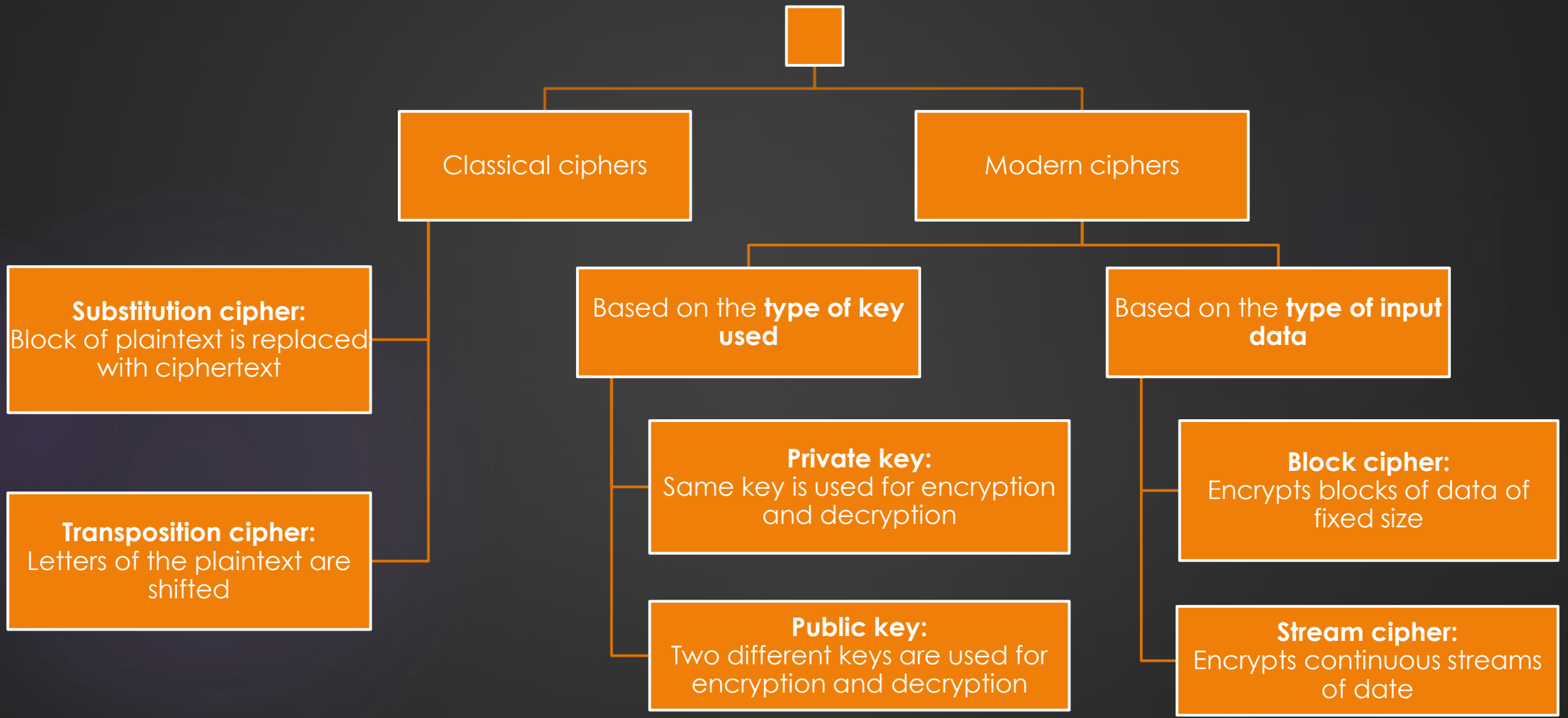
CIPHER TYPES

 Version : 0.0.4 Update : 23/03/2022

Types of ciphers



STREAM CIPHER

Stream ciphers

- A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).
- Stream ciphers are often used for their speed and simplicity of implementation in hardware, and in applications where plaintext comes in quantities of unknowable length like a secure wireless connection.
- Examples:
  - CryptMT,
  - RC4,
  - SEAL,
  - Etc.

