The Advanced Encryption Standard Block Cipher "Different Modes"

BICS- Sean ACHTATOU

University Of Luxembourg

E-mail : sean.achtatou@hotmail.be

1.INTRODUCTION

The Advanced Encryption Standard is an application known worldwide, used to Encrypt and Decrypt any data in security on your computer. The goal of this project is to understand if the security does really exist, and to not get fooled by anything providing a 100% security rate.

2.PROJECT DESCRIPTION AND BACKGROUND

The Advanced Encryption Standard Block Cipher concerns one of the most studied computing domain of the worldwide, the security. The notion of the Cryptography and Block Cipher need to be acquired.

The main objective of this project is to understand how works each parts of the algorithm of the Advanced Encryption Standard Block Cipher, then put them all together to get a clear overview of how it works. The need to implement the algorithm of the Advanced Encryption Standard is necessary. Thanks to that, the possibilities to manipulate the algorithm, deleting, adding parts, will help to understand how each parts are useful as the others.

This project will also work on three different modes for the Advanced Encryption Standard. Among these modes: the ECB [Electronic Book], the CBC[CipherBlockChaining] and the CTR[Counter]. These three modes will have their structure analyzed such as the Advanced Encryption Standard had, then compared between them to watch the Encryption result got each time for each one.

Some constraints must be considered. The first one is the comprehension of the different domains mentioned upper above. The second is the implementation of the algorithm of the Advanced Encryption Standard Block Cipher. Here, the language chosen was Python, indeed, it is a language quite easy to understand and to implement for anyone. This project provided consequently a new way to see how is implemented a security application and a new language to learn.

3. THE ADVANCED ENCRYPTION STANDARD [128 BITS/THREE MODES]

3.1. Requirements and design

The main requirement of this project is to first deliver a new wide idea about the conception of the real security image of the Advanced Encryption Standard or any other security system in the world. The user should apprehend the easy insecurity of the transmission of information that can happen if the system is not correctly mastered.
The user should be able to understand perfectly how works the Advanced Encryption Standard algorithm for each mode. The user should know each parts of each algorithm, and consequently being capable to compare after, by himself, the algorithm of any security system to others security system.
By using a programming language Python, the user should understand each lines written in the project. However, the use of this language should provide to the user a new type of programming language he didn't know or a possibility to master it.
This project works around three modes, there exist several others study on this subject providing others modes than those three worked with. Consequently, some parts might not be exploited in this project. This project will not considerate much about the Decryption of the Advanced Encryption Standard in any mode. The Decryption of the Advanced Encryption Standard, only being the inverse operation.
The project is focused on only those three modes for the Advanced Encryption Standard: ECB, CBC and CTR. The choice to choose those three is because there exist always a common and different point between them. Indeed, the ECB is using independent blocks [no connection]; CBC is using dependent blocks [connected between each other's] and an Initialization

Vector; and the CTR is using a Counter which will pass in the Advanced Encryption Standard Algorithm. For the design, as said the project work on the three modes: ECB, CBC and CTR. Each of the mode will contain each times, fixed table at the top of the code then will pass the data in the Advanced Encryption Standard Algorithm. The Advanced Encryption standard is structured like this: Initial Round [function: AddRoundKey (XOR each case of the Block Cypher of the data with the main random key)]; Rounds [functions: SubBytes (pass each case of the Block Cipher in a SubstituteBox), ShiftRows (Shift each rows of the data), MicColumns (transform each case of the date depending on multiples fix tables), AddRoundKey XOR each case of the Block Cypher of the data with the expansion key)] and Final Round providing the same functions but without the Mixcolumns.

3.2. Production and Assessment

In the production we did test all the three modes enumerated below: ECB, CBC and CTR.
At first, we took care of the ECB mode: provides independent block ciphers and no particularities. The result got were surprising. Some lines were just repeating over and over. By analyzing the clear data, we notice that those repetitions were the same letters. In fact, this mode would be really bad to encrypt data unless you were only encrypting maximum 16 characters. Still, the error propagation (a bit is providing an error compiling) wouldn't be a problem with it since it is independent.
With CBC: provides dependent blocks and an Initialization Vector [Random 128 Bits Block Cipher]. The result was more positive, no repetition or any security issues. Still with this mode the issue that can happen is with the error propagation, since it is using dependent blocks, the error would be propagated all along the encryption and would corrupt the data.
And CTR: provides independent blocks and a Counter. Here it is the Counter that were going through the Advanced Encryption Standard Algorithm. The result was similar to the CBC except this one wouldn't have difficulties to deal with the propagation error as CBC does.
The assessment was satisfied. The three modes have been analyzing in all their sides as the algorithm of the Advanced Encryption Standard and we have seen that the CBC and CTR were better than the ECB. The only bad thing is for the Decryption issues encountered during the project, even this one didn't talk much about it, the inverse MixColumns function was acting strangely with Windows.

3.CONCLUSION

In conclusion, the modes ECB is not recommended while CBC and CTR are highly recommended. Still it is depending on what data you are inputting in each mode. But even if the Encryption was satisfying, none security program is 100% secured.