2022 IEEE Smart Information Systems and Technologies (SIST)
28-30 April, 2022, Nur-Sultan, Kazakhstan

Analysis of block ciphers characteristics for CBC and OFB modes when input data are shifted

1st Zhanna Alimzhanova
Department of Information System of Al-Farabi Kazakh Nationl University, Department cybersecurity Almaty academy of the ministry of internal affairs of the Republic of Kazakhstan named after M. Esbulatov
Almaty, Kazakhstan
0000-0001-6282-5356

2nd Dauren Nazarbayev
Department of Information System of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0001-7505-0422

3rd Akzer Tleubergen
Department of Information System of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0002-1178-4491

4th Aivar Alimzhanov
Department of Mechanics of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0002-9924-7091

***Abstract*— This article presents a comparative analysis of DES and AES block ciphers in the CBC and OFB operating modes. In order to identify some regularities, the authors applied a multiple encryption method to determine the dynamics of block ciphers in the two modes of operation CBC and OFB. As a result of the study with different control input data, some regularities were obtained, in CBC mode symmetric matrices are obtained, in OFB mode a clear periodicity with respect to a certain number of iterations of data encryption is evident. For clarity, all the results of the study have been presented in the form of two-dimensional matrices.**

Keywords: DES, AES, block cipher mode, CBC, OFB, multiple encryption

I. INTRODUCTION

This article investigates DES (Data Encryption Standard) and AES (Advanced Encryption Standard) block ciphers to analyze the behavior of CBC (Cipher Block Chaining) and OFB (Output Feedback Mode) with different input data [1], [2], [3]. For the study, the authors have applied a multiple data encryption approach, which can be used to trace the dynamics of changes in block ciphers and the periodicity of the ciphertext. In terms of the characteristic features of each mode, some regularities with respect to blocks (sets of blocks) and iterations (sets of iterations) are derived. Regardless of the choice of block cipher, in the CBC mode the symmetry of the data sequence under certain input data manifests itself in multiple encryptions of the data. The practical significance of this work consists in the analysis of modes of operation of block ciphers to identify the main characteristics of the behavior of the encrypted texts for further study of the cryptographic strength of the studied ciphers. One of the characteristics of cryptographic strength of ciphers is the unpredictability of elements of the encrypted sequence [4]. If we find any regularity or periodicity, we have some support for predicting which sequence elements to expect in the future. In this paper, DES and AES block ciphers were chosen to perform a comparative analysis of the dynamics of ciphertexts with different inputs [9].

AES is a symmetric block encryption algorithm [2]. It replaced DES, which no longer meets the requirements of network security [3]. AES can be implemented in software, hardware, and firmware. The implementation may use a table lookup process or procedures using a clear algebraic structure. The conversion can be byte-by-byte or word-by-word. In general, AES can be described as a symmetric block cipher in which all operations within the algorithm work with 8 or more bits. The encryption block accepts plain text of 128, 192 and 256 bits [1]. The key for encryption and decryption is represented as a square matrix of bytes. The algorithm supports a 128-bit block and a 128-bit key, a 192-bit key and a 256-bit key. In the case of a 128-bit key, 10 rounds are used, for a 192-bit key 12 rounds are used, and for a 256-bit key 14 rounds are used [1]. For example, if each round can use different rounds for 128-bit code, it can be called a real key for AES. The relevance of the study is that since data encryption belongs to the field of cryptography, the use of encryption systems in the field of information protection is large and there are many different algorithms that allow encryption. The main criterion for each method is its cryptographic strength.

The following describes two modes of operation of the algorithm, which are provided for block symmetric encryption algorithms [5].

In CBC mode, each block of plaintext is pre-encrypted with the result of encrypting the previous block using the XOR operation. An initialization vector is added to the first block of plaintext, which generates a random image and is usually transmitted along with encrypted data so that it can be decrypted.

In CBC mode, to encrypt each subsequent block, you must have the result of encrypting the previous block in order to encrypt several blocks at once. But it is possible to decrypt several blocks in parallel, while only this block and the previous one should be used to decrypt each block.

The OFB mode operates on the principle of a synchronous stream cipher, generating key stream blocks, using an XOR operation to stack with the plaintext blocks to encrypt the data. As in CBC mode, OFB mode uses an initialisation vector as part of the control input data to encrypt the data.

II. COMPARATIVE ANALYSIS OF DES AND AES BLOCK CIPHERS IN CBC MODE

The first object of study is the CBC mode. For the analysis of the CBC mode, various control input data were selected, which are presented in Tables I, II, and III [6], [7].

