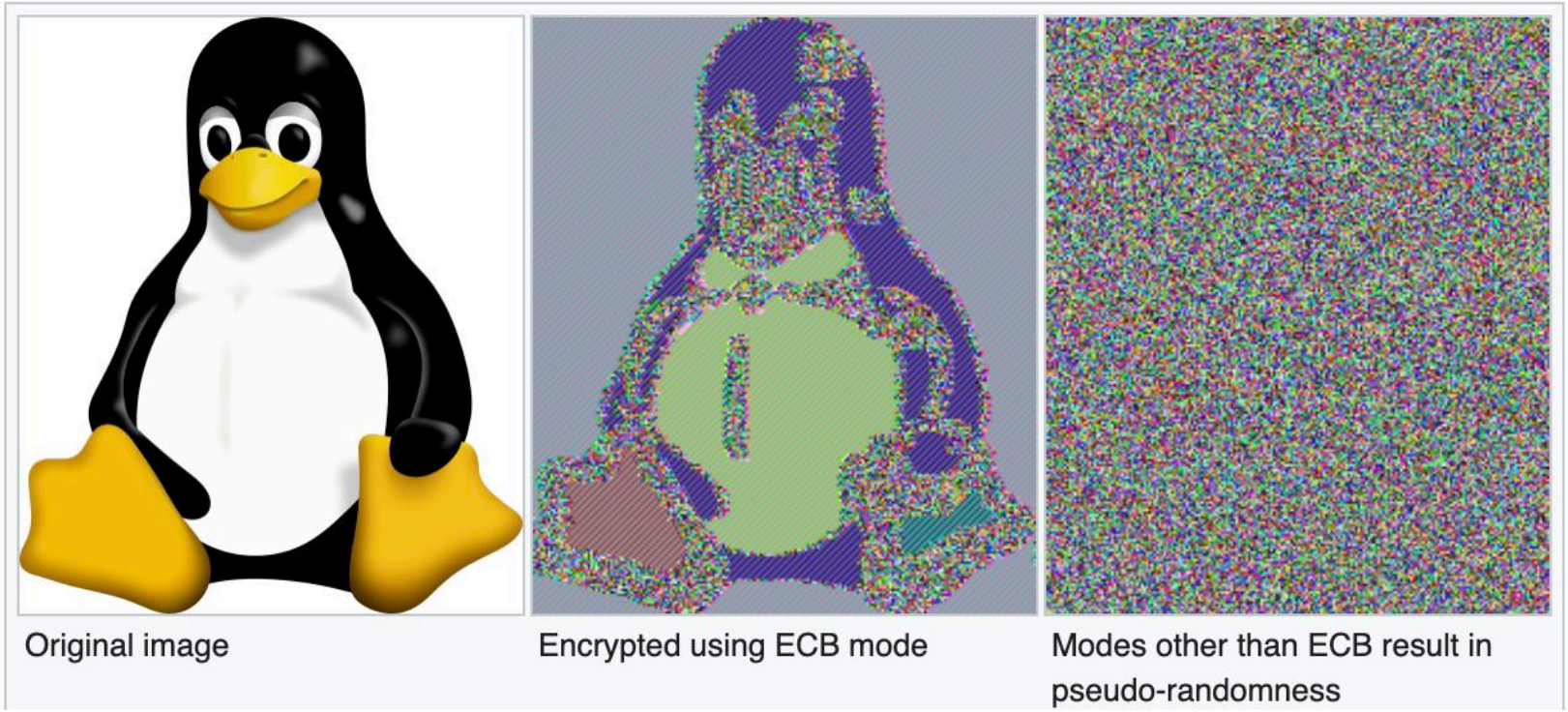
Pros

- Encryption/decryption can be parallelized (fast)
- Can decrypt parts of an encrypted file independently
- Bit errors in one ciphertext will not affect the rest of the plaintext
- Best for encrypting short messages, such as keys

Cons

- May require padding if the message is not a multiple of the block size
- Vulnerable to known plaintext attacks
- This is possible if the attacker knows the structure of the plaintext
- Statistical attacks are also possible if the message contains a lot of redundancies
- An attacker can remove, repeat, or interchange blocks at will

