MODES OF OPERATION OF THE AES ALGORITHM

Dobre Blazhevski
University American College Skopje
Skopje, Macedonia

Adrijan Bozhinovski
University American College Skopje
Skopje, Macedonia

Biljana Stojchevska
University American College Skopje
Skopje, Macedonia

Veno Pachovski
University American College Skopje
Skopje, Macedonia

ABSTRACT

AES is an algorithm for block encryption, which is in widespread use. Back in 2001, five modes of operation of the AES algorithm were standardized: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter). This paper describes these modes and the details of their operation, their strengths and weaknesses, as well as the demands for their parameters, which are necessary to guarantee security and are of utmost importance for a proper AES implementation. The parameters are often neglected, and even if that is not the case, the modes of operation can be unreliable and vulnerable to various kinds of attacks. In addition, as a result of the analysis of the AES modes of operation by studying the literature, the conclusion is that, in order to obtain a proper and secure AES implementation, the CTR mode should be used.

Keywords: encryption, block ciphers, AES, modes of operation

I. INTRODUCTION

The block ciphers are schemes for encryption or decryption where a block of plaintext is treated as a single block and is used to obtain a block of ciphertext with the same size [1]. Today, AES (Advanced Encryption Standard) is one of the most used algorithms for block encryption. It has been standardized by the NIST (National Institute of Standards and Technology) in 2001, in order to replace DES and 3DES which were used for encryption in that period. The size of an AES block is 128 bits, whereas the size of the encryption key can be 128, 192 or 256 bits. In each of the stages of encryption, four functions are applied: substitution of bytes, permutation, arithmetic operations over finite fields and an XOR operation with the encryption key. The size of the AES block provides efficiency, but also sufficient security. Taking into account the computing power of the technology in the period of the AES standardization and the assumed computing power projected for the future, it has been considered that the minimum size for the encryption key of 128 bits provides resistance to brute force attacks [2]. Also, the algorithm was constructed to be resistant to all block cipher attacks which were known at the time.

Block cipher algorithms should enable encryption of plaintext with size which is different from the defined size of one block as well. A way to provide this is presented in [2, 3]. Namely, it is proposed to add a ”1“ to the plaintext which is smaller than the block, and than to add ”0“’s padding to accomplish the required size. Another way is to use a mode of operation. The mode of operation may also provide application of the block cipher on a stream of plaintext and make the algorithm more efficient. On the other hand, the mode of operation may convert the block cipher into a stream cipher and also to strengthen the effect of the encryption algorithm. To meet these requirements, in 2001 the NIST standardized five modes of operation: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack) snd CTR (Counter), which apply to AES [4]. Each mode of operation has its own parameters which are important to provide the necessary security of the algorithm.

In this paper, the five AES modes of operation will be presented, along with their respective parameters that guarantee security. The presentation will first contain the principles of operation of ECB, CBC, CFB, OFB and CTR modes of operation, as they are described in the literature. For each mode of operation, the necessary parameters, their advantages and disadvantages, and also their proper application, will be presented. The modes of operation are the most important for a proper AES implementation, regardless of its software or hardware implementation. An improper implementation or use of the modes of operation may seriously compromise the AES algorithm reliability and lead to disclosure of a part or all of the plaintext [5]. On the other hand, personal experience indicates that even the people close to the field pay more attention to the size of the key, while neglecting the basic requirements of the modes of operation. The final section will contain a conclusion based on a critical analysis of the covered literature.

II. MODES OF AES OPERATION

A. ECB Mode of Operation

The ECB (Electronic Code Book) mode of operation is the simplest of all. A block scheme of this mode is presented in Fig. 1.

As it can be seen from Fig. 1, the plaintext message is divided in blocks (P_1, P_2, P_N), where each block is encrypted separately with the same key (K). The results of the encryption are the encrypted messages C_1, C_2 and C_N respectively.

If the size of the message is larger than n blocks, the last block is filled with padding. In this mode, if an error occurs in one of the blocks, it is not propagated to the other blocks, which is why decryption is possible in the blocks that don't contain an error [2, 6, 7].

According to [6], the encryption in this mode is deterministic, because identical P blocks will produce identical C blocks, which is why identical plaintext blocks or a message with the same beginning are easily recognizable. Also, the ordering of the C blocks can be changed without the receiver noticing. In general, this mode is not recommended for encryption of data that is larger than one block [2, 8]. In [3] it is strictly recommended not to use this mode at all, while [7] states that this mode of operation is wrong and abandoned.

