Vandana Publications
IJEMR

Volume-4, Issue-5, October-2014, ISSN No.: 2250-0758
International Journal of Engineering and Management Research
Available at: www.ijemr.net
Page Number: 103-105

New Symmetric Block Cipher Algorithm with Performance Evaluation

Shalini Aggarwal[1], Dev Baloni[2]
[1]Pursuing M.Tech., GRD Institute of Management & Technology, Dehradun, Uttarakhand, INDIA
[2]GRD Institute of Management & Technology, Dehradun, Uttarakhand, INDIA

ABSTRACT

The rapid growth of network communication system and the popularity of Internet have brought changes in the way of communication and entail high risk of breach in information security. Cryptography is one of the ways to provide security on electronic documents. In this paper, we propose a new symmetric block cipher, with 256-bit block size and 128-bit key length in ECB mode produces higher avalanche effect and reduces time complexity. The technique is implemented in C language.

Keywords — Avalanche Effect, Block Cipher, ECB mode, Private Key.

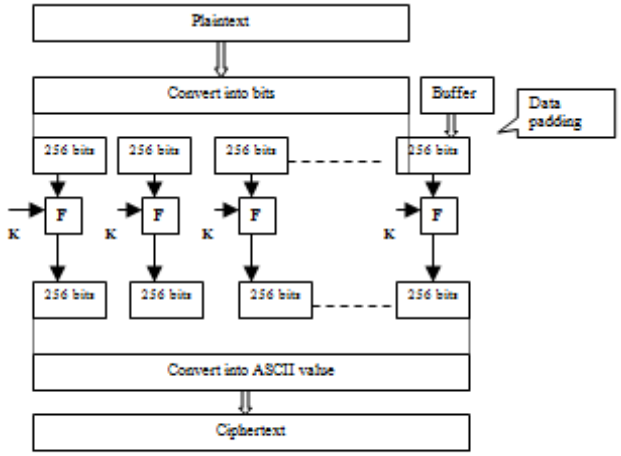
I. INTRODUCTION

The explosive growth in computer technology and communication via networks has increased the storage of data and awareness of data security. Most of sensitive information is exchanged electronically therefore the information has to be protected while transmitting. Encryption converts the actual document into a format that cannot be recognized except the sender and intended receiver. Modern techniques of encryption either use a symmetric (one key) or asymmetric (two keys) method. The proposed encryption algorithm is designed to provide a better symmetric block cipher that exhibits high avalanche effect with simple structure that will reduce the time taken to encrypt and decrypt the message.

II. NEW CIPHER ALGORITHM

This block cipher algorithm takes a fixed-length block of plaintext and transforms it through a series of operations into another cipher-text block.

Figure summarizes the overall structure of algorithm.

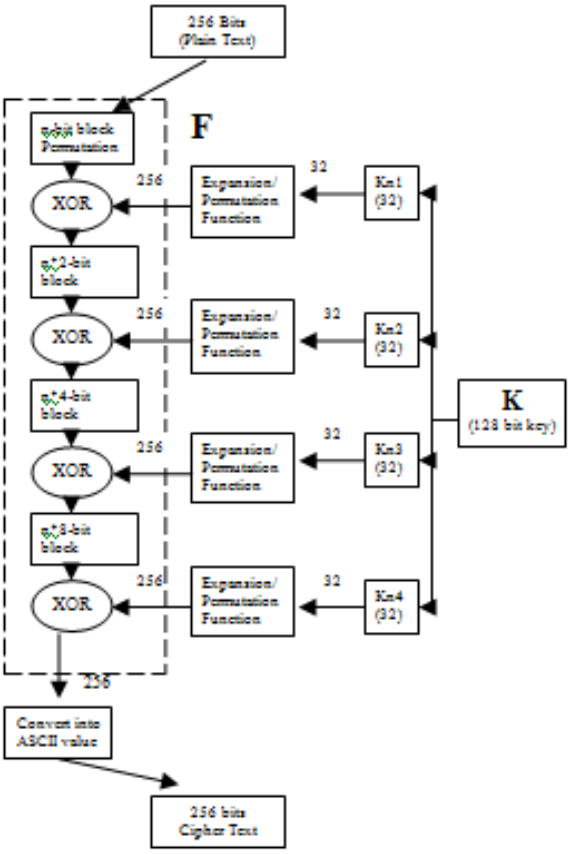


General structure of Encryption

Plain text is converted into 256 bits blocks and if required, buffer data is appended to the last block. Same Encryption function F is applied on each 256 bits block with 128 bits Key K and produces 256 bits cipher block.