ECB example: Patterns in plaintext

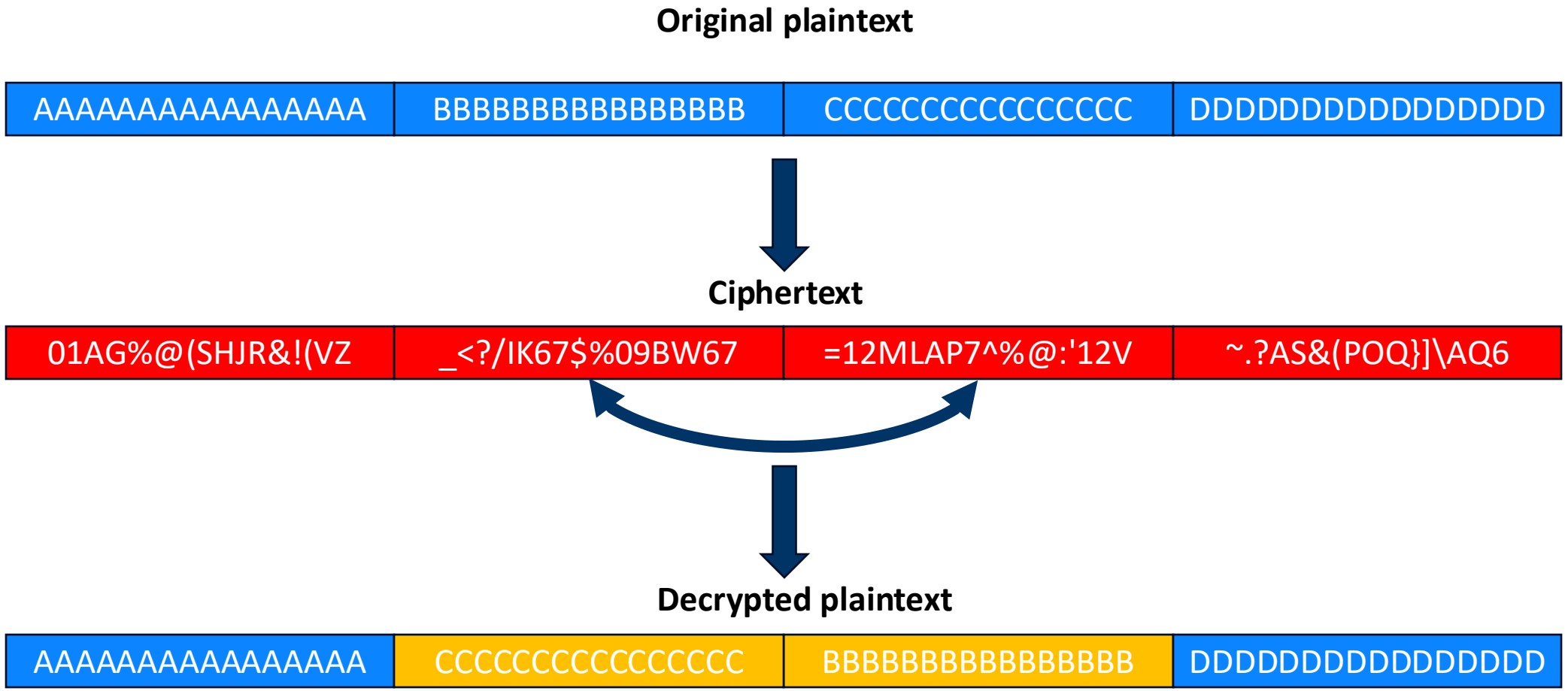


Original image

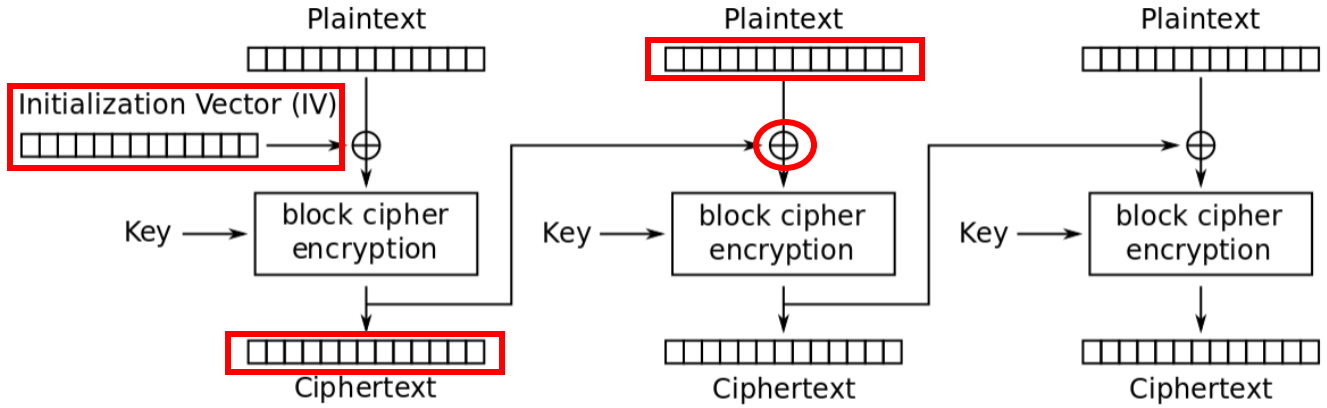
Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