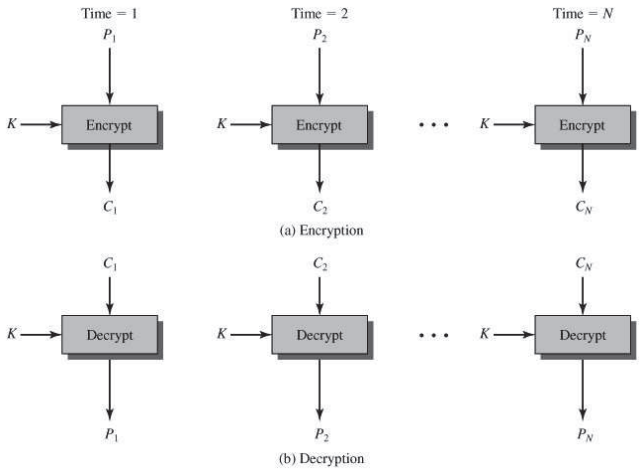

Figure 1: Scheme of the ECB mode of operation [2]

B. CBC Mode of Operation

In order to provide cryptographic security, every encryption of the same plaintext should result with a different ciphertext [6]. The CBC (Cipher Block Chaining) mode of operation (Fig. 2) provides this by using an initialization vector – IV [4]. The IV has the same size as the block that is encrypted. Fig. 2 presents the encryption process. First, an XOR operation is applied to the plaintext block (P_1) with the IV, and then an encryption with the key (K) is performed. Then, the results of the encryption performed on each block (C_1, C_2, … , C_{N-1}) is used in an XOR operation of the next plaintext block P_N which results in C_N. In this way, when identical plaintext blocks are encrypted, a different result is obtained. Also, using a different IV for each new encryption, an identical message will always be encrypted differently. It should be emphasized that the same key K is used in each of the encryption blocks.

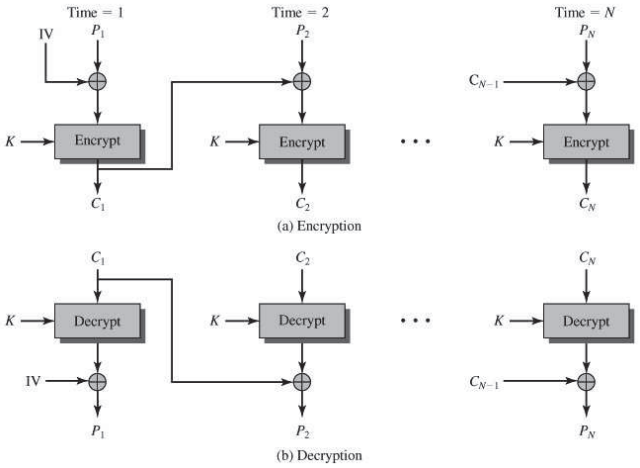

Figure 2: Scheme of the CBC mode of operation [2]

An error in one of the plaintext block will propagate in all the following blocks and will be manifested in the process of the description [8]. Specifications in [8] recommend that the Padding method 2 is used in case padding is needed with the CBC mode of operation because it provides protection from some of the known PA (Padding Attacks).

There are complex CBC attacks for which an unpredictable value of IV is needed in order to overcome them [2, 6]. In [7] it is emphasized that the CBC mode of operation is safe from CPA (Chosen Plaintext Attack) attacks (attacks in which the attacker chooses a set of plaintexts and is able to obtain respective ciphertexts) only if the IV has a random value, but not if the IV is a nonce (a number that is not repeated). The CBC mode of operation, besides its vulnerability to PA attacks, is also easily susceptible to CCA (Chosen Ciphertext Attack) attacks (where the attacker chooses a set of ciphertexts and is able to obtain respective plaintexts). According to [3], the encryption key has to be changed whenever condition (1) holds:

$$q << 2^{(n+1)/2} \tag{1}$$

In (1), q is the number of blocks that should be encrypted and n is the number of bits in the encryption blocks.

In order to provide protection from CCA attacks in this mode of operation, it is necessary to use AE (Authenticated Encryption), where, besides the encryption, authentication is also performed [3].

C. CFB Mode of Operation

The CFB (Cipher FeedBack) mode of operation allows the block encryptor be used as a stream cipher. The scheme of the CFB mode of operation is given in Fig. 3.

