AN ANALYSIS OF DIFFERENT CHAINING MODES IN SYMMETRIC CRYPTOGRAPHIC ALGORITHMS APPLIED IN DIGITAL IMAGE TRANSMISSION

Djordje Sarcevic
Academy of Professional Studies, Department of Medical and Business-Technological Studies, Sabac, Serbia, sarcevicdjordje@vmpts.edu.rs

Dragan Rudnjanin
Faculty of Technical Science, University of Pristina in Kosovska Mitrovica, Kosovska Mitrovica, Serbia, rudnjanin.dr@gmail.com

Ana Djokic
Information Technology School ITS Comtrade, Belgrade, Serbia, ana.djokic@its.edu.rs

Hana Stefanovic
Information Technology School ITS Comtrade, Belgrade, Serbia, hanapopstefanovic@gmail.com

Abstract:
In this paper the analysis of the difference between Electronic Code Book (ECB) chaining mode and Cipher Block Chaining (CBC) mode in secure data transmission is given. Advanced Encryption Standard (AES) encryption algorithm is applied while transmitting digital image. Some simulation results, presenting the advantage of using CBC mode, are also provided. A free e-learning software CrypTool is used to create the simulation model and analyze the simulation results.

Keywords: Advanced Encryption Standard (AES) algorithm, Electronic Code Book (ECB) chaining mode, Cipher Block Chaining (CBC) mode, CrypTool programming tool

INTRODUCTION

Many algorithms are used in order to encrypt sensitive data. The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the United States government to protect classified information [1]. The National Institute of Standards and Technology (NIST) started to develop AES in 1997 [2] when it announced the need for an alternative to the Data Encryption Standard (DES), which became vulnerable to brute-force attacks [7]. AES encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 or 256 bits. It is a symmetric algorithm, which means it uses the same secret key for encryption and decryption data. Both the sender and the receiver must know and use the same secret key. There are several steps followed in AES while encrypting or decrypting blocks of data: Add Round Key, Sub-Bytes, Shift Rows and Mix Columns, which are repeated in each round.

AES is widely used in many applications which require secure data storage and transmission [3], such as: wireless security [4], especially in Wi-Fi networks in order to ensure data confidentiality and prevent unauthorized access, in database encryption to protect personal information, financial records, and other confidential data from unauthorized access in case of a data breach [5], in different protocols for internet communications [6], email, instant messaging, and voice/video calls, in order to ensure that the data remains confidential. AES is also used to encrypt sensitive data stored on hard drives, USB drives, and other storage media, protecting it from unauthorized access in case of loss or theft, and for secure storage of passwords. In order to secure the password storage, their encrypted versions are stored instead of storing plaintext passwords.

Electronic Codebook (ECB) is essentially the first generation of the AES. It is the most basic form of block cipher encryption [8], while Cipher Blocker Chaining (CBC) is an advanced form of block cipher encryption. With CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point [9]. This adds an extra level of complexity to the encrypted data.

In this paper both modes ECB and CBC are analyzed and some simulation results are also provided. A digital image is chosen as data to be transmitted, in order to present the difference between ECB and CBC mode.

SIMULATION MODEL

The model is created in CrypTool programming environment [10]. The plaintext, which is a digital image converted to binary format, is encrypted using the AES algorithm, as it is presented in Fig.1. The upper branches presents an implementation of ECB mode, while the lower branches presents an implementation of CBC mode in order to chain the cipher blocks.