Encryption

In encryption function F, four rounds of same (permutation and XOR) operations are performed. In each round, n-bit block internal and external permutation operations rearrange the plain text bits. This is followed by XOR operation with 256 bit round key. For each round, a 32 bits sub key is passed through expansion/permutation function. The value that *n* take in each level is different (i.e. 4, 8, 16, 32).

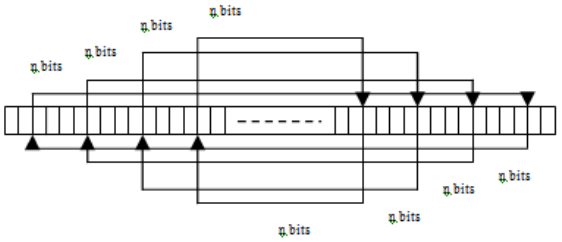


Overview of Encryption

Each round basically comprises three major functions, namely, Internal & External Permutation, Expansion Function, and a XOR Function. The 256-bit input to the first round undergoes an n-bit internal permutation then 256-bit output of the n-bit internal permutation is introduced to an n-bit external permutation, which again generates a 256-bit output. The 32-bits Key (Kn) gets expanded into a 256-bit with which the 256-bit output of the permutation gets XORed to produce a 256-bit intermediate output. This intermediate is again fed into the next round to carry out the procedure all over again.

External Permutation

In *n*-bit external permutation operation, 256-bit of text are grouped into distinct *n*-bit groups, where n is 4, 8, 16, 32 in different round at which we are operating. The groups are formed by starting from the first bit and grouping together the first *n* consecutive bits, then the next *n* consecutive bit, and so on. The first *n*-bit group gets interchanged the last *n*-bit group. The second *n*-bit group gets interchanged with the penultimate *n*-bit group and so on. External permutation can be depicted as follows:

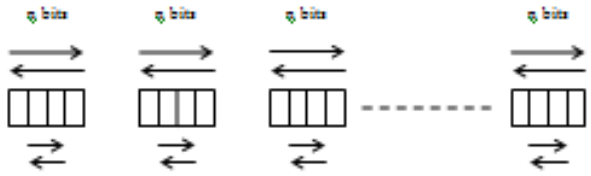


n-bits External Permutation

Internal Permutation

In *n*-bit internal permutation operation, 256-bit of text are grouped into distinct *n*-bits groups, where n is 4, 8, 16, 32 in different round at which we are operating. The groups are formed by starting from the first bit and grouping together the first *n* consecutive bits, then the next *n* consecutive bit, and so on. In *n*-bit group, first bit gets interchanged the last bit in same group. The second bit gets interchanged with the penultimate bit and so on. This procedure is applied on all n-bit blocks.

Internal permutation can be depicted as follows:



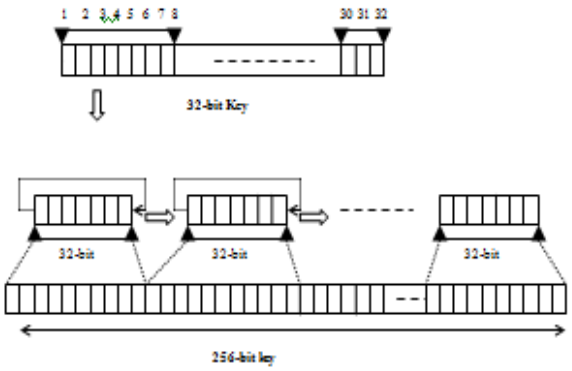
n-bits Internal Permutation

Expansion and Permutation

Key length is the most important security factor of any encryption/decryption algorithm. The effective key length is 128 bits, giving 2^{112} possible combinations. The 128-bits of the key have been divided into four 32-bits round key.

The Expansion Function transforms the 32-bits Key (Kn) into a 256-bit key, which is used as an input to the XOR Function. Left-rotation of bits modifies key and makes the next 32 bits of the expanded key. Next, another left-rotation is given to the next 32-bits to produce the next 32- Bits, and so on. Eight such modifications of the 32-bit key finally produce the 256-bit key for that particular round.