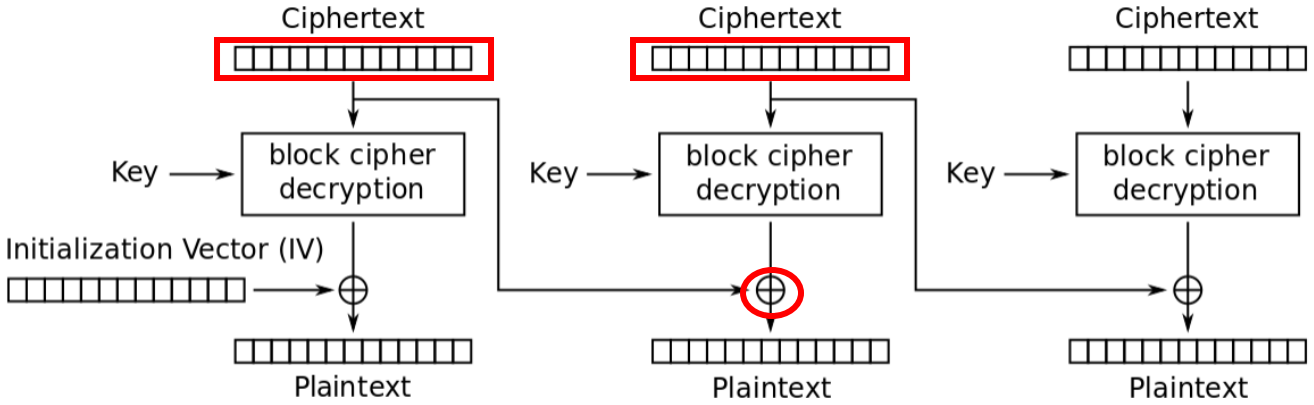
ECB example: Interchange blocks



Cipher block chaining (CBC) mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