BLOCK CIPHER

Introduction

- Blocks size must be fix.
- Initialization Vector (IV) is a unique random binary sequence used for each encryption operation.
- The IV is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key.
- The block cipher modes ECB, CBC, OFB, CFB, CTR, and XTS provide confidentiality, but they don't protect against accidental modification or malicious tampering.
- Modification or tampering can be detected with a separate message authentication code such as CBC-MAC, or a digital signature. The cryptographic community recognized the need for dedicated integrity assurances and NIST responded with HMAC, CMAC, and GMAC.

Common modes

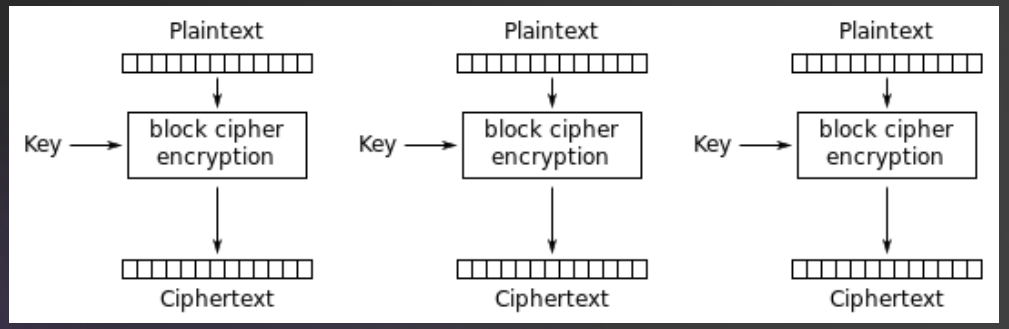
- Authenticated encryption with additional data (AEAD) modes:
  - Galois/Counter Mode (GCM) means Mode compteur.
- Common modes:
  - Electronic Code Book, ECB means Dictionnaire de codes
  - Cipher Block Chaining, CBC means Enchaînement des blocs
  - Cipher Feedback, CFB means Chiffrement à rétroaction
  - Output Feedback, OFB means Chiffrement à rétroaction de sortie

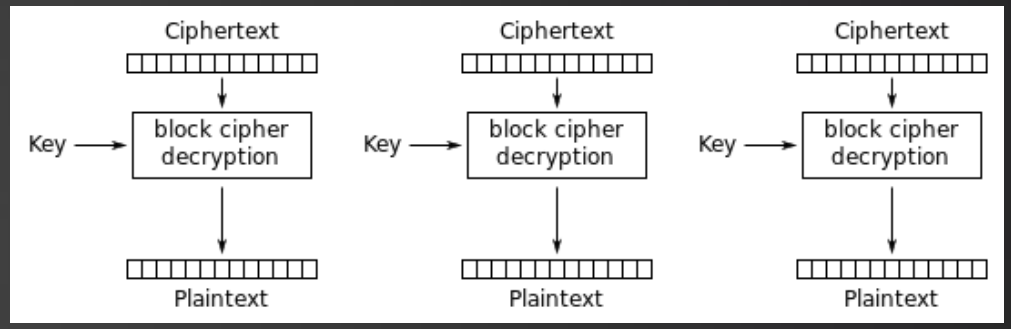
Galois/Counter Mode (GCM)

- GCM is an authenticated encryption algorithm designed to provide both data integrity, non-repudiation, and confidentiality. The encryption used is based on a counter mode in which the multiplication between the counter and the 128-bit key is performed in the Galois body.
- Galois Message Authentication Code (GMAC) is a variant limited to GCM authentication.
- The IEEE 802.1AE standard uses this algorithm, coupled with the Advanced Encryption Standard (AES).
- It's a secure cipher mode (not a weak) unlike ECB, CBC, OFB, CFB, etc.

Electronic codebook (ECB)

- This mode is the simplest: the same block is always coded in the same way. There is no input or output feedback on the encryption function.





- Advantages
  - Encryption or decryption can be parallelized.
  - Machines or CPUs can work simultaneously on different parts of the message.
  - It allows random access in ciphertext. A one-bit transmission error only affects the decoding of the current block.
- Disadvantages
  - Plain text repeats are not masked and occur as cipher text repeats.
  - Complete portions of the message can be edited, repeated or replaced without difficulty.
  - Loss or addition of a bit is irrecoverable.

