International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

An Improved in Feistel Cipher Structure of Encryption

Rajesh Kumar

BCA, 4th Sem, Graphic Era University, Dehradun, India

Abstract: ***In this paper, I propose improved encryption algorithms that have the differentFeistel cipher structure of encryption. So far, conventional Feistel cipher algorithms have difference structure of encryption. I devise my algorithm by inserting XOR operation in left half portion and inserting a function in right half portion of plain text. the proposed algorithm improves encryption security by inserting XOR operation in left half portion and inserting a function in right half portion of plain text.The proposed algorithm will be useful to the applications which require the same procedure of encryption.***

Keywords: Feistel cipher, improved Feistel encryption

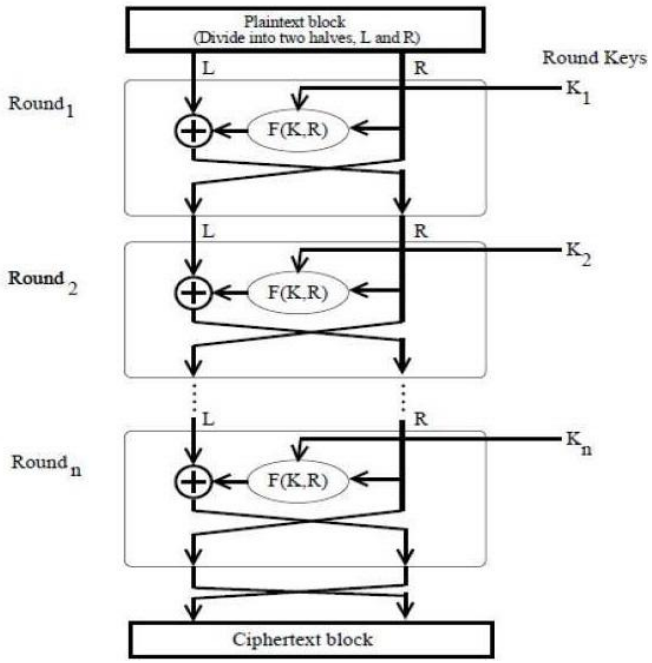
1. Introduction

A Feistel cipher structure is one of the most widely used. Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES (Data Encryption Standard) is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption. And here we study only encryption process.

2. Previous Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

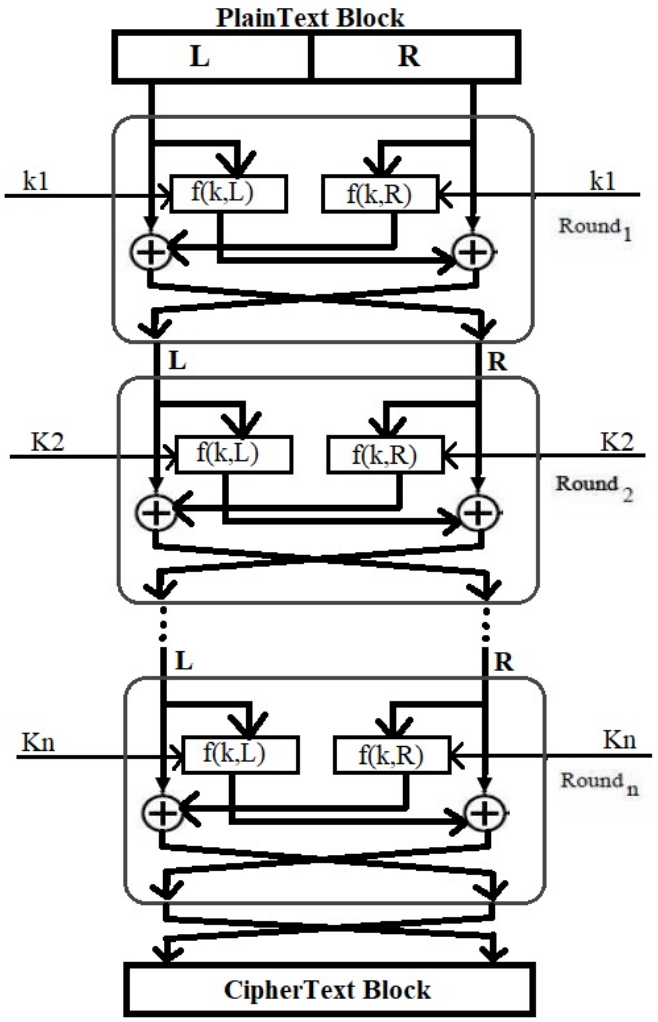
1) The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
2) In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input − the key K and R. The function produces the output f(R, K). Then, we XOR the output of the mathematical function with L.
3) In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
4) The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
5) Above substitution and permutation steps form a 'round'. The numbers of rounds are specified by the algorithm design.
6) Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.



Feistel Cipher Encryption Structure

3. Improved Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext. In this process we perform XOR operation and Function forboth left half and right half. Feistel Structure is shown blow in the following illustration.



1) The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
2) In each round, the right half of the block, R, goes through an operation that depends on L and the encryption key. First, we apply an encrypting function 'f' that takes two input − the key K and L. The function produces the output f(L,K). Then, we XOR the output of the mathematical function with R.
3) And the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input − the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
4) In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
5) The permutation step at the end of each round swaps the modified L and modified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
6) Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.
7) Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

4. Conclusion

I provide extended theory for the encryption process of Feistel structure. Which is more secure and both part (L and R) uses same key.

References

[1] Dinur I, Dunkelman O, Keller N, et al. New attacks on Feistel structures with improved memory complexities. In: Gennaro R, Robshaw M, eds. Advances in Cryptology - CRYPTO 2015, Part I. Lecture Notes in Computer Science, Vol 9215. Berlin: Springer-Verlag, 2015. 433–454
[2] Biryukov, Alex. (2005). Feistel Cipher. 10.1007/0-387-23483-7_159
[3] Matsui, M.: New structure of block ciphers with provable security against differential and linear cryptanalysis. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 205–218. Springer, Heidelberg (1996)
[4] Schneier, B., Kelsey, J.: Unbalanced Feistel networks and block cipher design. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (1996)
[5] Shimizu, H.: On the security of Feistel cipher with SP-type F function. In: Proceedings of SCIS – SCIS 2001 (2001)
[6] Shirai, T., Shibutani, K.: Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 260–278. Springer, Heidelberg (2004)