CBC mode properties

SINGAPORE INSTITUTE OF TECHNOLOGY

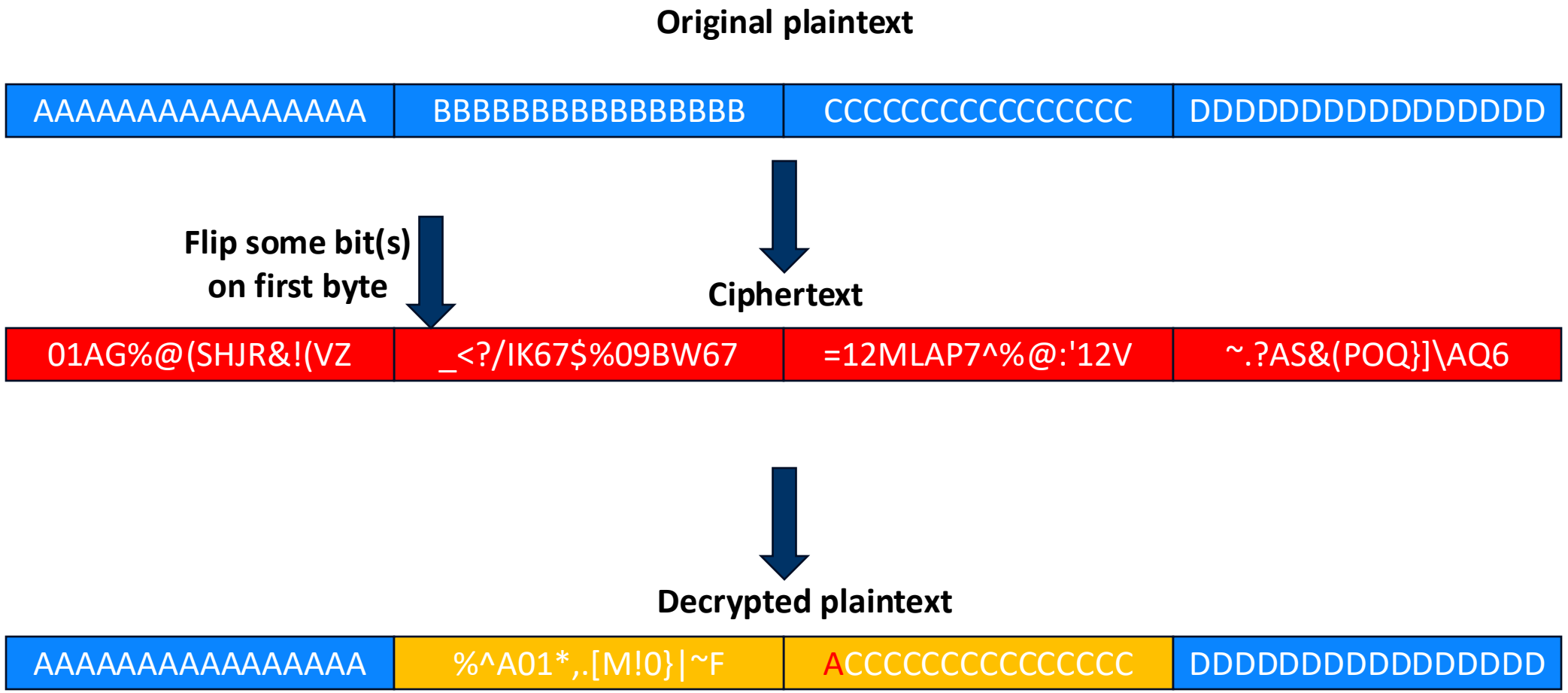
Pros

- Conceals patterns in a plaintext
- The IV randomizes the encryption, so the same plaintext will produce a different ciphertext every time it is encrypted (with the same key)
- Since the blocks are chained, an attacker cannot replay, insert or interchange blocks
- Good for encrypting files on disk

Cons

- Requires padding for incomplete blocks
- Cannot parallelize encryption because of chaining (slower)
- The attacker can flip certain bits of ciphertext block i to introduce controlled changes in plaintext block i+1 (due to XOR after decryption)

