International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Review of a New Distinguishing Attack Using Block Cipher with a Neural Network

Vina M. Lomte[1], Archana D. Shinde[2]

[1]Professor Computer Engineering department, RMD Sinhgad College of Engineering, Pune, Maharashtra, India
[2]M.E. Computer Engineering department, RMD Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: ***This paper describes a new distinguishing type attack to identify block ciphers, which grounded in a neural network, by means of a linguistic approach and an information retrieval approach, from patterns which is found on a ciphertexts set collection. The ideas were performed on a set of ciphertexts, which were encrypted by the finalist algorithms of AES contest: MARS, RC6, Rijndael, Serpent and Twofish; each one has a unique 128-bit key. This experiment shows the processes of clustering and classification were successful, which allows the formation of well-formed and well-defined groups, here ciphertexts encrypted by the same algorithm stayed close to each other.***

Keywords: Distinguishing attack; neural networks; cryptography; block ciphers

1. Introduction

In general, there are two types of attacks namely passive attacks and active attacks. The Passive attack means interception which includes Release of message contents and Traffic analysis. The Active attack means Interruption, modification, fabrication which includes Masquerade, Replay, Modification, and Denial of service. Cryptography algorithms (or ciphers) must be resistant to different kinds of attacks. The majority of ciphers are grounded on hard mathematical problems, i.e., there is not known way to solve that class of problems in a feasible computational time. However, those theoretical attacks can be useful to understand the capacity of generate randomness of a cipher. This capacity is used as a measure of strength of a cipher.

For instance, we have the linear cryptanalysis and the differential cryptanalysis. in theory, all block ciphers are susceptible to differential and linear cryptanalysis. In this context, this work proposes a new distinguishing attack against block ciphers. The attack is based on a neural network. Which is capable to cluster n ciphers, for any value of n. the experiments are performed for a specific case of n = 5, for the ciphers: mars, rc6, rinjdael, serpent and two fish; each one has a unique 128-bit key. Those five ciphers were the finalist of the AES (advanced encryption standard) cipher contest. The experiments were successful, forming well-defined and well formed clusters, where cipher texts encrypted by the same algorithm stayed closed to each other, from a topological standpoint. Additional experiments allow identifying the ciphers, taking in account the clusters previously formed. by analogy, this attack can be classified as a ciphertext.

The remaining of this work is organized as follows. in section ii, we will present the fundamentals of cipher identification including the fundamentals of cryptography and neural networks. in section iii, we detailed describes the proposed methodology. in section iv, we express the anatomy of the proposed attack. in section v, we explain the experiments and results and in section 6 we present the conclusion.

2. Theoretical Fundamentals for Cipher Identification

2.1 A hard problem to solve with unconventional application

According to the design principles of ciphers, that cannot leak or propagate any information in the ciphertext which can reveal details of the plaintext, for that, the cryptographic key used or the cipher that encrypted the plaintext. This, it is a hard problem to identify a cipher only taking in account the ciphertexts. Even though, it remains as a hard task since a ciphertext has no structure and, a priori, we can't infer any type of information related to the lexical, syntax or semantic of a ciphertext.

2.2 Cryptosystem

A cryptosystem can be defined by 5 tuple (P, C, K, E, D), with the conditions that are follows:

a) P={p1,p2,…,pn} is a finite set of possible plaintexts;
b) C={c1,c2,…,cn }is a finite set of possible ciphertexts;
c) K={k1,k2,…,kn} is a finite set of possible cryptographic keys;
d) E={e1,e2,…,en} , is a finite set of possible encryption rules;
e) D={d1,d2,…,dn} , is a finite set of possible decryption rules.

2.3 Block cipher

It is consists of a cryptographic process, that transforms blocks of bits of plaintext to blocks of bits of ciphertext. The bit block size can be determined according to some cryptographic parameter, such as: the algorithm, the size of the key or the number of rounds in the algorithm. In this, we use block of size n bit, where n =128.

