

A Novel Encipherment Technique-DRONA

Rachana B. Nair

Independent Researcher, Kalpathy, Palakkad, Kerala, India

Abstract— In this proposed encryption/decryption technique, the data is divided into blocks and each block is processed to obtain blocks of enciphered data. This mathematical algorithm has got an iterative structure, where rounds of processing are carried out to enhance the security. One major advantage of DRONA is that it does not require a secret key. It is primarily based on substitution and permutation techniques. Major concern of any encipherment/decipherment technique is to keep the privacy of secret key intact. Moreover, it consumes a lot of hardware and memory of the system to store this secret information. Cryptanalysis based on the knowledge of secret key is thwarted. A novel algorithm to protect the data from adversaries is proposed in this article.

Keywords— cryptography, des, drona, encipherment, encryption, fiestal cipher.

I. INTRODUCTION

Security of information is a cause of major concern nowadays. Infringement of data has to be thwarted at any cost. Maintenance of data secrecy has evolved in a major way. In the present scenario, it has become a necessity of each and every individual. With the evolution of computer/information age, there is a high rise in the requirement to protect data from adversaries. E-commerce has also paved way for high dependency on cryptography to safeguard confidential information from attackers which cause millions of loss to firms. OSI (Open System Interconnection) security architecture defines various kinds of security attacks, security mechanisms and security services [1]. Security attacks are broadly divided into passive attacks which include unauthorised reading of confidential information and active attacks include modification of messages or files and also denial of services [3].

A security mechanism detects, prevents or recovers from a security attack. Various kinds of encryption/decryption algorithms, digital signature, hashing algorithms and message authentication codes fall under this category [2].

By the implementation of security mechanism, security attacks are prevented and security services such as authentication, access control, data confidentiality, data integrity, non repudiation and availability are attained [1].

In this proposed algorithm, substitution and permutation techniques are incorporated. The plaintext is viewed as a sequence of bits and it is divided into blocks and plain text bit patterns are replaced with cipher text bit patterns. This mathematical encipherment algorithm involves complex permutation that is not easily reconstructed.

Block cipher is a scheme in which a block of plain text is converted to a cipher text block with repeated rounds of processing. In each round, certain functions are performed, exhibiting a fiestal structure [4]. It uses 128 bit data and no secret key is used in this algorithm making it advantageous over other encipherment techniques where secret key is an essential ingredient.

II. PROPOSED ALGORITHM – DRONA

The binary representation of data is computed. Zeros are appended to make it a 128 bit data representation. The 128 bit data is divided into 16 blocks, each block is 8 bits in length. The overall scheme is illustrated as follows:

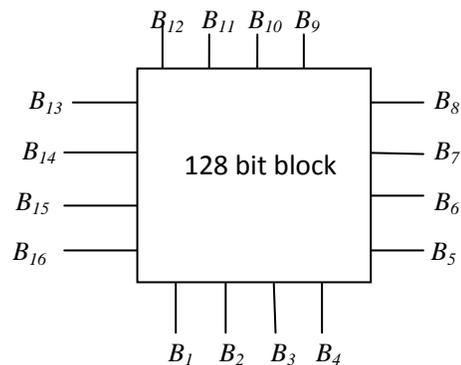


Fig:1.1

$$\begin{aligned}
 &B_1(x_1 \dots x_8) \oplus B_2(x_9 \dots x_{16}) = A(y_1 \dots y_8) \mid \mid \overline{B_2} = Z_1 \\
 &B_3(x_{17} \dots x_{24}) \oplus B_4(x_{25} \dots x_{32}) = B(y_9 \dots y_{16}) \mid \mid \overline{B_4} = Z_2 \\
 &B_5(x_{33} \dots x_{40}) \oplus B_6(x_{41} \dots x_{48}) = C(y_{17} \dots y_{24}) \mid \mid \overline{B_6} = Z_3 \\
 &B_7(x_{49} \dots x_{56}) \oplus B_8(x_{57} \dots x_{64}) = D(y_{25} \dots y_{32}) \mid \mid \overline{B_8} = Z_4 \\
 &B_9(x_{65} \dots x_{72}) \oplus B_{10}(x_{73} \dots x_{80}) = E(y_{33} \dots y_{40}) \mid \mid \overline{B_{10}} = Z_5
 \end{aligned}$$