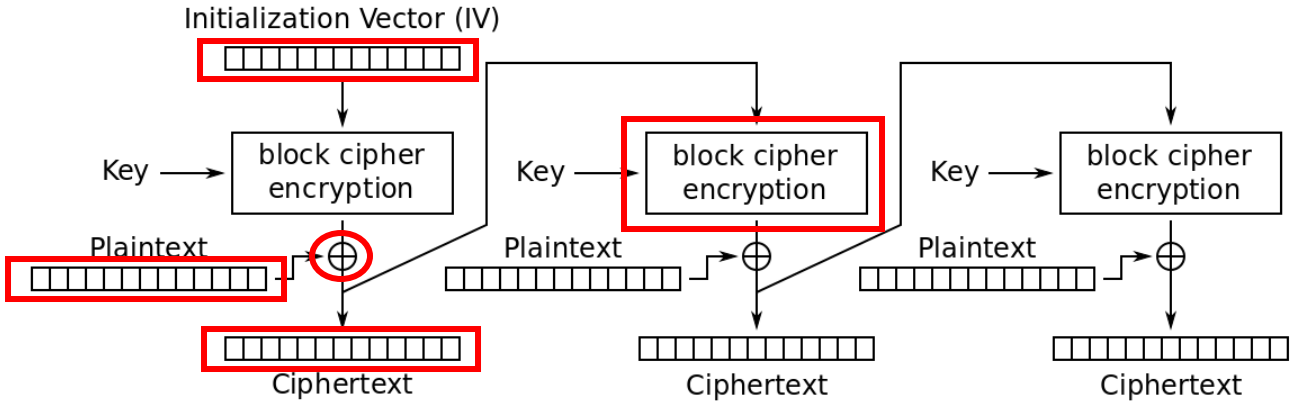
CBC example: Bit flipping attack



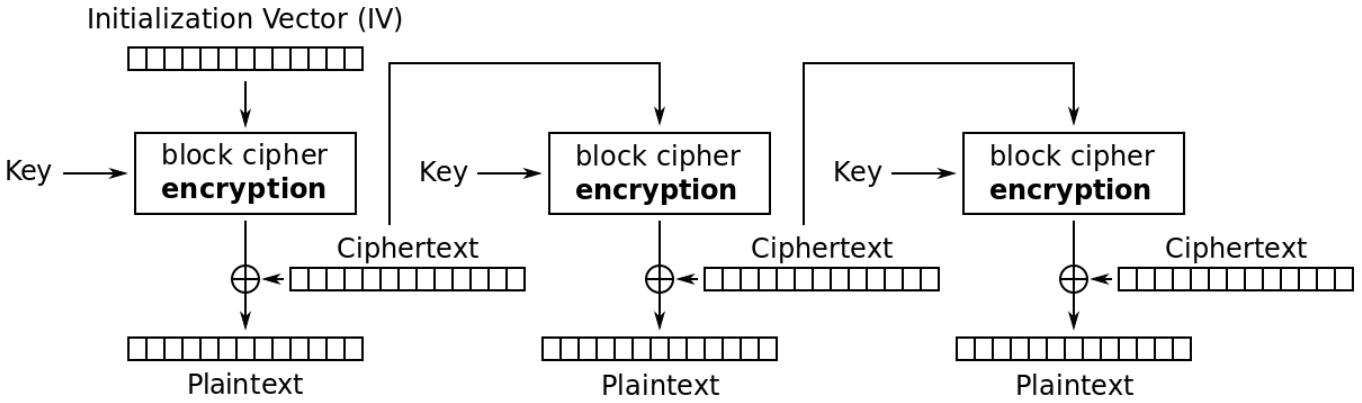
Stream ciphers

- Stream ciphers convert plaintext to ciphertext one byte at a time
- A keystream generator outputs a stream of bytes
- During encryption, this keystream is XORed with a stream of plaintext bytes
- For decryption, the ciphertext bytes are XORed with an identical keystream to recover the plaintext bytes
- The system's security depends entirely on the insides of the keystream generator
  - If the keystream has a short, repeating pattern, the algorithm will be a simple XOR with negligible security
  - If the keystream is an endless stream of real random bytes, you have an OTP and perfect security
- The reality of stream cipher security lies somewhere in the middle—deterministic keystream (based on a key), but sufficiently random