2.4 Mode of operation

The goal of a mode of operation is to improve the application's result of a cipher or prepare a cipher to a particular use or, yet, determine specific functionalities for an application.

2.5 Taxonomy of cryptanalytics attacks

The task of cryptanalysis is also called as attack that is in general classified according to the information available and according to the objective and necessity of the attacker. The attacks are listed as follows, in a decrescent order of difficulty:

a) Ciphertext only: the cryptanalyst has just the ciphertext.
b) Known plaintext: the cryptanalyst has how many plaintexts and its respective ciphertexts, as he wish.
c) Chosen plaintext: the cryptanalyst has access to the cipher and thus, he chooses the plaintexts to be encrypted.
d) Adaptative chosen plaintext: the cryptanalyst can modify the plaintexts chosen according to the results of previous tests.

2.6 Vector space model for ciphertexts:

In this, vectors are represented in ciphertexts.

3. Methodology for Cipher Identification

There are two methodologies are used for cipher identification as follows:

3.1 Modelling Ciphertexts Over a Vector Space

The vector space model is used in the task of modelling a document collection. Thus, a collection of cryptogram can be modelled in vector space So, in order to represent the ciphertexts it may be used vectors of n-dimension, where n is the number of distinct blocks over collection of cryptogram, and where each block represents an axis on the vector space and, a point in the vector space computed a ciphertext (figure 1).

In the figure 1 we can observe that the ciphertexts 1, 2 and 3 are points in the space, represented by the coordinates (X, Y, Z), (X, 0, Z) and (0, Y, Z), respectively.

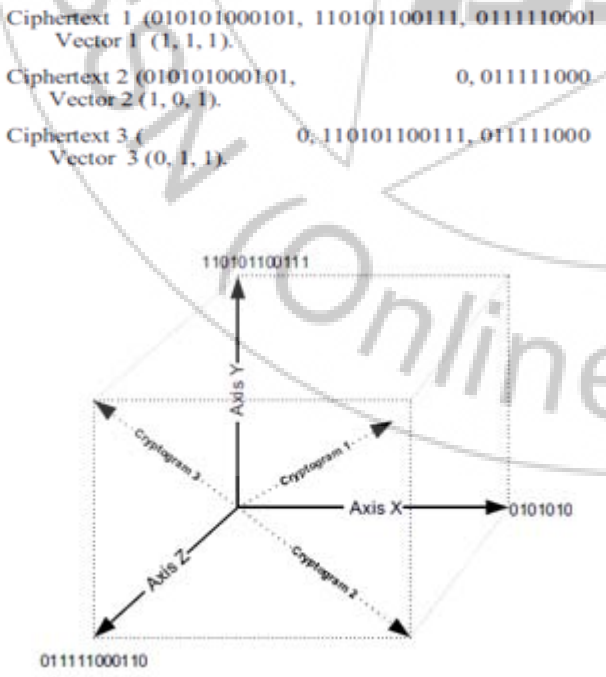

Figure 1: Ciphertexts Vector Space Model

3.2 Self-Organizing Neural Network

A self-organizing neural network is a mathematical model which has suitable properties to perform clustering of patterns. The neural network is composed from a set of neurons. Each neuron is with a synaptic weight vector of n-dimension assigned to it.

$$m_{\cos}(\vec{c_i}, \vec{sw_j}) = \frac{\sum_{k=1}^{n}(c_{i,k} \times sw_{j,k})}{\sqrt{\sum_{k=1}^{n}(c_{i,k})^2 \times \sum_{k=1}^{n}(sw_{j,k})^2}}$$

Where:

$\vec{c_i}$ is a vector representing the ciphertext i; $\vec{sw_j}$ is the synaptic weight vector of the neuron j; $c_{i,k}$ is the block k from the ciphertext i; and $sw_{j,k}$ is the weight k from the synaptic weight vector of the neuron j.

The above formula is used to determine the value of each neuron in the network, taking as a base the ciphertext vector and the synaptic weight vector of this neuron. This computing can be performed using the cosine angle.

