A New Approach for Designing Cryptographic Systems based on Feistel Structure

S.G.Srikantaswamy
Research Scholar, National Institute of Engineering, Mysore, Karnataka, India
sg_srikantaswamy@yahoo.com

Dr. H.D.Phaneendra
Professor & Research Guide, National Institute of Engineering, Mysore, Karnataka, India
hdphanee@yahoo.com

Abstract : **Many Classical and modern cryptographic algorithms have been developed by the Cryptographers to facilitate data security operations. Classical ciphers are not being widely used because of limited key space. Public key cryptosystems are effective compare to symmetric systems but are slower than symmetric ciphers. Feistel Cipher structure is the reference structure for designing block-ciphers. In this paper we have proposed three variants to feistel structure to enhance the security of the data. The three constructive variants includes new design structure (The features of the derived structure includes 256 block length, processing of four parts of plaintext blocks, involvement of compression and padding operations), Generation of Round Key Using Random Number Generator approach and Use of unique round function for each round .Thus the existing Feistel structure has been modified to create a new block-cipher structure which incorporates effective key generation and round function approaches to provide effective data security.**

Keywords :Feistel Cipher, Compression, Random number, Round function, Encryption

I.INTRODUCTION

In Cryptography, the Caesar cipher is one of the simplest and most widely known encryption techniques. It is a type of Substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of position down the alphabet.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes such as Vigenere cipher and ROT13 System [1]. The Data Encryption Standard (DES) is a previously predominant algorithm for the encryption of data. DES is now considered to be insecure for many applications. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES) [2]. The Vigenere Cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of poly alphabetic Substitution [3]. RSA is an algorithm for public-key cryptography that is based on the presumed difficulties of factoring large integers , the factoring problem. RSA stands for Ron Rivest , Adi Shamir and Leonard Adleman, who first publicly described it in 1977 [4]. Feistel Cipher is a symmetric structure used in the construction of block ciphers, named after the German-born Physicist and cryptographer Horst Feistel. It is also known as Feistel network. Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with K_i used as the seed, then 3 rounds is sufficient to make the block cipher a pseudorandom permutation, while 4 rounds is sufficient to make it a strong pseudorandom permutation [5].A cipher design using random enciphering and deciphering approach for Vigenere cipher has been discussed in [6]. This approach makes use of random key stream generation method. A comparative study of algorithms like AES, 3DES, Blowfish and DES was made with respect to throughput and blowfish stands better compare to other with respect to different input sizes [7].A new symmetric encryption block cipher with bit shifting approach has been explained[8]. The proposed method is easy to adopt the advanced coding languages. The encryption system which can encrypt 256 bits of data with complement, rotation, mix column approaches to provide good level of security has been indicated [9]. The proposed cipher works well but vulnerable to brute-force attack. Playfair cipher has been modified using rectangular matrix to provide better security than Playfair cipher [10]. Classical ciphers provides good security if used with enhanced effective logic.

Thus by studying various ciphers we can say that design of computationally secure is really the ultimate task. A cryptographic Scheme for a given task is Secure if no adversary of a specified power can achieve a specified break [11]. For each performance study, a set of performance criteria or metrics must be chosen. If the system perform the service correctly, its performance is measured by the time taken to perform the service, the rate at which the service is performed, and the resources consumed while performing the service [12]. The design criteria used in the block-cipher focused on the block size, key size and the number of rounds to select a trade off between the resources and throughput. The criteria used in the design of DES, focused on the design of the S-boxes and the P function that takes the output of the S boxes [13]. A modified Feistel cipher has been developed which involves modular arithmetic addition and modular arithmetic inverse of a key matrix [14]. The purpose of the paper is to improve existing block cipher. A block cipher based on Feistel cipher has been proposed with the operations involving key matrices with XOR operations [15]. Feistel cipher has been modified with key based substitution, shifting of rows with modular arithmetic addition [16]. Modular multiplication is an important operation in several public key cryptosystems. The remainder in regard to n can be constructed from the remainder with modulus 2(n+1) and remainder with modulus (2n+2) [17]. A block cipher by blending modified Feistel cipher and Hill cipher involving a single key matrix has been proposed [18].

