Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Neural Cryptanalysis of Block Cipher

Shweta Pandey
Dept. of comp. science and engineering
RCET, Bhilai, India

Prof. Megha Mishra
Dept. of comp. science and engineering
SSCET, Bhilai, India.
megha16shukla@gmail.com

***Abstract*— In this paper Neural Network is applied in the field of cryptanalysis of Block cipher based on their ability to selectively explore the solution space of a given problem. New algorithm is proposed that offers a new approach to attack ciphering algorithms based on the principle that any function could be reproduced by a neural network. Neural Network and Feistel block cipher is explained. A complete problem formulation is explained. Conclusion and References are given as appropriate.**

***Keywords*— Block cipher, Cryptanalysis, Feistel Network, Neural Network, Plain Text.**

I. INTRODUCTION

Cryptology is the art and science of making secret codes and breaking secret codes. Cryptography is the technique to camouflage the message, and only intended recipients can remove the camouflage and read the message. The message we want to send is called plaintext and the camouflage message is called cipher text. The process of converting a plaintext into cipher text is called encryption and the reverse process is called decryption Cryptanalysis is the process of recovering the plaintext and/or key from a cipher.

Cryptanalysis of block cipher is a challenging task due to non-linearity in nature. Many cryptographic systems have a finite key space and, hence, are vulnerable to an exhaustive key search attack. Yet, these systems remain secure from such an attack because the size of the key space is such that the time and resources for searches are not available. Ayman M.B.Albassal and Abdel-Moneim A.Wahdan [1] have used the concept of interpolation attack. Their proposed attack has the benefit of being parallel by nature and can be easily extended to a distributed version. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

Saptarshi Neil Sinha Supravo Palit, Mostafiz Amin Molla, Atreyee Khanra, Malay Kule [2] presents a cryptanalytic attack on Merkle-Hellman Knapsack cipher using Differential Evolution.

Joseph Alexander Brown, Sheridan Houghten [3] provides a preliminary exploration of the use of Genetic Algorithms (GA) upon a Substitution Permutation Network (SPN) cipher. The purpose of the exploration is to determine how to find weak keys.

In this paper back propagation neural network is used to find out the plain text from cipher text. In neural network by using some function value we will get output as plain text from cipher text using weight values by mathematical calculation in Feistel rounds. We are having two simultaneous value of cipher text and by applying the reverse method we will get final plain text.

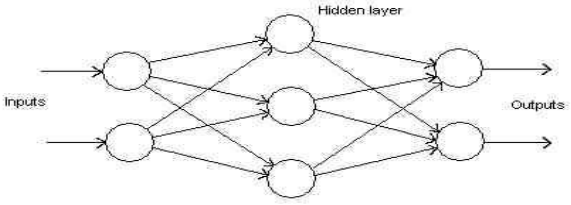
Cryptanalysis can be done either by transposition or substitution. Here cryptanalysis is done by substitution. We calculate the key value by applying mathematical formula of feistel on simultaneous cipher text values. That key is the unique weight value to calculate the output from neural network.

II. NEURAL NETWORK

The network functions as follows:

Each neuron receives a signal from the neurons in the previous layer, and each of those signals is multiplied by a separate weight value.

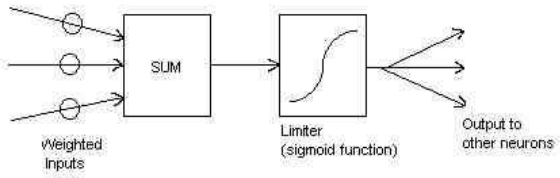
The weighted inputs are summed, and passed through a limiting function which scales the output to a fixed range of values. The output of the limiter is then broadcast to all of the neurons in the next layer. So, to use the network to solve a problem, we apply the input values to the inputs of the first layer, allow the signals to propagate through the network, and read the output values.



A Generalized Network [10] by Pete McCollum. Stimulation is applied to the inputs of the first layer, and signals propagate through the middle (hidden) layer(s) to the output layer. Each link between neurons has a unique weighting value.

The Structure of a Neuron [10] by Pete McCollum. Inputs from one or more previous neurons are individually weighted, then summed. The result is non-linearly scaled between 0 and

+1, and the output value is passed on to the neurons in the next layer.



Back Propagation Neural Network:

Here are some situations where a BP NN might be a good idea:

- A large amount of input/output data is available, but you're not sure how to relate it to the output.
- The problem appears to have overwhelming complexity, but there is clearly a solution.
- The solution to the problem may change over time, within the bounds of the given input and output parameters (i.e., today 2+2=4, but in the future we may find that 2+2=3.8).
- Outputs can be "fuzzy", or non-numeric.

III. FEISTEL CIPHER

Most of the old attacks on simple ciphers were based on comparing the statistical characteristics of the cipher output and the language of the used cipher text. For example, knowing that the most frequent letter in the English language is the letter **E,** leads to full discovery of the key used in the Caesar cipher, which is a simple substitution cipher **[**4**].**Shannon proposed to protect the cipher against the statistical analysis of its output by utilizing a product cipher, which is an approximation to the ideal block cipher [5]. A product cipher performs two or more basic ciphers in sequence in such a way that the resultant cipher is cryptographically stronger than any of it components. Shannon cipher alternates confusion and diffusion [6].

Diffusion dissipates the statistical information of the plain text in a longer range of statistical structure of the cipher text. It makes a single plain text bit affects many bits in the cipher text or, equivalently, makes each cipher text bit a function of many plain text bits [4]. Diffusion can be implemented by applying some permutation on the input bits and applying some other function on the output of the permutation. This mechanism makes bits from different positions in the plain text contribute in the production of a single bit in the cipher text, thus complicating the relation between the statistics of the input text and the output cipher text. Confusion works in the same way as diffusion but applied to the output bits and the key bits [7]. Confusion can be implemented by applying complex non-linear substitution mapping keyed by the key bits. Knowing any information about the statistics of the cipher text, the attacker will have no idea about how the key bits were used to produce that output.