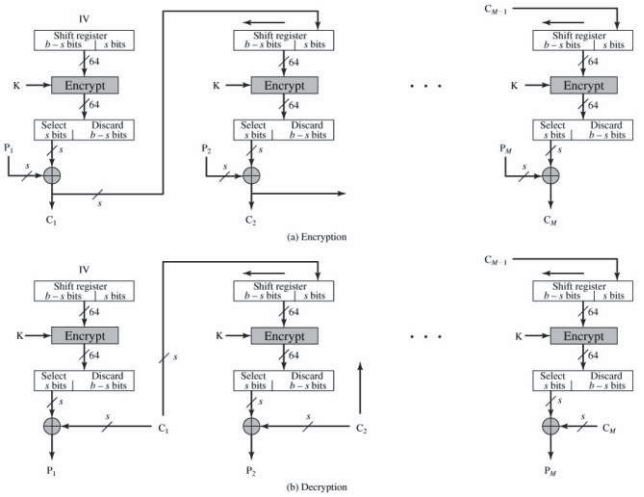

Figure 3: Scheme of the CFB mode of operation [2]

As can be seen in Fig. 3, in the CFB mode of operation, at the beginning (at the first block) the encryption (uses an encryptor denoted with Encrypt) is performed by using an IV and an encryption key K. After that, the XOR operation between the encryption result (the output form the encryptor) and the plaintext block (P_1) is performed. For all the other blocks, the encryption is performed over the result of the encryption of the previous blocks accordingly (C_1, C_2, ...). Then an XOR is performed with the corresponding plaintext block (P_2, P_3, ...). In the beginning, the IV is placed in a shift register, the size of which can be e.g. 64 bits. The result of the encryption of the IV is again 64 bits. But, the XOR is applied to only a few bits s (for example, s=8) of the encrypted IV with also s bits from the plaintext P_1. The least significant bits from the IV that will not be used are discarded. The result C_1 from the XOR operation is then placed at the rightmost position in the shift register from the next block, and the operation is repeated in the same manner. The encryption and decryption operations in the CFB mode of operation are the same operations [2, 6]. Also, an error in one block will propagate to the next block, which is manifested in the process of decryption [8].

In [8] it is pointed out that the IV should be a unique identifier, e.g. a counter, whereas in [6] it is stated that the value of the IV should be a nonce. The CFB mode of operation is safe form CPA attacks only if the IV has a random value, and is not safe if the IV is a nonce [7]. Moreover, this mode of operation is not safe from CCA attacks [7]. According to [3], the encryption key needs to be changed each time condition (1) holds.

D. OFB Mode of Operation

The OFB (Output FeedBack) mode of operation (Fig. 4) also enables a block encryptor to be used as a stream encryptor. As shown in Fig. 4, the difference between the CFB and OFB mode is such that, in the case of an OFB, as an input for the shift register from the next block, the output from the encryptor (Encrypt) from the previous block is chosen. At the same time, the XOR operation with the s-bits of plain text P uses only s bits from the encryptor. Encryption and decryption are the same operation [6]. If there is an error in a block during the encryption, while performing the decryption, it will influence only a part of the plain text that will result from that block, i.e. there is a limited propagation of error [2, 3]. Therefore, this mode of operation is often used in communication through media that carry noise (for example, satellite communications).

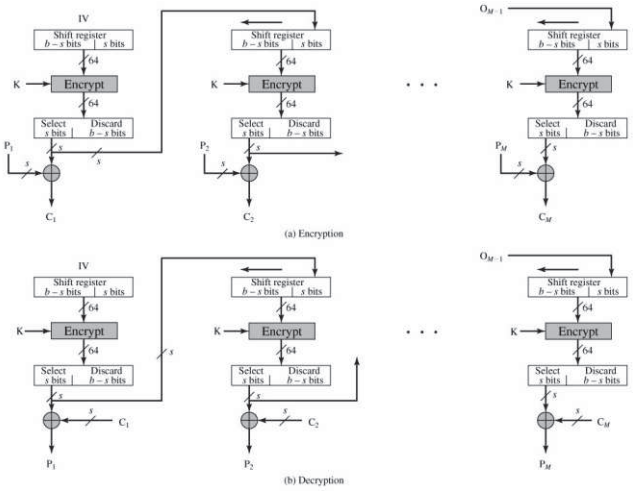

Figure 4: Scheme of OFB mode of operation [2]

According to [6], the IV should be a nonce. The guidelines given in [8] suggest that the IV should be chosen randomly and used only once with the given encryption key K. In [7] it is stated that security does not exist if the IV is a nonce, but the sequence generated by some counter is acceptable. The CFB mode of operation is vulnerable to attacks performed by modification of bits in the encrypted stream [2]. To provide security in the OFB mode of operation, the encryption key K

should be changed for every $2^{n/2}$ encryption blocks, where n is the number of bits in the block [3]. But, in [7] it is pointed out that the OFB does not offer security from CCA attacks.