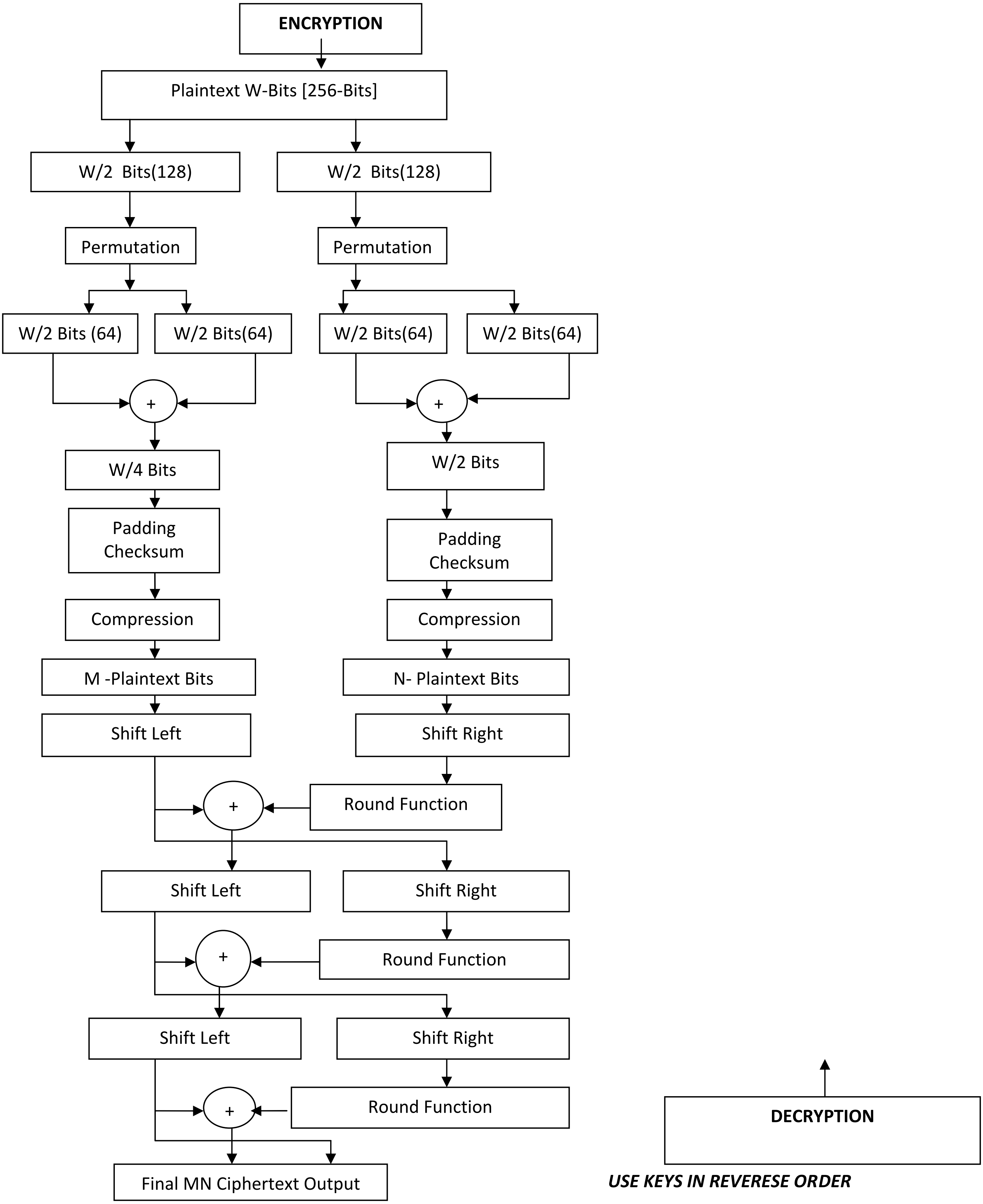
Thus by studying the these papers we can conclude that the existing ciphers are providing better security but there is a need to make this ciphers still more non-linear to increase the confusion property of the ciphers by keeping in view of throughput also. Keeping this motivation, In our paper ,we have given an innovative method to improve Feistel cipher by increasing its non-linearity by using three significant approaches which includes the modification of its structure ,flexible round function approach and round key generation by random number generator approach using suitable seed value.

II. PROPOSED SYSTEM:

The proposed system fundamentally considered Feistel structure. The drawbacks of Feistel structure have been studied and following changes have been incorporated to improve the performance of the cipher. The three security measurers includes, derived cipher structure, effective round function selection and key generation based on random number generator.

III. NEW PROPOSED BLOCK-CIPHER STRUCTURE[SGSPP-CIPHER STRUCTURE]

The proposed structure involves the division of Plaintext –block in to four parts and processing them simultaneously. The Structure is designed such that it involves Permutation function, Compression and Padding of Checksum to plaintext block as Pre-Processing Steps before the actual Round function . The Structure recommends a Block-length of 256-bits and 32 round functions. The left shift and right shift of partial ciphertext has been applied after each round function. Thus multiple measures have been taken in designing the structure for providing effective security. The Structure involving the above features is depicted below.