TABLE I. CONTROL INPUT DATA

Input data	DES	AES
Plaintext	$\underbrace{\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}}_{8\text{ blocks}}$	$\underbrace{\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}}_{8\text{ blocks}}$
Key	$\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}$	$\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}$
Init. vector	$\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}$	$\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}$

TABLE II. CONTROL INPUT DATA

Input data	DES	AES
Plaintext	$\underbrace{\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}}_{8\text{ blocks}}$	$\underbrace{\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}}_{8\text{ blocks}}$
Key	$\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}$	$\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}$
Init. vector	$\underbrace{[1,1,\dots,1]}_{8\text{ numbers}}$	$\underbrace{[1,1,\dots,1]}_{16\text{ numbers}}$

TABLE III. CONTROL INPUT DATA

Input data	DES	AES
Plaintext	$\underbrace{\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}}_{8\text{ blocks}}$	$\underbrace{\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}\dots\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}}_{8\text{ blocks}}$
Key	$\underbrace{[1,1,\dots,1]}_{8\text{ numbers}}$	$\underbrace{[1,1,\dots,1]}_{16\text{ numbers}}$
Init. vector	$\underbrace{[0,0,\dots,0]}_{8\text{ numbers}}$	$\underbrace{[0,0,\dots,0]}_{16\text{ numbers}}$

To analyze the behavior of the CBC mode when the control input data specified in in Tables I, II, and III the authors used the method of multiple encryptions to identify patterns. In this paper, the control input data is selected from 8 blocks and 8 iterations.

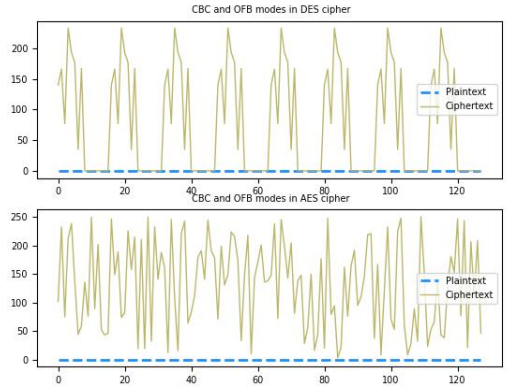

Figure 1. Visualisation of data from eight blocks in CBC and OFB modes in DES, AES algorithms at the first encryption iteration

Figure 1 shows the result of encrypting eight blocks of data in CBC and OFB modes in DES and AES algorithms of the first iteration when control input data from Table 1 [8]. On the first iterations in CBC and OFB modes, the results are the same for both DES and AES algorithms [9].

To illustrate the results of the study, it is best to present it in the form of a matrix. Each element in the matrix represents some encrypted sequence of a certain block and iterations.

Only one element of the entire sequence can be displayed as an element, instead of the entire length of the sequence of each block. For example, instead of the entire sequence consisting of [140, 166, 77, 233, 193, 177, 35, 167] elements, the first element will be selected as the matrix element: 140. Each column of the matrix is a block of an encrypted sequence, each row is the number of iterations of multiple encryptions. To distinguish one matrix from another, we will introduce the designation of matrices by capital letters of the English alphabet. Consider the following matrix:

$$A = \begin{pmatrix} 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 140 & 140 & 0 & 0 & 140 & 140 & 0 \\ 140 & 140 & 140 & 0 & 140 & 140 & 140 & 0 \\ 0 & 0 & 0 & 140 & 140 & 140 & 140 & 0 \\ 140 & 0 & 140 & 140 & 140 & 140 & 140 & 0 \\ 0 & 140 & 140 & 140 & 140 & 140 & 140 & 0 \\ 140 & 140 & 140 & 140 & 140 & 140 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 140 \end{pmatrix}$$

$$B = \begin{pmatrix} 102 & 247 & 161 & 71 & 148 & 20 & 167 & 53 \\ 247 & 102 & 237 & 73 & 1 & 12 & 107 & 176 \\ 161 & 237 & 102 & 58 & 182 & 227 & 171 & 164 \\ 71 & 73 & 58 & 102 & 238 & 255 & 217 & 184 \\ 148 & 1 & 182 & 238 & 102 & 206 & 89 & 41 \\ 20 & 12 & 227 & 255 & 206 & 102 & 233 & 182 \\ 167 & 107 & 171 & 217 & 89 & 233 & 102 & 20 \\ 53 & 176 & 164 & 184 & 41 & 182 & 20 & 102 \end{pmatrix}$$

Here A and B are 8x8 matrices consisting of DES and AES algorithm encryption results, respectively, with control inputs from Table I.