Electronic codebook (ECB)

Example with a salary list, the following two messages are encrypted with an ECB mode and a block cipher algorithm which works with a block of two characters.

JOHN__105000

JACK__500000

The encryption on the first message looks like this:

JO | HN | __ | 10 | 50 | 00

Q9 | 2D | FP | VX | C9 | IO

And on the second message, we get:

JA | CK | __ | 50 | 00 | 00

LD | AS | FP | C9 | IO | IO

We see that pairs of characters appear in the two encrypted messages, the same goes for the plain messages:

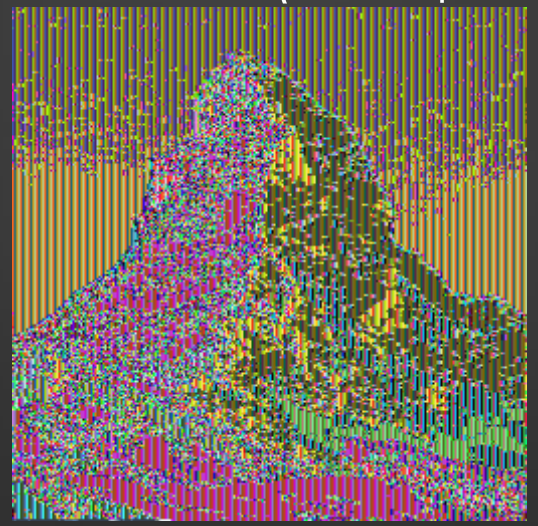
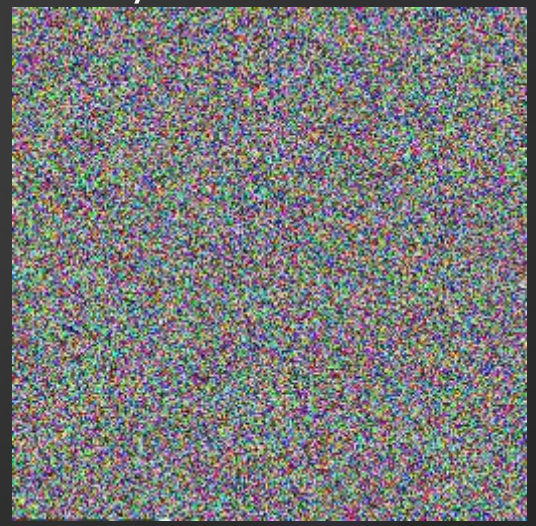
Q9 | 2D | FP | VX | C9 | IO

LD | AS | FP | C9 | IO | IO

Assuming that John knows his salary, he could guess Jack's salary because the sequence "C9" is "50" and "IO" is "00". John deduces that Jack's salary, quantified in "C9IOIO" corresponds to "500,000".

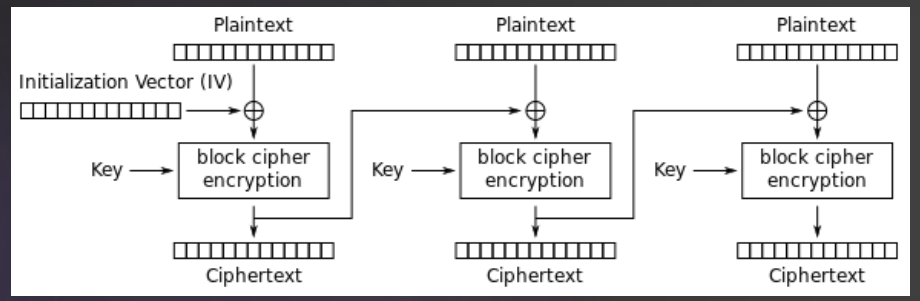
Electronic codebook (ECB)