Cipher feedback (CFB) mode



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption

Properties of CFB mode

SINGAPORE INSTITUTE OF TECHNOLOGY

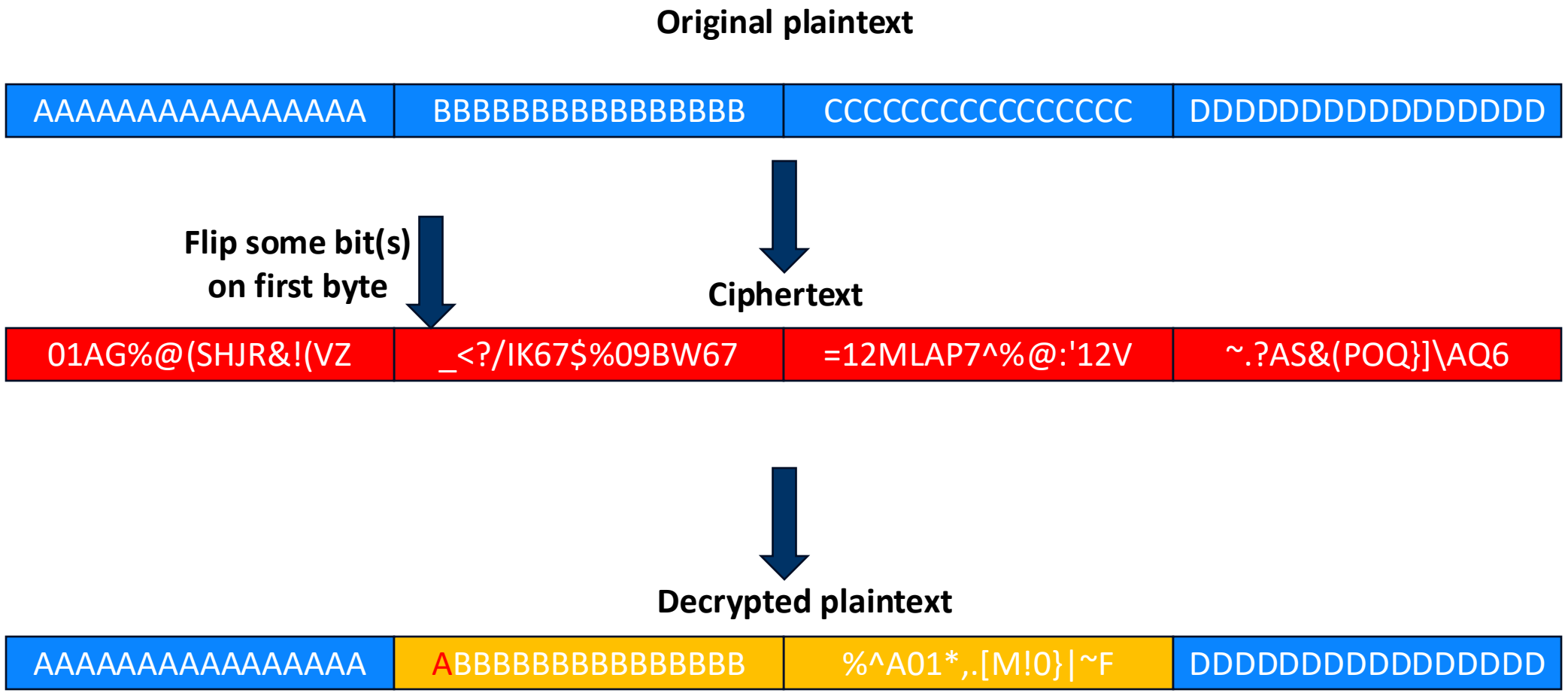
Pros

- No need for padding
- Data can be encrypted in units smaller than the block size, i.e., s bits instead of b bits (b is the block size of the cipher)
- The cipher is self-synchronizing, i.e., it can recover automatically from ciphertext bit errors

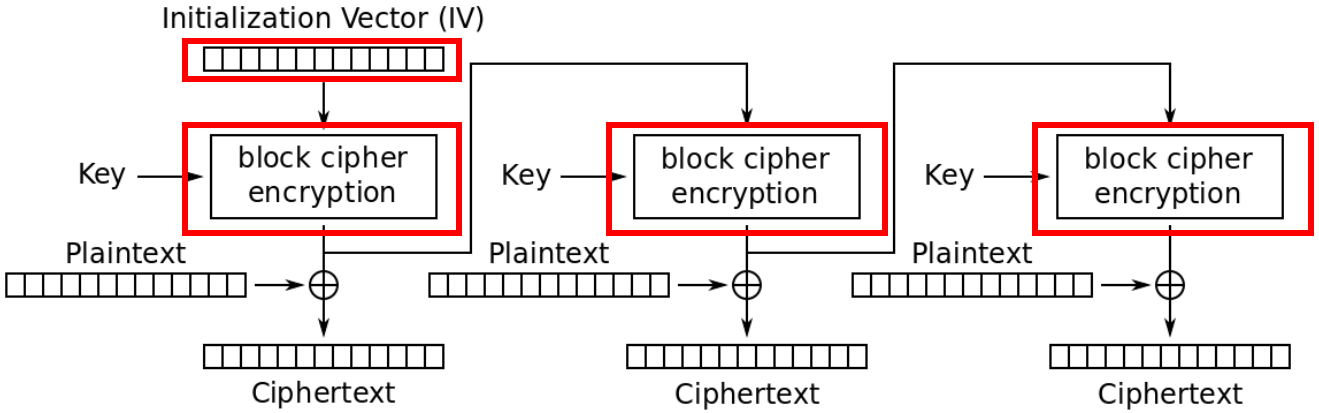
Cons

- Encryption cannot be parallelized
- An attacker can introduce controlled errors in the plaintext by manipulating the ciphertext
- An attacker can change the final bits of a message without detection

