"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 2
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

A SURVEY ON SYMMETRIC TEXT ENCRYPTION ALGORITHMS

Elena BAIBARAC[1]
[1]"Politehnica" University of Bucharest, Bucharest, Romania

Abstract: *In this paper we consider a survey on encryption algorithms. Several security analysis are presented as secret key size, secret key sensitivity, frequency with histograms, autocorrelation analysis, information entropy analysis, differential analysis, classic attacks analysis, and encryption/decryption time. The framework for information entropy analysis is developed on new generalized entropy measures.*
Keywords: *Encryption, Entropy, Information Theory, Security*.

I. INTRODUCTION

Nowadays, the main way people use to communicate and store data is based on the use of the Internet. That is the reason why the information security becomes a very important issue to deal with. Any message that is being sent through the internet can be understood by anybody who is aware of the language in which the text is written, as long as the message is not encrypted.

Cryptography comes in help whenever sending any confidential and sensitive information over a public channel is needed, without being intercepted by an eavesdropper who could steal the information. Cryptography is the art of achieving security by encrypting messages. The concept cryptography is based on, is that A, who wants to transmit a message to B, applies an encryption process to the message, and sends it across the channel. B, who knows the decryption process that he has to apply, recovers A's original message. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Cryptographic algorithms can be based on symmetric key or public key cryptography.

The two most famous symmetric key algorithms are Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES). From these ones, AES is considered to be the best one, because it has the advantage of low memory space and also, speed and known to be based-in permutation-diffusion architecture.

II. THE STATE OF THE ART

Murillo-Escobar et al. [2] used a 128 bits secret key in a 32 digit hexadecimal format and performed a security analysis. The algorithm developed provides a big secret key size to resist a force-brute attack, all secret keys are considered strong, it is sensitive at secret key and plain text, it can resist an entropy attack, it is robust against classic attacks, and the encryption time is fast. Therefore, the algorithm proposed can encrypt text with high performance, high security.

Haleem et al. [1] proposed the so called opportunistic encryption framework, which uses channel opportunities, i.e. acceptable signal to noise ratio with the goal of maximizing the throughput subject to desired security constraints. They have developed mathematical models to capture the security-throughput trade-off, adversary models and their effects, joint optimization of encryption and modulation, for the single and multirate case. Also, they used forward error correcting codes in order to protect encrypted packets from bit errors. Performing simulations for Rijndael cipher they have obtained that opportunistic encryption produces significant improvement in the performance compared to alternative approaches.

Frequency with histograms

Frequency analysis is based on the fact that in any written language, certain letters and combination of letters occur with varying frequencies. The best way to be able to find the plain text or maybe the secret key is to analyze the frequency with histograms. If the distribution of the symbols in a cipher text is uniform, the text has a very good chance to resist a frequency attack. On the other way, if the distribution is not uniform, it reveals a weak encryption scheme.

Autocorrelation and differential cryptanalysis

Autocorrelation means that a text is compared to shifted copies of the same text. The characters from both texts, that match each other in such a comparison, are determined. The autocorrelation analysis is said to be more efficient and clearer than the Friedman or Kasiski test because of its versatility.

As for differential analysis, the attack relies on the fact that a given input/output pattern only occurs for certain values of inputs. The attack is usually applied to the non-linear components, and by observing the desired output difference suggests possible key values. In essence, for an n-bit non-linear function one would ideally seek as close to $2^{-(n-1)}$ as possible to achieve *differential uniformity*. When this happens, the differential attack requires as much work to determine the key as simply brute forcing the key. For example, AES has a 4/256 maximum differential probability, and it is very possible to resist to differential attack even with a much weaker non-linear function.

SYMMETRIC TEXT ENCRIPTION USING SHAFEE ENTROPY

Entropy represents a fundamental concept of the information theory. Entropy maximization represents one of the fundamental principles in statistical physics. It states that systems, within the

boundary of their limiting constraints, always tend towards a state of maximal disorder, called maximal entropy. The maximal entropy principle states that, when given some information about a random variable, the least biased probability distribution is obtained by maximizing entropy subject to the given constraints. Considering a complex system whose output is a real-valued random variable, the output corresponding to the maximal entropy under the constraints of a given mean and a given standard deviation is given by the Gauss distribution. The maximal entropy principle has been used to solve problems arising in many fields [3, 4].

We consider a message *m* and denote by *N* the number of bits of this message. Thus, the number of all possible symbols is 2^N. We denote by m_i a possible combination obtained by the message *m* and by $p(m_i)$ the probability of m_i.

We will evaluate the entropy corresponding to a message *m* by using the Shafee entropy, defined as follows:

$$\mathrm{E}(m) = -\sum_{i=0}^{2^{N-1}} [\, p(m_i)]^q \log p(m_i)\,. \qquad (1)$$

CONCLUSIONS

In terms of Cryptography, entropy must be supplied by the cipher for injection into the plaintext of a message so as to neutralize the amount of structure that is present in the unsecure plaintext message. The method used for entropy measurement depends on the cipher.

By increasing the entropy we obtain the increasing of the degree of security of the encryption.

ACKNOWLEDGMENT

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/187/1.5/S/155536.

BIBLIOGRAPHY:

[1] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshm," Opportunistic Encryption: A Trade-off between Security and Throughput in Wireless Networks, *IEEE Transactions on Dependable Computing*, 4, 4, pp. 313-324, 2007.

[2] M. A. Murillo-Escobar, F. Abundiz-PÈrez, C. Cruz-Hernandez, R. M. Lopez-Gutierrez, "A novel symmetric text encryption algorithm based on logistic map", *Proceedings of the 2014 International Conference in Communications, Signal Processing and Computers*, 2014.

[3] V. Preda, "On maxentropic reconstruction of countable Markov chains and matrix scaling problems", *Studies in Applied Mathematics*, 111 (1), pp. 85-100, 1994.

[4] V. Preda, "The Student distribution and the principle of maximum entropy", *Annals of the Institute of Statistical Mathematics Mathematics*, 34 (1), pp. 335-338, 1982.

[5] F. Shafee, "Lambert function and a new non-extensive form of entropy" IMA Journal of Applied Mathematics 2007, 72, 785-800