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

$$\begin{aligned}
 &B_{11}(x_{81} \dots x_{88}) \oplus B_{12}(x_{89} \dots x_{96}) = F(y_{41} \dots y_{48}) \mid \overline{B_{12}} = Z_6 \\
 &B_{13}(x_{97} \dots x_{104}) \oplus B_{14}(x_{105} \dots x_{112}) = G(y_{49} \dots y_{56}) \mid \overline{B_{14}} = Z_7 \\
 &B_{15}(x_{113} \dots x_{120}) \oplus B_{16}(x_{121} \dots x_{128}) = F(y_{57} \dots y_{64}) \mid \overline{B_{16}} = Z_8 \\
 &Z = Z_1 \mid \mid Z_2 \mid \mid Z_3 \mid \mid Z_4 \mid \mid Z_5 \mid \mid Z_6 \mid \mid Z_7 \mid \mid Z_8
 \end{aligned}$$

Each input bits of a block are exclusive-ored with the input bits of consecutive block. A block and its consecutive counterpart after xoring operation will not be involved in a functional operation (exclusive-or) with any other blocks.

The result after xoring operation is concatenated with the complement of consecutive block. The procedure is repeated until the last and pre- last block are xor-ed and the resultant is concatenated with the complement version of last block. Each intermediate outputs of 8 steps are concatenated to form a result, Z which is 128 bits in length.

The 128 bit pre-output is divided into two halves-right and left half, each half is 64 bits in length. They are denoted as RZ and LZ, respectively. The RZ is left circularly shifted and divided into two halves, each of which is 32 bits in length. The right half is RU and left half is LU, both halves are swapped. RU is applied to a S-box in which first and last bit of RU gives the row number and column number respectively. The output of S-box is a 30 bit value, which is expanded to form a 32 bit length intermediate cipher, Q₁. During expansion, the first and last bit of S-box output is placed at the first and last bit positions of 32 bit representation and remaining bits are in their respective positions.

LU is left circularly shifted and divided into two halves, each of which is 16 bits in length and represented as LM and RM respectively, then swapped.