4. Anatomy of the Attack

The aim of the distinguishing attack is identify a cipher that encrypted a ciphertext from a set of ciphertexts. In this sense the clustering as well as classification processes are suitable for the given task. In the proposed attack one or more ciphers from a collection of ciphertexts can be identified, as presented in following figure 2.

This distinguishing attack proposed is passive. In the proposed architecture, a sender sends a message which is encrypted by any of algorithm and a receiver receives the message normally. An attacker monitoring the information channel, collect passively the encrypted messages and composes a ciphertexts collection.

After that, they submit the ciphertexts collection to the clustering process, obtaining as much possibleas many clusters as it is the number of ciphers that had encrypted the ciphertexts. After clustering the ciphertexts and obtain the clusters, the attacker can get a new ciphertext from the information channel, submits it to the classification process, which tests the new ciphertext against the existents clusters, and identifies the correct cluster that it belongs to. As each cluster is co-related to just one cipher, this process consequently identifies the cipher. If the classification process is not able to identify the cipher, it will state that a new cipher (unknown) was identified.

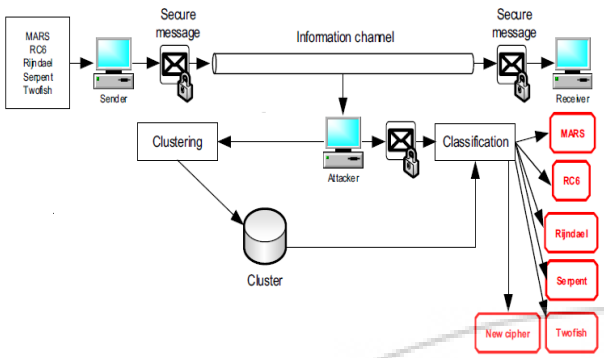

Figure 2: The attack scheme in a scenario with 5 ciphers

5. Experiments, Result and Evaluation

Initially, we start performing a test experiment with languages in order to check the capacity of the neural network clustering languages. It is utilized 30 plaintexts for each of two sizes: 6144 and 8192 bytes.

5.1. Plaintexts and Ciphertexts Collections

A collection is composed by 240 plaintext, each one has about 6144 bytes, for each of the following languages, represented by follow color, respectively (30 texts for each language): Portuguese (yellow), Spanish (magenta), French (black), German (blue), Danish (cyan), Dutch (orange), Greek (green) and Hebrew (red).

5.2 Test Experiment: Clustering of Languages

Observing the two-dimensional map formed (Figure 3), it can be concluded that the clustering was successful. The languages used in the experiment indicate the existence of eight natural clusters, each cluster identify a language following the colour scheme planned. In the map, each small colored square represents a plaintext learned by each neuron and the neurons are represented by a gray big square.