E. CTR Mode of Operation

At the CTR (Counter) mode of operation, shown on Fig. 5, as an input block to the encryptor (Encrypt), i.e. as an IV, the value of a counter (Counter, Counter + 1, … , Counter + N - 1) is used.

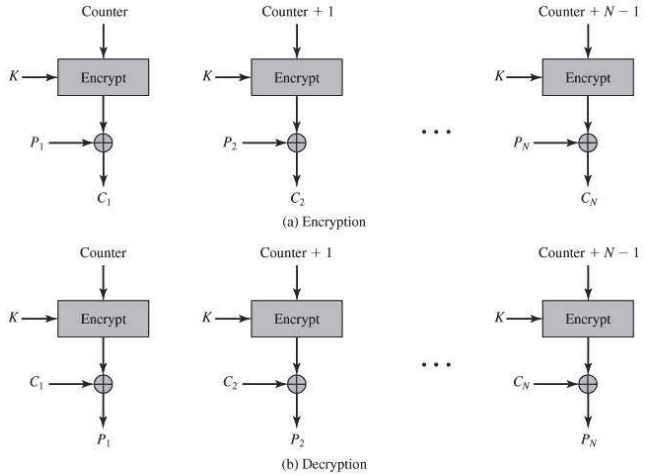

Figure 5: Scheme of CTR mode of operation [2]

The counter has the same size as the used block [2]. As shown in Fig. 5, the XOR operation with the block of plain text (P_1, P_2, … , P_N) is performed on the output block from the encryptor. All encryption blocks use the same encryption key K. If the last block of clear text P_N has the number of bits s smaller then the number of bits in the block, then only the s most significant bits for the XOR operation on the block P_N are used from the output block of the encryptor. The remaining bits are discarded. Hence, as it is pointed out in [4], there is no need for adding bits (padding) to the last block. Values of the counters are independent from the output of the previous block; therefore, there is no propagation of error from one block to another [5, 8]. Considering the independence of the blocks, this fact allows for parallelism in the encryption and the decryption, and there is also the possibility of preprocessing the values of the encryptors [2], which speeds up the process.

The encryption and decryption operations at the CTR mode of operation are the same [8]. The counter sequence should be different for every block [4]. On the other hand, in [5] and [6] it is suggested that the same value of the counter (Counter, Counter + 1, Counter + N - 1) and the same key K should not be used in the encryption of more than one block of data. If this requirement is not upheld, the plaintext can be revealed by performing the XOR operation on the two blocks of text encrypted by the same set of parameters. In that case, there is a complete breach of privacy [7]. Usually the counter is initialized to some value, and then it is incremented by one for every block [2]. In [6] it is explained that the initializing value of the counter is a non-repeatable number on the order of 96 bits. The other 32 bits are zero at the beginning of the process, and then their values are incremented by 1 for every block. The guidelines found in [8] recommend using a unique value for the Counter, chosen in a random manner. In order to ensure security with the CTR, the encryption key K should be changed for every $2^{n/2}$ blocks of encryption where n is the number of bits in a block [3]. In summation on the modes of operation in [7], the CTR mode is marked as the best choice among all the others.

III. CONCLUSION

This paper represents the ECB, CBC, CFB, OFB and CTR modes of operation of AES algorithm through analysis of the available literature. Accordingly, the requirements on their parameters to guarantee security are discussed.

Although the propagation of errors through the blocks is prevented, there are several reasons why the ECB mode of operation is considered unsuitable for implementation. During the process of encryption, the identical blocks are encrypted into identical cipher blocks, which allows for easy recognition of a repeated message. On the other hand, the attacker can change the order of the encrypted blocks, without giving it away to the receiver. Although this mode of operation is intended for encryption of the data within the size of a single block, the reviewed literature considers it as an erroneous one and abandoned, and therefore it should not be used.