Feistel proposed a general structure that applies Shannon concepts. The basic Feistel block cipher with five rounds are shown in Figure 1. Feistel alternates the use of substitution and permutation [5].

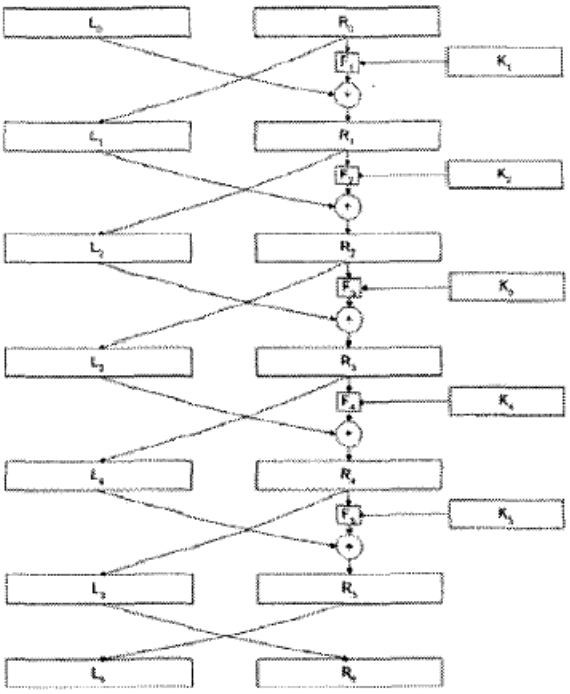


Figure 1. A five round Feistel Network.

As shown in Figure 1**[1],** Feistel cipher gets a block of 2n bits of plain text and produces a 2n bits block of cipher text. Each block is divided into two halves: left **(L)** and right (R) ones. The **2** halves block passes through a number of rounds (in our case they are ***5*** and a final rounds). In each round, an initial permutation of the right half into the left half is done. Then, the right half is passed through a keyed function. The keyed function, *F*, uses an m bits key (usually ***m*** = ***n).***To map ***n*** bits input to ***n*** bits output. Finally, the output is mixed with the left half with an XOR.

If the input block to round i is $\mathbf{L_{i-1}R_{i-1}}$ the output of the round is described by Equations 1 and 2 as follows:

$$L_i = R_{i-1}$$

$$R_i = F_i (R_{i-1}, K_i) \oplus L_i$$

After the final round, there is s block permutation round that gives the Feistel cipher a very interesting characteristic, That is, decryption is basically an encryption with reversed order keys and functions (Ki, Fi).

Encryption is performed by passing the 2n bits block through rounds and decryption is, as described above, is by passing the cipher text through the system but with reversed order keys and functions. This implies that we do not need to implement separate encryption and decryption algorithms.

IV. PROPOSED WORK

As in neural network after applying some mathematical calculation on input we get output, so here cipher text is taken as an input and by adding weight function we get output as plain text. This procedure work in reverse direction as we are

having two simultaneous cipher text values. Suppose we are having the cipher text of 16 bit.So according to Feistel cipher round it is divided into L8 and R8. So according to the equations of Feistel Network

L8=R7
K=R8-L8-L7
K=R8-R7-L7

So from the above concept we find C7 from C8 and C6 from C7 and in the same way C1from C2.And finally we get plain text from C1 by using the key. So in reverse order by using neural network we find out the plain text.

V. CONCLUSION

Neural Network is used for cryptanalysis tool. It is not restricted and can be applied for other block ciphers also. The paper also indicates that it is a much better and efficient technique. The inclusion of this new technique will force the creation of defenses against it. Differential and linear attacks have lead to the creation of security against them. We believe this being used to break non-classical ciphers to be an interesting, emerging field of research which must be expanded upon in upcoming years.

References

[1] Ayman M. B. Albassal and Abdel-Moneim A. Wahdan1993. Neural Network Based Cryptanalysis of a Feistel Type Block Cipher.

[2] Saptarshi Neil Sinha1, Supravo Palit 2, Mostafiz Amin Molla3, Atreyee Khanra4 , Malay Kule51997 A Cryptanalytic Attack on Knapsack Cipher Using Differential Evolution Algorithm.

[3] Joseph Alexander Brown, Sheridan Houghten, *Member, IEEE,* and Beatrice Ombuki- Genetic Algorithm Cryptanalysis of a Substitution Permutation.

[4] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press 1997, ISBN: 0-8493- 8523-7.

[5] Howard M. Heys,"A Tutorial on Linear and Differential Cryptanalysis", Cryptologia, vol. **XXVI,** no. 3, pp. 189-221, 2002Cryptologia, vol. XXVI, no. 3, pp. 189-221, 2002

[6] H. Feistel, "Cryptography and Computer Privacy", Scientific American, vol. 228, no. 5, pp. 15-23, 1973.

[7] C. E. Shannon, 'Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, pp. 656-715, 1949.

[8] R. P. Lipmann, "An introduction to computing with neural networks", IEEE ASSP Magazine, pp. 4-22, Apr. 1987.

[9] National Institute of Standards, Advanced Encryption Standard (AES) web site: http: l/www.nist eoviaes

[10] An Introduction to Back-Propagation Neural Networks by Pete McCollum Saipan59@juno.com

[11] Khalil Shihab (2006). "A back propagation neural network for computer network security". *Journal of Computer Science 2*: 710–715.