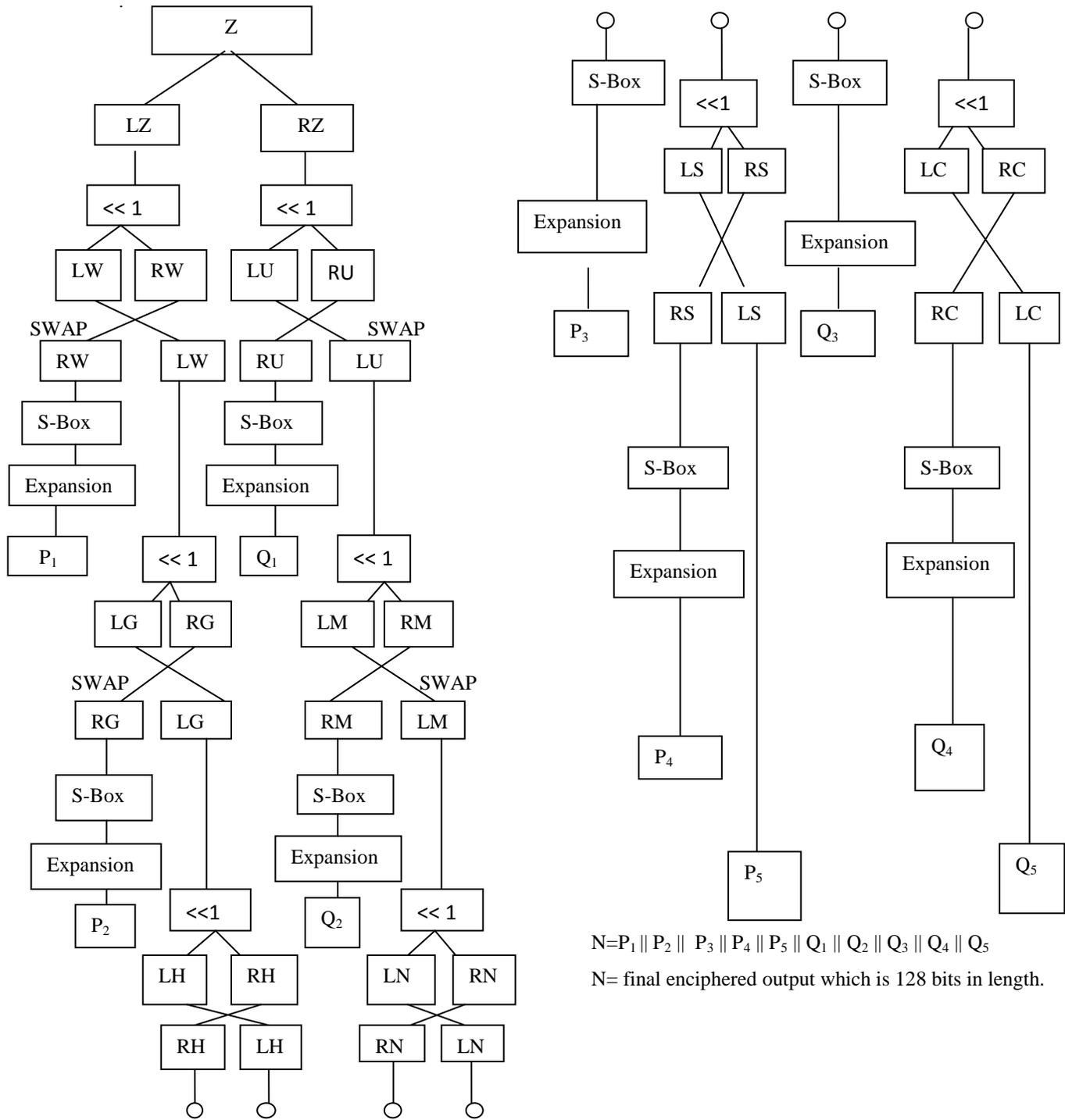
RM is applied to S-box and output of S-box is 14 bits in length, later expanded to produce a 16 bit output, Q₂. LM is left circularly shifted and divided into two halves, LN and RN which are 8 bits in length. Swapping is done. RN is applied to S-box, producing a 6 bits in length value, which is expanded to form a 8 bits intermediate cipher, Q₃.

LN is left circularly shifted and divided into two halves, each half is 4 bits in length, represented as RC and LC respectively. Swapping is carried out. RC is inputted to a S-box to form a 2 bit value, expanded to produce Q₄ which is 4 bits in length. LC is Q₅.

Repeat the same procedure on the left half 64 bits (LZ) where the intermediate pre-output values of 32 bits, 16 bits, 8 bits, 4 bits values after expansion and LS denoted as P₁, P₂, P₃, P₄ and P₅ respectively are concatenated with Q₁, Q₂, Q₃, Q₄ and Q₅ to produce the final enciphered output denoted as N. N is 128 bits in length.

The number of rounds is large making the crypt analysis relatively, difficult. The algorithm has avalanche properties.

Decryption uses the same algorithm, except that instead of left circular shift operation right circular shift is performed.



$$N = P_1 \parallel P_2 \parallel P_3 \parallel P_4 \parallel P_5 \parallel Q_1 \parallel Q_2 \parallel Q_3 \parallel Q_4 \parallel Q_5$$

N = final enciphered output which is 128 bits in length.

III. CONCLUSION

The structure of DRONA is complex. It is motivated by design principles of fiestal cipher and also a large majority of network based cryptographic application makes use of block encipherments. The final encrypted block is cryptographically stronger than any of the component ciphers. The statistical structure of plain text is reflected into long range statistic of cipher text. No secret key is used in the implementation of this algorithm making it still harder for adversaries. Large data size incorporates greater data security by achieving greater diffusion. Multiple rounds offers high security. Increased complexity in this algorithm leads to increased difficulty of crypt analysis.

REFERENCES

- [1] ITU-T Rec. X.800 (03/91) Security Architecture for Open Systems Interconnection for CCIT Applications .
- [2] A. J. Menezes, P.C. van Oorschot, S. Vanstone. "Handbook of Applied Cryptography," CRC Press Boca Raton FL USA. 1996.
- [3] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall Upper Saddle River, USA, 1999.
- [4] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Reaffirmed 1999 October 25 U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology (DES)