Unlike the ECB, the CBC mode of operation, by means of the initialization vector – IV, when encrypting identical blocks of plaintext, produces different outputs for every block. If there is an error in a block, it will propagate through all the following blocks. The literature points out that, in order to achieve security in this mode of operation, the IV must be a random non-predictable value, and the key must be changed before encrypting $2^{(n+1)/2}$ blocks with the size of n bits. Still, the CBC mode of operation is vulnerable to PA and CCA attacks. Although CCA attacks can be avoided by using AE encryption, a considerable variety of PA attacks conclude that this mode of operation should be avoided.

The CFB mode of operation allows stream encryption. The encryption operation is the same as the decryption. An error in a block affects the other blocks. According to the reviewed literature, this mode of operation is secure in the case of CPA

attacks only if the IV has random values. The other condition for reaching security is to change the encryption key before reaching $q<<2^{(n+1)/2}$, where q is the number of blocks consisting of n bits that will be encrypted. However, this mode of operation does not offer security over CCA attacks, so, accordingly, it should not be used.

The OFB mode of operation also enables stream encryption, and the operation of encryption is used for decryption as well. An error in a block does not affect the other blocks. According to the reviewed literature, although some authors consider it acceptable to use a value for the IV generated by a counter, the value of the IV should nevertheless be chosen randomly and used only once with the given encryption key K. The security of this mode of operation is achieved if the encryption key is changed for every $2^{n/2}$ blocks of encryption, where n is the number of bits in a block. But, the reviewed literature also states that the OFB does not offer security from CCA attacks and that it is to attacks by modification of bits in the encryption stream. Therefore, this mode of operations should be avoided.

The CTR mode of operations treats the blocks independently, so there is no propagation of error from one block to another, which furthermore enables parallelism in the encryption and decryption. On the other hand, this mode allows for preprocessing outputs of the encryptors, which additionally speed up the process of encryption in general. The encryption and decryption in this mode are one and the same operation. The reviewed literature states that, in order to ensure security of this mode of operation, the same value of the counter and the same key should never be used to encrypt more than one block of data. If this is not so, there will be a complete breach of privacy. According to the reviewed literature, the counter should be assigned a unique random variable. Also, to ensure security in the CTR mode, the encryption key K should be changed for every $2^{n/2}$ blocks of encryption, where n is the number of bits in the block. In the reviewed literature, no negative aspects of this mode could be found. On the contrary, it is considered to be the best.

The analyzed literature clearly shows that every mode of operation has parameters which require careful and correct selection and implementation. On the other hand, regardless of the appropriate selection of parameters, the majority of modes of operation are not secure because they are vulnerable to various attacks. Accordingly, it can be concluded that irregular implementation of modes of operation can compromise the security of the AES algorithm (in general) and to contribute in revealing part of the plain text or the entire message.

Taking into account the positive and negative sides of the analyzed modes of operation of the AES algorithm, it can be concluded that, for its proper and secure implementation, the CTR mode of operation should be implemented.

REFERENCES

[1] J.A. Buchmann. *Introduction to Cryptography*. NY, Springer, 2001

[2] W. Stallings. Cryptography and Network Security : Principles and Practices. Fourth Edition. NJ, Prentice Hall, 2005

[3] H.C.A. Tilborg ed. *Encyclopedia Of Cryptography And Security*. NY: Springer Science+Business Media, Inc, 2005

[4] N. Dworkin. "Recommendation for Block Cipher Modes of Operation, Methods and Techniques". *NIST Special Publication 800-38A Edition 2001*, available at: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf, [last accessed on December 20, 2012]

[5] F.R. Henriquez, N.A. Saqib, A.D. Perez and C.K. Koc. *Cryptocraphic Algorithms on Reconfigurable Hardware*. NY, Springer, 2006

[6] C. Paar and J. Pelzl. Understanding Cryptography : Textbook for Students and Practitioners. London, Springer, 2010

[7] P. Rogaway. "Evaluation of Some Blockcipher Modes of Operation". *Cryptography Research and Evaluation Committees (CRYPTREC)*, 2011, available at: http://www.cryptrec.go.jp/estimation/techrep_id2012_2.pdf [last accessed on December 16, 2012]

[8] ISO/IEC FCD 10116. "Information technology - Security techniques-Modes of operation for an n-bit block cipher". 3rd edition. Geneve: ISO, 2006, available at: http://www.nhzjj.com/asp/admin/editor/newsfile/2010318171240586.pdf [last accessed on December 13, 2012]