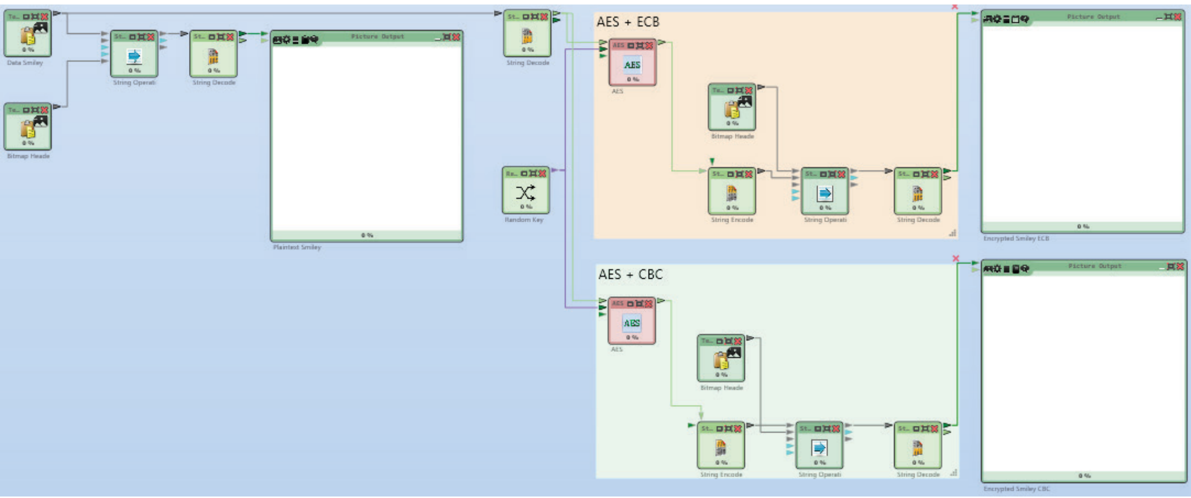
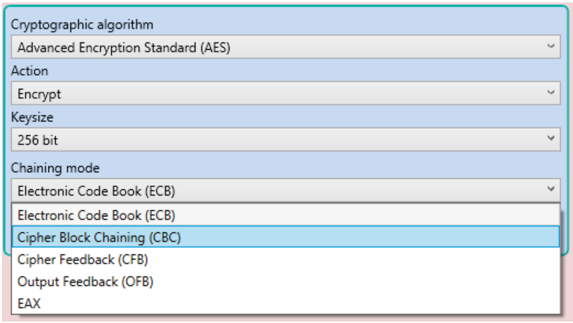


Fig.1.The simulation model of AES encryption/decryption

In the process of encryption/decryption, a 256-bit AES key length is used, as it is presented in Fig.2. The 256-bit key is significantly more difficult for brute-force attacks than 192-bit key or 128-bit key.



Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
256 bit
Chaining mode
Electronic Code Book (ECB)
Electronic Code Book (ECB)
Cipher Block Chaining (CBC)
Cipher Feedback (CFB)
Output Feedback (OFB)
EAX

Fig.2.AES key and chaining modes

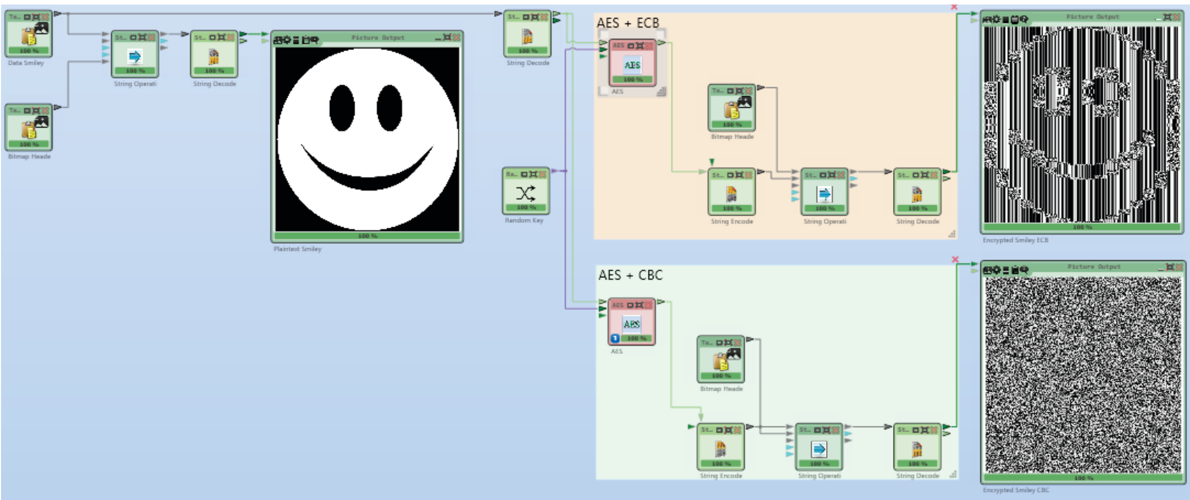


Fig.3.The simulation results for different chaining modes

SIMULATION RESULTS AND DISCUSSION

Simulation results are presented in Fig.3. By comparing results both in the lower and the upper branch, it can be concluded that even if a picture is encrypted, its content may remain recognizable due a wrong chosen chaining mode.

ECB does not chain the cipher blocks while CBC does. The result using ECB is, that every plaintext block, for instance for instance all white and all black blocks, are encrypted to the same cipher block, so the structure of the picture remains visible, as it is shown in Fig.4.