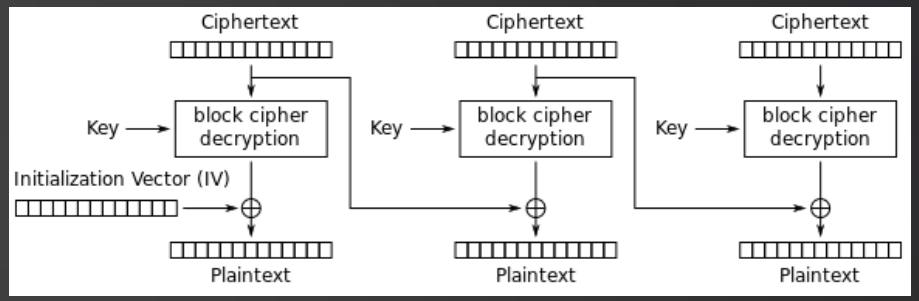
- The vulnerability is even more glaring in an image.
- Images consist of numerous redundancies which cause the blocks to be encrypted in the same way in ECB mode.
- In the example below, the ECB encryption is performed on blocks of 4 pixels. Last image is more secure (exemple with CBC).

Cipher Block Chaining (CBC)

- In this encryption mode, each block of plaintext is first combined by an **exclusive or** with the last block of the ciphertext. The output of this **exclusive or** is then applied to the encryption function.
- This encryption mode also has an **Initialization Vector** which allows the process to be initialized when no block has yet been encrypted.

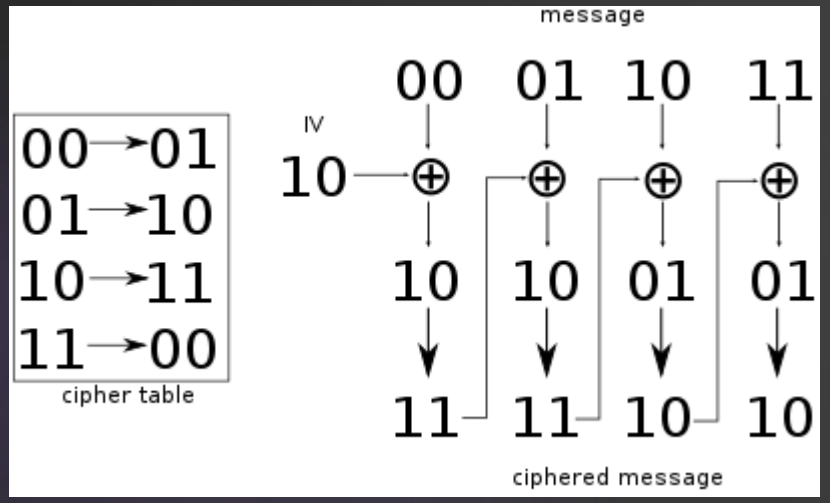


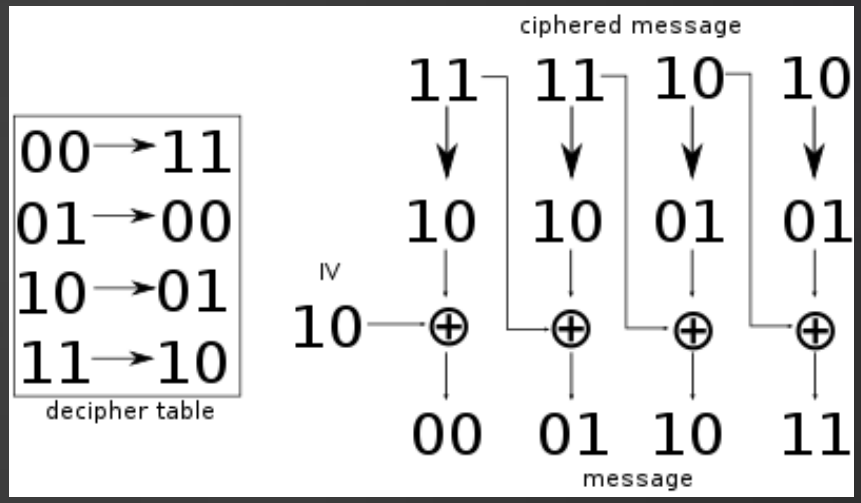


- Advantages
  - Clear text repetitions are hidden in the cipher text.
  - The value of the IV need not be secret.
- Disadvantages
  - Two identical plaintext will have the same beginning of cipher text.
  - A one-bit transmission error only affects the decoding of the current block as well as the decoding of the same bit in the following block;
  - The loss of synchronization (loss or addition of a bit) is irrecoverable.

