American Journal of Industrial and Production Engineering
1(1):7-8, August 2019.

RANDOMIZATION-BASED BLOCK CIPHER WITH KEY-MAPPED S-BOX SELECTION

Krishna Yadav, University of Central Missouri, Warrensburg, US
Warron Pietman,Professor, University of Central Missouri, Warrensburg, USA

ABSTRACT

ABSTRACT This paper proposes a new system of Substitution-Permutation network along with Randomization Expansion of 240 bits of input data. System uses 16 S-Boxes which are selected randomly based on the subkey values throughout 64 rounds of substitution steps. 64 sub-keys are generated during the SubstitutionPermutation process. The middletext is transposed based on decimal value of the sub-key generated during the each round. A CBC mode is the best associated with this system.

KEYWORDS

Middletext, Randomization, SP-network, S-Box, CBC

1. INTRODUCTION

In this internet world every transaction of data is confidential. Day by day the importance of the information security is exponentially increasing. Any organization that relies on transmitting the data is prone to an attacker on the network. Under these critical circumstances we need to protect our data using Cryptographic algorithms [2,4,5] which morph the data before transmitting over networks or store it in a physical location. Cryptography [2,4,5] is a field of study where the data is secured by changing it to non-readable format using different types of algorithms. Every algorithm has its own merits and demerits. In this paper we proposed a new approach to randomize the substitution and permutation which will remove any linearity of the system.

2. RANDAMIZATION EXPANSION

Randomization [1] provides a set of ciphertexts corresponding to message and key pair. A 16-bit string is generated randomly which is used] to XOR the 240-bit plaintext. Later this 16-bit random generated string is appended to the XOR-ed output of 240-bit plaintext keeping the bandwidth expansion factor [1] to 1.066 and possible ciphertexts to 65,536 for a message and key pair. This is achieved by dividing 16-bit random generated string into 4 equal halves i.e., 4 halves of 4 bits each and XOR 240 bits of plaintext. The output obtained after XOR is concatenated [1] with 16-bit random generated string

3.ROUGH DESIGN

There are 64 rounds in the substitution-permutation network. Each round consists of a substitution from the S-Box and a permutation which is a left circular shift. Later after permutation the middletext is XOR with a subkey. We have 16 S-Boxes numbered from 0 to 15. The S-Box for that specific round is selected by the subkey K1. As the subkey K1 is 4 bit the decimal value of it lies always between 0 and 15. Using a S-Box which is selected based on the key will make analysis difficult because each time key changes the order of selection of S-Boxes changes. To substitute bits from the S-Box the subkey K2 is used. the subkey K2 chooses the row of values to be substituted from the selected S-Box. The corresponding middletext values are substituted from the S-Box. Now a permutation, a left circular shift is applied. The value of how many bits needs to be shifted is derived from the subkey K3 and K0. The subkeys K3 and K 0 oth are concatenated [1] to form 8 bit string. Now the decimal value of this 8 bit string is used to perform the left circular shift on the middletext.

4. EVALUATION

a. Plaintext - Ciphertext

correlation Plaintext - CIphertext correlation [2,5,6] gives us a statistical weakness of the algorithm. This is taken greater care while developing the algorithm. By any means for the same set of Plaintext and the Key, Ciphertext will not be the same for different executions because of the Randomization expansion. And flipping a bit in the Plaintext or Key will never have the same Ciphertext bit positions changed. An analysis is done on large set of input Plaintexts at different levels in the encryption algorithm to observe how many bits are changed from the input to output. First level of observation is on the Randomization expansion. This gives a clear idea of how many bits are changed in the level of Randomization expansion. We are 95% confident that 128.1117 bits are changed during this level. The summary of the analysis is as followed.

b. S-Box security

The most non-linear part of the algorithm is the Substitution-Permutation network [4,5,6]. The design criteria of each S-Box are as follows.

1) Each S-Box takes 4 input bits and gives 4 output bits.

2) The output bits are not related with any of the input bits. The values of the S-Box are random generated fixed values.

3) Each S-Box has 256 substitution values which is a 16x16 matrix. The values follow the rules

5. CONCLUSION

In this paper we illustrated new approach of encrypting and decrypting the data using a symmetric key. This approach can be applied on any file formats which can be read as binary data. In this paper we used 240 bit plaintext as our block size, further enhancements can be done on increasing the block size. The ciphertext is of length 256 bits which 16 bits of it is a data head because of randomization expansion. A possible future enhancement can be the removal of 16 bits data head but still should be able to do randomization expansion.

REFERENCES

[1] Rivest, Ronald L., and Alan T. Sherman. "Randomized encryption techniques." In Advances in Cryptology, pp. 145-163. Springer US, 1983.

[2] Schneier. B, Applied Cryptography, Second Edition: protocols, algorithms, and source code in C. New York: Wiley, 1996.

[3] Dworkin, M., NIST Special Publication 800-38A, 2001 Edition: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, December 2001, Natl. Inst. Stand. Technol. [Web page], http://www.csrc.nist.gov/publications/ nistpubs/800-38a/sp800-38a.pdf

[4] I. Tanenbaum, AS.: “Computer Networks” 2nd edition, Prentice Hall, London. 1989

[5] Cryptography and Network security, 2nd Edition by Atul Kahate. Tata Mc- Graw-Hill Publications, New Delhi.

[6] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems" Journal of Cryptology. 4 (1): 3–72

[7] National Institute of Standards and Technology. Data Encryption Standard. FIPS PUB 46-2. December 30, 1993.