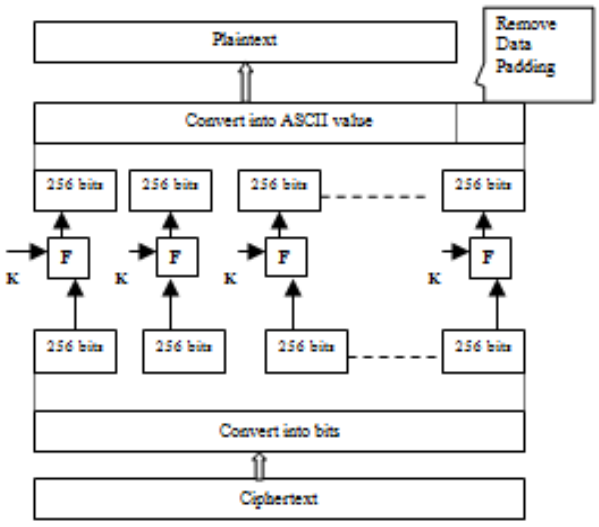
Thus, a 256-bits output is generated by the expansion function. After that 256-bits key is permuted using permutation operation in which data is arranged in rows and columns.



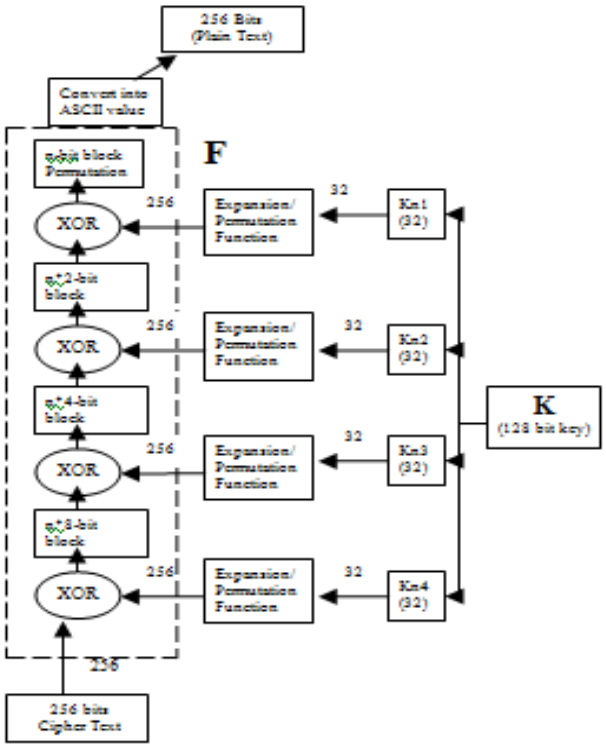
Key Expansion

Decryption

The decryption function is just the reverse of the encryption function. In decryption, four rounds of same operations (XOR and permutation) are performed. In each round, 256-bit cipher text is XORed with 256 bit round key followed by external and internal permutations that rearrange the cipher text bits. As encryption function, 128-bits key is divided into four 32-bits sub key then 32- bits sub key is passed through expansion / permutation function in each round.



General Structure of Decryption



Overview of Decryption

III. CONCLUSIONS

In this paper, a new algorithm is proposed to provide security on data using simple operation based on substitution-permutation network that enhances the security as well as speed of the encryption scheme. A key size (128-bits) ensures security from brute force attacks. The time complexity of the proposed algorithm is considerably better than RSA and TDES Algorithms. Proposed algorithm can be easily modified by adding any other module to enhance the performance and security. Because of simple structure, it can be implemented in any platform

REFERENCES

[1] William Stallings, Cryptography and Network Security, Principles and Practice, Prentice Hall, Fourth Edition, 2007.

[2] Sriram Ramanujam and Marimuthu Karuppiah, — ”Designing and algorithm with high avalanche effect”, International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.

[3] Rajdeep Chakraborty, Sonam Agarwal, Sridipta Mishra and J. K. Mandal, “Triple SV : A bit level symmetric block cipher having high avalanche effect”, International Journal of Advance Computer Science & Applications, Vol 2, No 7,2011.