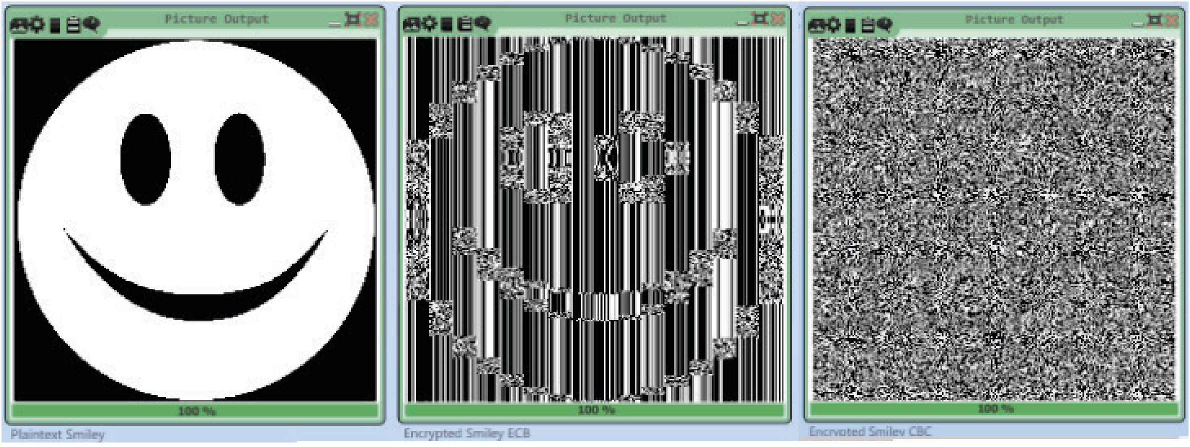


Fig.4.Comparing original image (a) with ECB encrypted image (b) and CBC encrypted image (c)

The result using CBC is, that every plaintext block, even if they were the same, are encrypted to a different cipher block. This happens, because all cipher blocks were connected using the CBC chaining mode. Thus, no structure remains and everything is hidden.

In the case when ECB mode is applied, each block of ciphertext that is encrypted is independent of other cipher blocks, whereas in CBC each block of ciphertext is dependent on the corresponding current input plaintext as well as a previous plaintext block. ECB mode doesn't use a feedback mechanism whereas CBS uses it. As the consequence, if a plain text block is repeated in the original message, ECB mode generates the same ciphertext block for each corresponding plaintext block, whereas CBC mode generates different ciphertext blocks for each corresponding plain text block.

CBC mode ensures that if the block of plain text is repeated in the original message, it will produce a different ciphertext for corresponding blocks, while ECB mode produces the same ciphertext blocks if the block of plain text is repeated in the original message. Some advanced cipher techniques and cipher modes are used to improve the security of data transmission of multifunctional sensors and Internet of Things (IoT) nodes [11] in wireless sensor networks.

CONCLUSION

A cryptographic protection against attacks and malicious penetration is determined by the strength of the keys and the effectiveness of mechanisms and protocols associated with the keys and the protection of the keys through key management.

The choice of block cipher mode is also very important, as it is presented and illustrated in this paper.

REFERENCE

[1] Trang H, Loi VN. An efficient FPGA implementation of the Advanced Encryption Standard. In Proceedings of International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), DOI:10.1109/rivf.2012.6169845, 2012.

[2] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES), 2001.

[3] Gupta A, Ahmad A, Sharif MS, Amira A. Rapid prototyping of AES encryption for wireless communication system on FPGA. In Proceedings of International Symposium on Consumer Electronics (iSCE), 2011, p. 571-575.

[4] Karimian GH, Rashidi B, Farmani A. A High Speed and LowPower Image Encryption with 128-Bit AES Algorithm. International Journal of Computer and Electrical Engineering, vol. 4, no. 3, 2012.

[5] Daemen J, Rijmen V. The Design of Rijndael: The Advanced Encryption Standard (AES) (Information Security and Cryptography), Springer, 2nd ed., 2020.

[6] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2nd ed, 2000.

[7] Ferguson N, Schneier B, Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2nd ed, 2010.

[8] Rogaway P. Evaluation of Some Blockcipher Modes of Operation, Technical report. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, 2011.

[9] Dworkin M. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. NIST Special Publication 800-38E, 2010.

[10] https://www.cryptool.org/en/, 2023 (date of access)

[11] Y. Guo, L. Li, B. Liu. Shadow: A Lightweight Block Cipher for IoT Nodes. IEEE Internet of Things Journal, vol. 8, no. 16, pp. 13014-13023.