The usage and the impact of shift registers on the CFB mode of operation

HW1 - CNS Sapienza

Andrea Fioraldi 1692419

2018-10-12

1 Introduction

With the aim to provide confidentiality and authenticity of information, *Block Ciphers* are widely used in cryptography. Block Chiphers operates on fixed-length messages, called *blocks*, and *Modes of Operations* are the techniques used to apply block chiphers to messages longer than a block.

Cipher Feedback (CFB) is a popular mode of operation. In this technique, regards the ecryption, the produced cyphertext block xored with the corrispindendt plaintext block is forwarded to the next encryption unit to produce the next cyphertext block.

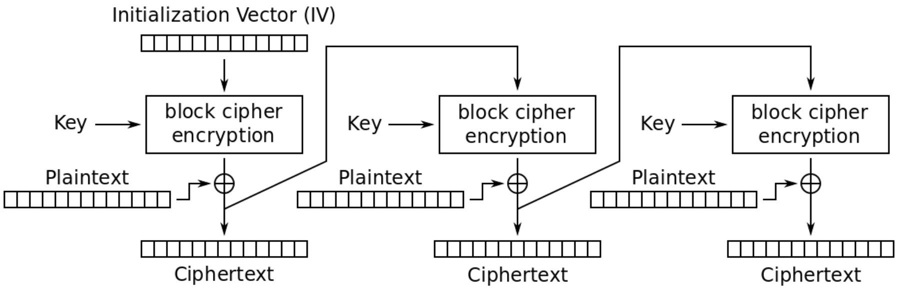

Figure 1: CFB encryption, from [1]

Viceversa, during the decryption, the produced plaintext xored with the correspondent cyphertext is forwarded to produce the next plaintext block.

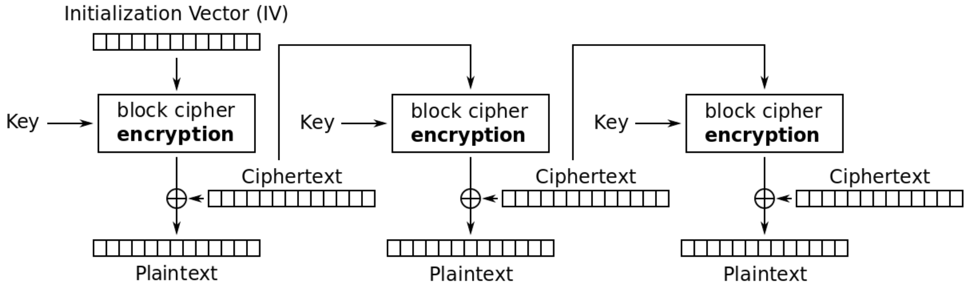

Figure 2: CFB decryption, from [1]

This mode of operation requires an initialization vector (IV) as initial input block. As you can see in figure 2 the encryption unit is used also for decryption.

2 Shift registers

One of the most used variant of CFB introduces shift registers as input for the encryption unit.

2.1 Usage

2.2 Impact

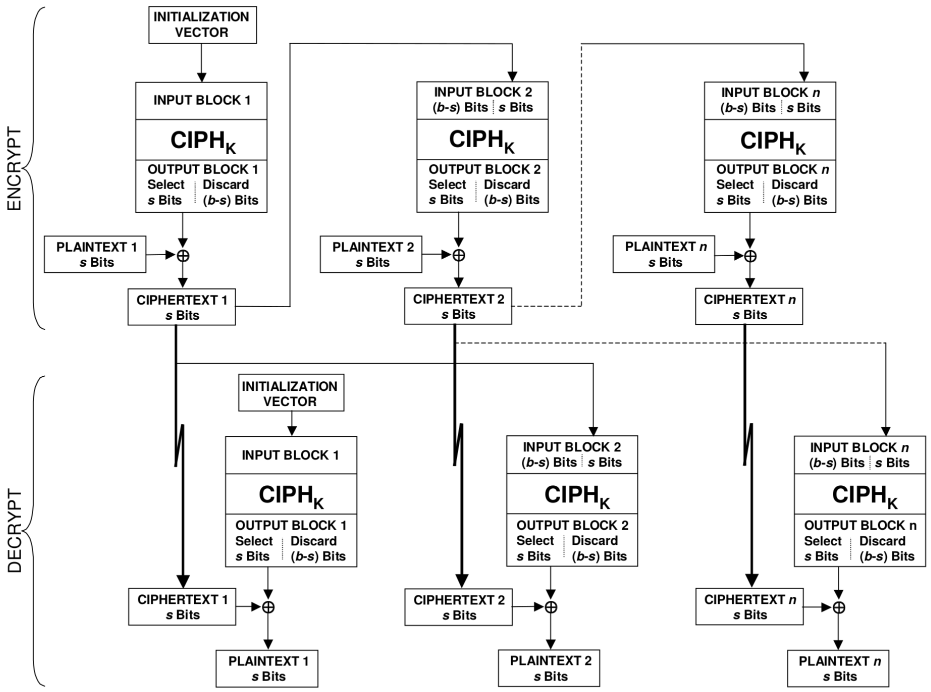

Figure 3: CFB with shift registers, from [2]

References

[1] *Block cipher mode of operation - Wikipedia.* `https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`. Accessed: 2018-10-12.

[2] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. Methods and Techniques.* Tech. rep. 800-38A. National Institute of Standards and Technology, 2001. `url: http://www.dtic.mil/docs/citations/ADA400014`.