ABSTRACT

A secure cryptosystem could be very complicated, time consuming and hard to implement. Therefore, the complexity of the cryptosystem should be taken into account during design and implementation. In this work, the authors introduce a comprehensive and platform independent complexity analysis for a class of symmetric block cryptosystems, by which it will be easier to evaluate the performance of some used cryptosystems. Previous works lacked the comprehensiveness in their analysis, due to the fact that the memory access time was completely ignored, which greatly degrades the accuracy of the analysis and limits it to one data block only. In this paper the authors analytically compute the complexity for a class of symmetric cryptosystems in terms of the number of the clock cycles required and in terms of the required time for encryption/decryption, independently of the hardware or software used in the encryption/decryption process. Moreover, this is the first complexity analysis that considers the required time to access and retrieve information from memory, which makes the analysis more comprehensive and accurate than previous work as well as being general for any number of encryption data blocks. In addition, computer simulations are used to truly evaluate the accuracy of the analysis and to show how the analytical results match the simulation results.

Keywords: 3-DES, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Encryption Complexity, Modified Data Encryption Standard (M-DES)

DOI: 10.4018/jisp.2013010105
INTRODUCTION

Encryption is becoming a primary part of any wired or wireless communication technology, due to the increased threat of attackers and their ability to access secure and confidential information. However, in addition to the fact the encryption algorithm should be as secure as possible and very hard for the attacker to break, the encryption process should be fast and should be able to use hardware and software resources efficiently. Therefore, the complexity is a major factor that needs to be considered in choosing an encryption algorithm in addition to the efficiency of the algorithm in terms of its strength against attacks as stated in Kamruzzaman (2008). The complexity of encryption algorithms can be measured in terms of the number of logical and arithmetic operations, which can be translated to clock cycles and eventually into time as shown in Y. Xiao (2005), F. Granelli (2004), R. Tomoiaga (2010), Soyjaudah, K. S. (2007). However, these works lacked the comprehensiveness in computing the complexity, due to the fact that the memory access time was ignored in all of the previous analysis, which effectively degraded the accuracy of their analysis. In addition, the analysis the authors introduce in Y. Xiao (2005), F. Granelli (2004), R. Tomoiaga (2010); Soyjaudah, K. S. (2007) is only performed for the first encryption block, by ignoring the memory access time their analysis can not be generalized to any number of blocks. The uniqueness of the work presented in this paper is in fact based on the consideration of the required time to access and retrieve data from the memory in addition to the number of logical an arithmetic operations performed on the retrieved data, hence the complexity analysis is generalized to any number of encrypted blocks rather than just being limited to the first block. Moreover, the proposed analysis is independent of any platform that could be used to implement the cryptosystems under study. Furthermore, we use computer simulations to show that the proposed analytical results match the simulation results.

The rest of the paper is organized as follows: In the second section, we analytically compute the complexity of the data encryption standard (DES), triple-DES (3-DES), advanced encryption standard (AES) and the modified data encryption standard (MDES). Simulation results, comparisons and some discussions are presented in the third. Finally some conclusions are drawn in the fourth section.

ANALYTICAL COMPLEXITY ANALYSIS

In this section we provide analytical derivation for the time required for encryption using different symmetric block cryptosystems. We perform the analysis for DES, 3-DES, AES and M-DES cryptosystems. In this analysis, we will break down the operations performed on the data for each cryptosystem into simple byte-wise AND, OR, XOR, Shift and memory access operations. In general, the total required time to encrypt one block of data is given by the number of operations that are required to encrypt this data block multiplied by the clock cycle time for each operation. The following equation gives a general method for computing the total time required to encrypt one data block using any cryptosystem

\[
T_{encr} = (N_{xor} \times T_{xor}) + (N_{and} \times T_{and}) + (N_{or} \times T_{or}) + (N_{shift} \times T_{shift}) + (N_{ma} \times T_{ma}),
\]

where \(T_{encr}\) is the total encryption time for one data block, \(N_{xor}, N_{and}, N_{or}, N_{shift}\) and \(N_{ma}\) are the number of clock cycles required to perform one byte-wise XOR, AND, OR, Shift and memory access operations respectively. And \(T_{xor}, T_{and}, T_{or}, T_{shift}, T_{ma}\) are the clock cycle times for one byte-wise XOR, AND, OR, Shift and memory access operations respectively.

The number of clock cycles required to perform each operation will depend on the instruction set architecture that is used. For example, in Intel x86 one byte-wise XOR operations requires 3 clock cycles as stated in T. Shanley (2009). While the clock cycle time depends on the processor speed that is in the
Related Content

Methods for Counteracting Groupthink Risk: A Critical Appraisal
[www.igi-global.com/article/methods-for-counteracting-groupthink-risk/106027?camid=4v1a](www.igi-global.com/article/methods-for-counteracting-groupthink-risk/106027?camid=4v1a)

Local Resident Perceptions of Border Security Dynamics: Are Citizens Safe or Intimidated?
[www.igi-global.com/article/local-resident-perceptions-of-border-security-dynamics/106029?camid=4v1a](www.igi-global.com/article/local-resident-perceptions-of-border-security-dynamics/106029?camid=4v1a)

Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy
[www.igi-global.com/chapter/surveillance-public-spaces-means-protecting/50410?camid=4v1a](www.igi-global.com/chapter/surveillance-public-spaces-means-protecting/50410?camid=4v1a)
Applying Enterprise Risk Management on a Fiber Board Manufacturing Industrial Case
[www.igi-global.com/article/applying-enterprise-risk-management-on-a-fiber-board-manufacturing-industrial-case/120557?camid=4v1a](www.igi-global.com/article/applying-enterprise-risk-management-on-a-fiber-board-manufacturing-industrial-case/120557?camid=4v1a)