By analyzing the elements of matrices, A and B in CBC mode, we see a regularity in the fact that these matrices are symmetric matrices relative to the main

diagonal. In CBC mode, in matrix A, periodicity is manifested by columns, rows and the main diagonal, in matrix B, periodicity is manifested only by the main diagonal.

$$C = \begin{pmatrix} 153 & 1 & 153 & 1 & 153 & 1 & 153 & 1 \\ 42 & 57 & 61 & 200 & 34 & 154 & 235 & 14 \\ 57 & 140 & 10 & 120 & 88 & 46 & 59 & 1 \\ 199 & 91 & 93 & 140 & 53 & 48 & 72 & 30 \\ 165 & 11 & 16 & 69 & 238 & 212 & 27 & 181 \\ 91 & 94 & 203 & 4 & 140 & 223 & 102 & 1 \\ 248 & 63 & 2 & 175 & 179 & 175 & 199 & 251 \\ 110 & 95 & 60 & 37 & 210 & 46 & 30 & 251 \end{pmatrix}$$

$$D = \begin{pmatrix} 225 & 116 & 216 & 159 & 144 & 185 & 47 & 125 \\ 102 & 155 & 139 & 250 & 163 & 75 & 48 & 147 \\ 15 & 241 & 163 & 131 & 150 & 246 & 139 & 167 \\ 9 & 160 & 100 & 2 & 151 & 132 & 46 & 92 \\ 8 & 137 & 56 & 70 & 62 & 210 & 117 & 158 \\ 234 & 187 & 49 & 216 & 111 & 109 & 32 & 20 \\ 33 & 245 & 125 & 123 & 121 & 48 & 126 & 35 \\ 40 & 117 & 141 & 164 & 72 & 199 & 121 & 185 \end{pmatrix}$$

Matrices C and D are obtained when the input data from Table II. The difference between these matrices from the previous matrices considered is that here, due to the change in the initialization vector, the matrices appeared in a different form, namely, in these matrices there is no symmetry and periodicity, except in matrix C, periodicity appears only in the first row.

The following matrices E, F show the encryption results by the control input data of Table III.

$$E = \begin{pmatrix} 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 140 & 140 & 0 & 0 & 140 & 140 & 0 \\ 140 & 140 & 140 & 0 & 140 & 140 & 140 & 0 \\ 0 & 0 & 0 & 140 & 140 & 140 & 140 & 0 \\ 140 & 0 & 140 & 140 & 140 & 140 & 140 & 0 \\ 0 & 140 & 140 & 140 & 140 & 140 & 140 & 0 \\ 140 & 140 & 140 & 140 & 140 & 140 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 140 \end{pmatrix}$$

$$F = \begin{pmatrix} 182 & 100 & 190 & 121 & 240 & 192 & 90 & 84 \\ 100 & 182 & 53 & 182 & 174 & 118 & 47 & 98 \\ 190 & 53 & 182 & 85 & 209 & 220 & 233 & 99 \\ 121 & 182 & 85 & 182 & 114 & 209 & 180 & 229 \\ 240 & 174 & 209 & 114 & 182 & 104 & 51 & 29 \\ 192 & 118 & 220 & 209 & 104 & 182 & 108 & 175 \\ 90 & 47 & 233 & 180 & 51 & 108 & 182 & 164 \\ 84 & 98 & 99 & 229 & 29 & 175 & 164 & 182 \end{pmatrix}$$

These E and F matrices show the same regularities as the A and B matrices discussed above.

The next object of study is the OFB mode III [6], [7]. When the control inputs from Tables I, II and III the following matrices are obtained by multiple encryptions, which shows a clear periodicity in the DES algorithm by blocks and by iterations, in the AES algorithm by iterations only.

$$G = \begin{pmatrix} 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$H = \begin{pmatrix} 102 & 247 & 161 & 71 & 148 & 20 & 167 & 53 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 102 & 247 & 161 & 71 & 148 & 20 & 167 & 53 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 102 & 247 & 161 & 71 & 148 & 20 & 167 & 53 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 102 & 247 & 161 & 71 & 148 & 20 & 167 & 53 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Here G and H are 8x8 matrices consisting of DES and AES algorithm encryption results, respectively, with control inputs from Table I. I, J matrices, respectively, from Table II, and K, L matrices, respectively, from Table III.