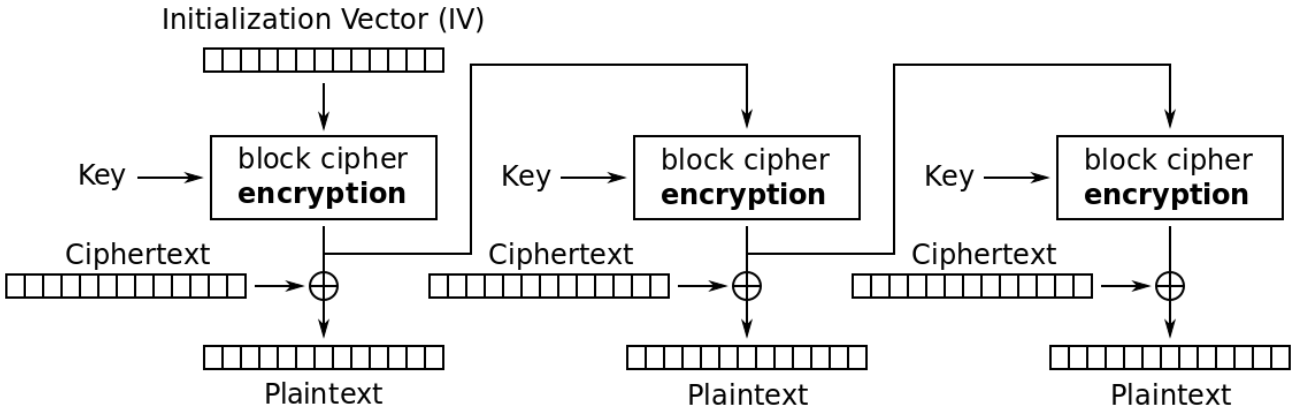
CFB example: Bit flipping attack



Output feedback (OFB) mode



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Properties of OFB mode

SINGAPORE INSTITUTE OF TECHNOLOGY

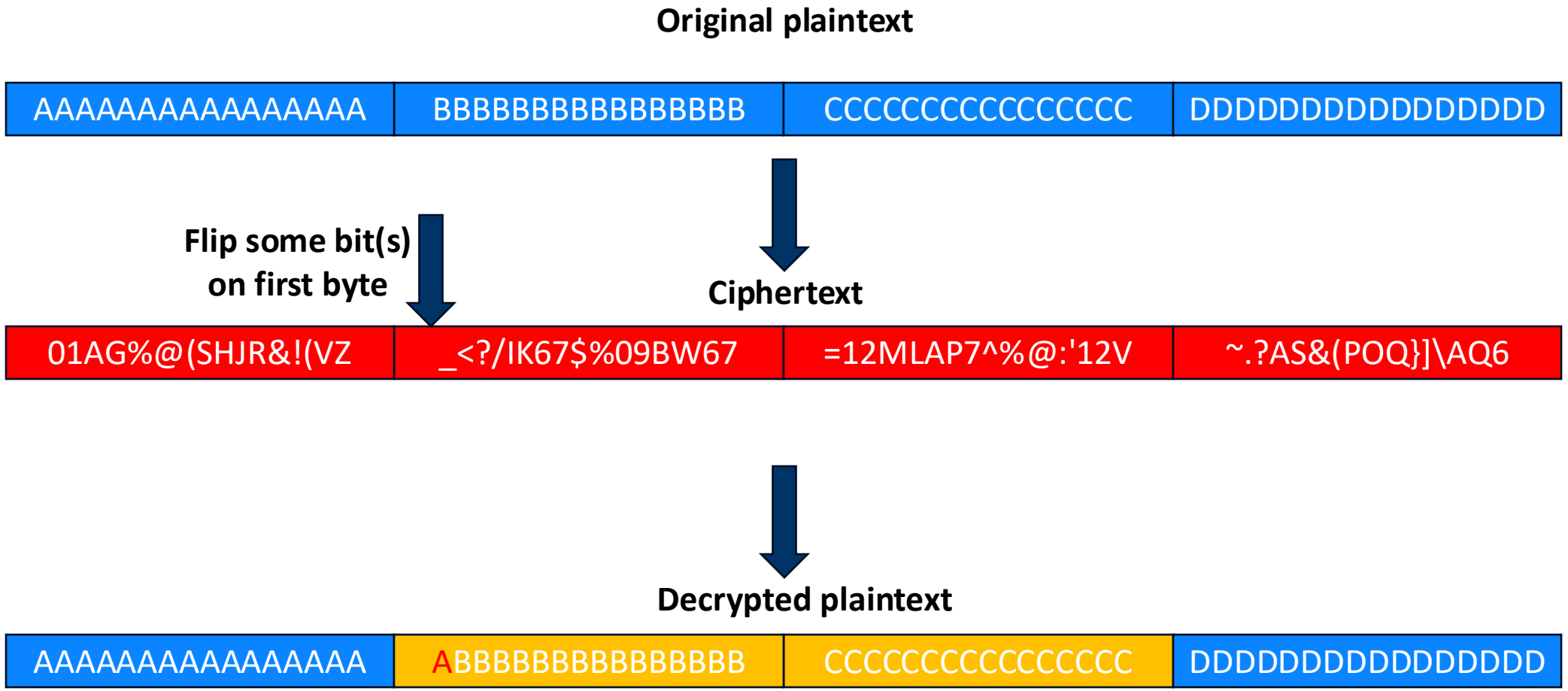
Pros

- No need for padding
- Most of the work (keystream generation) can occur offline
- This is because the keystream is independent of the plaintext or ciphertext
- No error extension—bit errors only affect the corresponding plaintext
- Resilient against ciphertext insertions or deletions—loss of synchronization