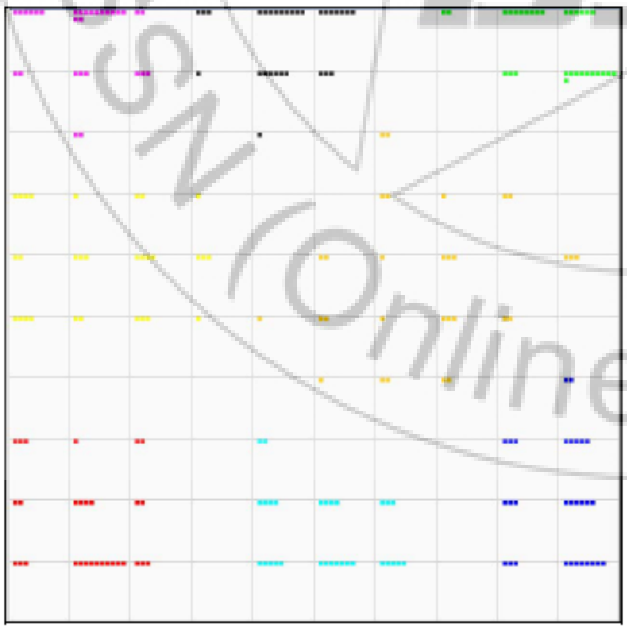

Figure 3: Result for the Text Experiment

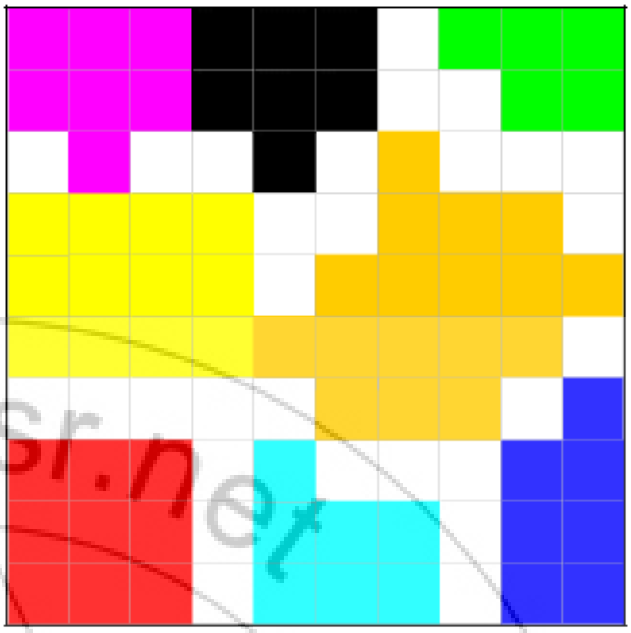

Figure 4: Formed Clusters for the Test Experiment

In figure 4, we have a better view of the formed clusters. Here we can see that the pattern of colors in the two-dimensional map and the plaintexts contents, we can clarify that the texts of languages that share more common words which are topologically closest.

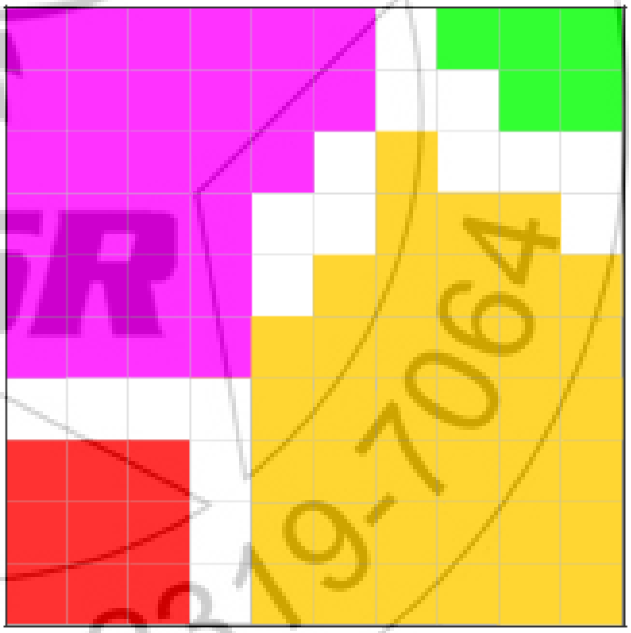

Figure 5: Formed Clusters for the Test Experiment in a higher level

Observing the two-dimensional map formed (Figure 5) it can be noted that it shares more and more common texts of languages with different alphabets that results in the clusters were well-formed and well-defined. The color patterns are clearly put into neurons, with no inaccuracies.

5.3 Clustering by Cipher

The goal of this experiment is to distinguish the cryptograms into five clusters therefore; each cluster contains cryptograms generated by the same cipher and only by it. Finally, the neural network was configured with 400 neurons, with

blocks of 16 bytes (128 bits) to carry out the training phase using the measure of cosine angle, and neighborhood size of 400, i.e. all neurons.

5.4 Cipher Identification by Classification

The goal of this experiment is classifying the ciphertexts into the clusters previously formed. Then, if the classification is successful the distinguishing attack is also successful. They are used 45 ciphertexts generated by five finalist algorithms of AES contents: MARS (orange), RC6 (red), Rijndael (magenta), Serpent (black) and Twofish (blue). In the classification process was used 400 neurons.