$$I = \begin{pmatrix} 153 & 1 & 153 & 1 & 153 & 1 & 153 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 153 & 1 & 153 & 1 & 153 & 1 & 153 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 153 & 1 & 153 & 1 & 153 & 1 & 153 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 153 & 1 & 153 & 1 & 153 & 1 & 153 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$J = \begin{pmatrix} 225 & 116 & 216 & 159 & 144 & 185 & 47 & 125 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 225 & 116 & 216 & 159 & 144 & 185 & 47 & 125 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 225 & 116 & 216 & 159 & 144 & 185 & 47 & 125 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 225 & 116 & 216 & 159 & 144 & 185 & 47 & 125 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$K = \begin{pmatrix} 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 140 & 0 & 140 & 0 & 140 & 0 & 140 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$L = \begin{pmatrix} 182 & 100 & 190 & 121 & 240 & 192 & 90 & 84 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 182 & 100 & 190 & 121 & 240 & 192 & 90 & 84 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 182 & 100 & 190 & 121 & 240 & 192 & 90 & 84 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 182 & 100 & 190 & 121 & 240 & 192 & 90 & 84 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

III. Conclusion

In this article, symmetric DES and AES block ciphers were chosen for the study and investigated in two modes of operation CBC and OFB with different input data. To analyze the characteristics of the block ciphers, the authors applied the data re-encryption method to reveal some regularities [10]. To illustrate the identified features in this research work, all the encryption results have been represented as a two-dimensional matrix. All modifiable control inputs were represented in three tables I, II and III. In these tables, the plaintext consists of 8 blocks. The following results have been obtained by investigating the two modes: in CBC mode with different inputs from tables I and III, symmetric matrices are obtained: matrices A, B, E and F. In DES algorithm, periodicity in blocks, iterations and main diagonal is observed. In the AES algorithm, it is only on the main diagonal. In OFB mode, all its matrices: G, H, I, J, K and

L show explicit periodicity, in DES algorithm periodicity is observed with respect to blocks and iterations [11], in AES algorithm - only iterations. To implement the DES and AES encryption algorithms and obtain the results, the authors used the Python programming language, which contains the Crypto.Cipher package that contains data privacy algorithms [12].

REFERENCES

[1] J. Daemen and V. Rijmen, *AES Proposal: Rijndael, AES Algorithm Submission*, September 3, 1999.

[2] National Bureau of Standards, DES modes of operation, U.S. Department of Commerce, *FIPS 81* (1980)

[3] Advanced Encryption Standard, National Institute of Standards and Technology, U.S. Department of Commerce, *FIPS 197* (2001)

[4] Korchynskyi, Volodymyr, et al. "The generating random sequences with the increased cryptographic strength." *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska* 10 (2020).

[5] Rogaway, Phillip. "Evaluation of some blockcipher modes of operation." Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan (2011)

[6] Zh. Alimzhanova, D. Nazarbayev, S. Zhunusbayeva, A.Ayashova “Analysis of the behavior ciphertexts on the example of a block symmetric AES algorithm in ECB, CBC, OFB and CFB modes, using the multiple encryption method” unpublished.

[7] Zh. Alimzhanova, Sh. Mussiraliyeva, D. Nazarbayev, A. Kaliyeva “Evaluative analysis of behavior in symmetric Vigenère and DES encryption algorithms under conditions of various complexity modes of operation” unpublished.

[8] Alenezi, Mohammed N., Haneen Alabdulrazzaq, and Nada Q. Mohammad. "Symmetric encryption algorithms: Review and evaluation study." *International Journal of Communication Networks and Information Security* 12.2 (2020): 256-272.

[9] Vaidehi, M., and B. Justus Rabi. "Design and analysis of AES-CBC mode for high security applications." *Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014*. IEEE, 2014.

[10] Soni, Shraddha, Himani Agrawal, and Monisha Sharma. "Analysis and comparison between AES and DES Cryptographic Algorithm." *International Journal of Engineering and Innovative Technology (IJEIT)* 2.6 (2012): 362-365.

[11] Nachef, Valérie, Jacques Patarin, and Emmanuel Volte. "Feistel ciphers." *Cham: Springer International Publishing* (2017).

[12] Sweigart, Albert. *Hacking Secret Ciphers with Python*. Al Sweigart, 2013.