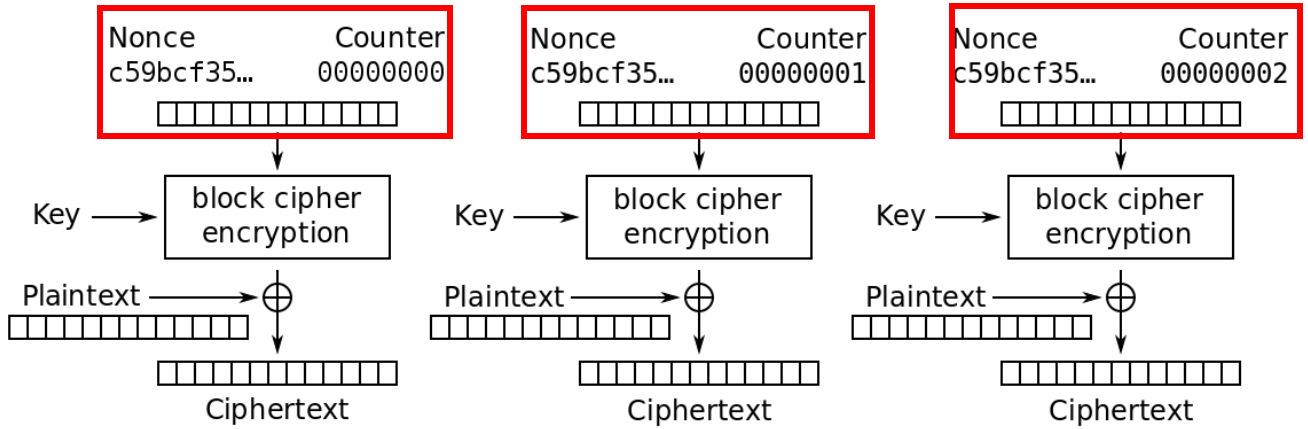
Cons

- An attacker can introduce controlled errors in the plaintext by manipulating the ciphertext
- Such changes cannot be detected
- As such, there is a need for authentication of the plaintext

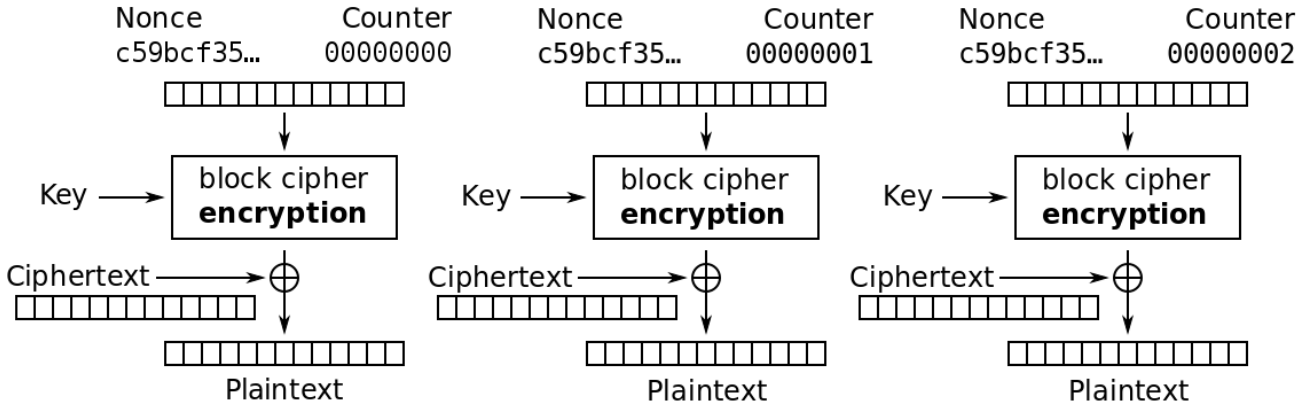
OFB example: Bit flipping attack



Counter (CTR) mode



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Choosing a cipher mode

- ECB is the easiest and fastest mode to use a block cipher
- However, ECB mode is also the weakest
  - Vulnerable to replay attacks, easiest to cryptanalyze
- For encrypting random data, such as other keys, ECB is a good mode to use, since the data is short and random
- CBC is generally used for encrypting files
- CFB is generally the mode of choice for encrypting streams of characters when each character has to be treated individually
- OFB or CTR is the mode of choice in an error-prone environment, because they have no error extension

Current recommendations

- There have been known attacks for CBC mode when used in TLS context (for Internet communications)
  - BEAST attack and POODLE attack
- Current best practice is the use of authenticated encryption, i.e., a mode that provides both confidentiality and integrity
  - Integrity is provided via the use of message authentication codes
- The most widely used cipher today that employs authenticated encryption is AES-GCM (Galois/Counter Mode)
- ChaCha20-Poly1305 is a more recent cipher that has been standardized by the IETF
  - Faster than AES-GCM
  - Less vulnerable to timing attacks