Cipher Block Chaining (CBC)

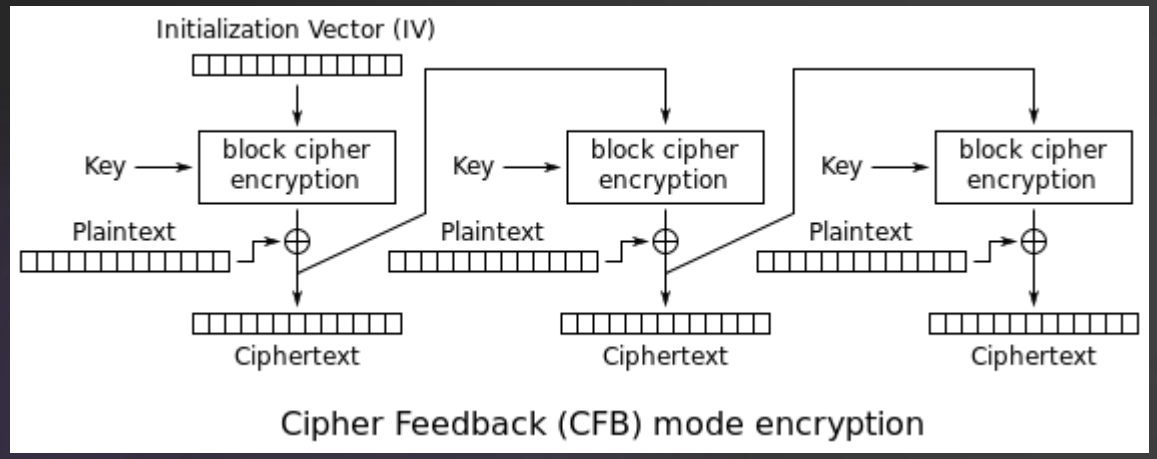
- Example :

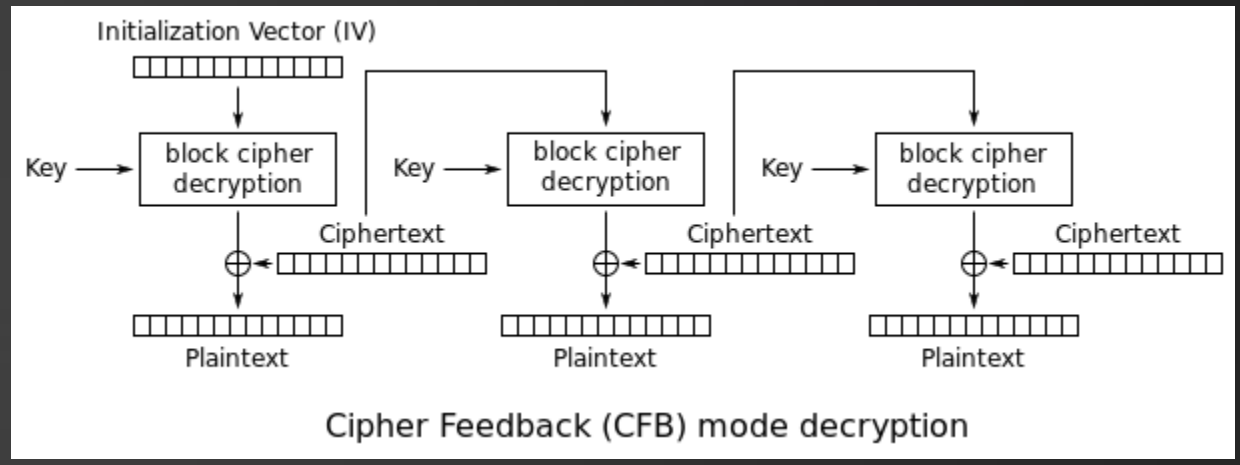




Cipher feedback (CFB)

- The cipher feedback (CFB) mode, in its simplest variation, is using the entire output of the block cipher. In this variation, it is very similar to CBC, makes a block cipher into a self-synchronizing stream cipher.