Observing the two-dimensional map formed (following figure 6) we observed that the classification process was successful, where all new ciphertexts submitted to the neural network were classified in the correct cluster.

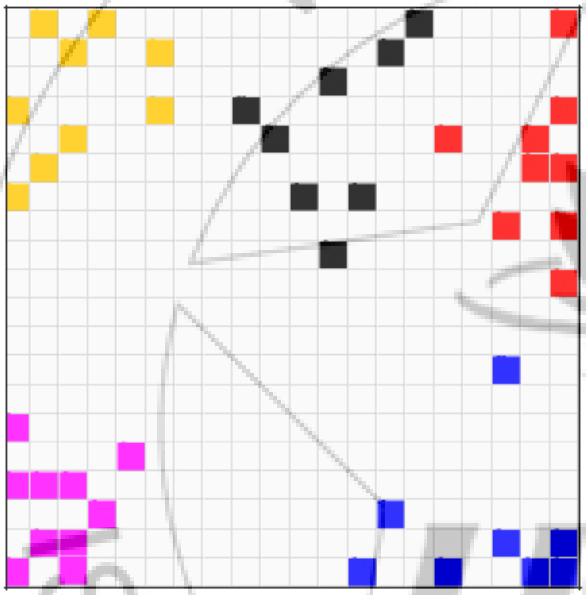

Figure 6: Cipher classification

6. Conclusion

This work generates a new distinguishing attack which based on a neural network (self-organizing map). The attack clusters, classifies and consequently identifies block ciphers by means of a linguistic approach, from patterns found on a ciphertexts set. The experiment proposes that the correct identification of the algorithms depends on the appropriate configuration of the neural network.

References

[1] W. A. R. de Souza, J. A. M. Xexeo, G. A. Oliveira and R.Linden, "Identification of Keys and Cryptographic Algorithms Using Genetic Algorithm and Graph Theory". IEEE Latin America Transactions, v. 9, p. 178-183, 2011.
[2] W. A. R. de Souza, L. A. V. Carvalho and J. A. M. Xexeo, Identification of N Block Ciphers. IEEE Latin America Transactions, v. 9, p. 184-191, 2011.
[3] L. Fausset, Fundamentals of neural networks: architectures, algorithms, and applications, Prentice Hall, 1994.
[4] W. A. R. de Souza, J. A. M. Xexeo and C.M.G.M. Oliveira," Method for clustering cryptograms by means of cryptographic key", Anais do IV Workshop Algoritmos Data mining, 2008.
[5] W. Stallings, Cryptography and network security: principles and practice, 5th ed, Prentice Hall, 2010.
[6] NIST, Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38A. Revision 1. Washington D.C., 2001
[7] M. Matsui, "Linear cryptanalysis method for DES cipher". In Eurocrypt 1993, volume 765, LNCS, Journal of Cryptology, Springer-Verlag.
[8] A. D. Dileep and C. C Sekhar, "Identification of block ciphers using support vector machines," in International Joint Conference on Neural Networks (IJCNN 2006), Canada, July 2006.
[9] N. Fergunson, B. Schneier and T. Kohno. Cryptography engineering: design principles and practical applications, Wiley, 2010.
[10] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of applied cryptography, CRC Press, 1996.
[11] B. Schneier, Applied cryptography: protocols, algorithms and source code in C, Addison-Wesley, 1996.
[12] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology, Springer-Verlag, 1991, 4(1): pp.3 – 72.
[13] S. Nagireddy, A Pattern Recognition Approach to Block Cipher Identification. Master of Science Dissertation – Indian Institute of Technology Madras. http://lantana.tenet.res.in, 2008.

Author Profile

Archana D. Shinde received the B.E. degree in Computer Engineering from Pune University in 2011 and Pursuing M.E. degree in Computer Engineering from Pune University.

Vina M. Lomte received the B.E. degree in Computer Science and Engineering from Amravati University – BNCOE- , Pusad and ME in Computer Engineering from Mumbai University - MGMCET- Kamothe.