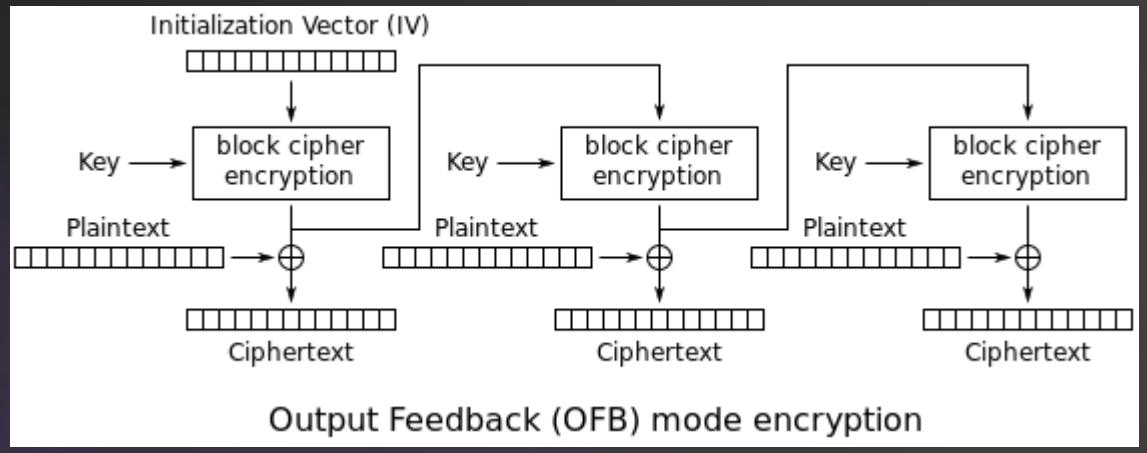




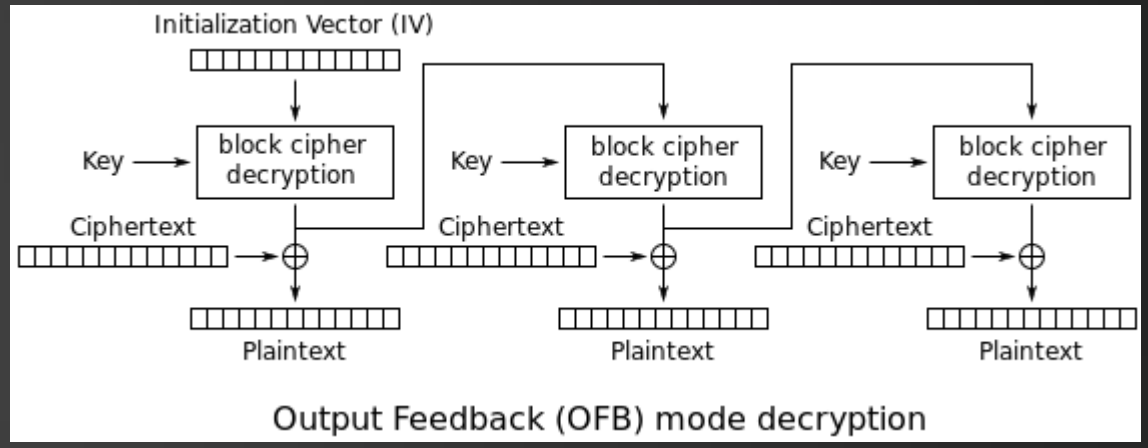
- Advantages
  - Clear text repetitions are hidden in the cipher text.
  - The value of the initialization vector IV need not be secret.
  - The loss of synchronization (loss or addition of a bit) is recoverable.
- Disadvantages
  - A one-bit transmission error only affects the decoding of the current block as well as the decoding of the same bit in the following block.

Output feedback (OFB)

- OFB mode resembles CFB mode. The only difference is that the byte injected into the shift register is the least significant byte of the ciphertext.



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

- Advantages
  - Clear text repetitions are hidden in the cipher text.
  - The value of the initialization vector IV need not be secret.
  - This mode does not amplify errors. A one-bit transmission error only affects that bit during decoding.
- Disadvantages
  - The loss of synchronization (loss or addition of a bit) is irrecoverable.

Conclusion

- After exploring the different encryption modes that can be used, we will now take a look at the different encryption algorithms.
- There are in all four major families of algorithms used in cryptography.
- These families are:
  - Hash functions,
  - Symmetric algorithms,
  - Asymmetric algorithms,
  - Methods of generating random numbers.