ENCRYPTION
Plaintext W-Bits [256-Bits]
W/2 Bits(128)
W/2 Bits(128)
Permutation
Permutation
W/2 Bits (64)
W/2 Bits(64)
W/2 Bits(64)
W/2 Bits(64)
+
+
W/4 Bits
W/2 Bits
Padding Checksum
Padding Checksum
Compression
Compression
M -Plaintext Bits
N- Plaintext Bits
Shift Left
Shift Right
+
Round Function
Shift Left
Shift Right
+
Round Function
Shift Left
Shift Right
+
Round Function
Final MN Ciphertext Output
DECRYPTION
USE KEYS IN REVERESE ORDER

IV.EFFECTIVE ROUND FUNCTION APPROACH:

The Conventional Feistel Structure includes a common and same round function for all rounds. This step is vulnerable to security attacks. Instead of using the same round function for all rounds, it is better to use unique round function for each round. The proposed structure recommends 32 rounds and fixed 32 round functions which are selected using Multiplexer Circuit. Let the round functions for round 1 to round 32 be RF1, RF2,etc up to RF32. The user can incorporate their own round functions for designing the cipher. The round function which have been selected in the present Design includes : AND,OR,EX-OR,NOR,NAND,EX-NOR,MOD-2ADDITION,MOD-2 SUBTRACTION, ARITHMETIC MULTIPLICATION, SHIFT LEFT ONCE and ADD, SHIFT RIGHT ONCE and ADD, SHIFT RIGHT TWICE and ADD ,SHIFT TWICE LEFT and ADD, SHIFT TWICE LEFT and SUBTRACT,ROTATE LEFT ONCE and ADD, ROTATE LEFT TWICE and ADD, ROTATE RIGHT ONCE and ADD,ROTATE RIGHT TWICE and ADD,AND and SHIFT LEFT ONCE, OR and SHIFT LEFT ONCE, EX-OR and SHIFT LEFT ONCE,OR and ROTATE RIGHT ONCE,AND and ROTATE RIGHT ONCE ,EX-OR and ROTATE RIGHT ONCE.

Selection of Round function Logic:

Round function Selection Signals					**Round Function Selected**
S4	S3	S2	S1	S0	
0	0	0	0	0	F1
0	0	0	0	1	F2
0	0	0	1	0	F3
0	0	0	1	1	F4
0	0	1	0	0	F5
0	0	1	0	1	F6
0	0	1	1	0	F7
0	0	1	1	1	F8
0	1	0	0	0	F9
0	1	0	0	1	F10
0	1	0	1	0	F11
0	1	0	1	1	F12
0	1	1	0	0	F13
0	1	1	0	1	F14
0	1	1	1	0	F15
0	1	1	1	1	F16
1	0	0	0	0	F17
1	0	0	0	1	F18
1	0	0	1	0	F19
1	0	0	1	1	F20
1	0	1	0	0	F21
1	0	1	0	1	F22
1	0	1	1	0	F23
1	0	1	1	1	F24
1	1	0	0	0	F25
1	1	0	0	1	F26
1	1	0	1	0	F27
1	1	0	1	1	F28
1	1	1	0	0	F29
1	1	1	0	1	F30
1	1	1	1	0	F31
1	1	1	1	1	F32

V.KEY GENERATION FOR EACH ROUND ROUND USING RANDOM NUMBER GENERATOR:

Conventional Feistel Cipher Structure involves a separate Key generation Algorithm with key length 56-bits. In our system we have proposed variable Key –length for each round and unique key for each round can be selected by applying proper seed value .by concatenating the first 10 values , the required key value can be obtained. The efficiency of the generator depends on the seed selected.

Consider the generator X_n=(25,173X_{n-1}+13,849) mod 2^{16}

Let the seed Value X_0=1. The First 20 numbers generated are as follows [12].

25173	12345	54509	27825	55493	25449
13227	53857	64565	1945	6093	24848
48293	52425	61629	18625	2581	25337
11949	47473				

By Concatenating the values generated , we can get the key of required length. The Variable length key can be obtained by flexible manner. By Concatenating the first 10 values of the generated random numbers, the value of the key is calculated as below.

K=2517312345545092782555493254491327753857645651945.

By using different Seed Values , the keys required for all 32 rounds can be generated as described above.

VI.COMPARISON OF THE PROPOSED STRUCTURE WITH EXISTING STRUCTURES:

The Proposed Structure is an improved version of the existing Block-cipher Structures. The proposed structure is being named as SGSPP- structure. S stands for Srikantaswamy and PP stands for Professor Phaneendra.The Proposed Cipher involves more processing operations such as division of Plaintext into 4 parts, padding and compression and exhibits the properties of confusion . The proposed cipher suggests 32 rounds of operations and exhibits the property of diffusion. The use of unique round function for each round is the another efficient feature of the proposed scheme. The variable key generation using random number generator made the scheme more stronger against cryptanalytic attacks.

CIPHER	**Block-Size in- Bits**	**Number of Rounds**	**Key-Size In-Bits**	**Round Function**	**Additional Functions**
FEISTEL-CIPHER	64	16	64	Same for all rounds	EX-OR, Permutation
DES-CIPHER	64	16	56	Same for all rounds	EX-OR, Permutation
PROPOSED SGSPP-CIPHER	256	32	Variable	Different for each round	EX-OR, Permutation, Padding, compression

Thus the Proposed Structure is very efficient model for designing block-ciphers for data security.

VII.CONCLUSION

The Proposed System is an improved Version of Feistel Cipher. The System works well for any size of data and occupies less memory and executes very fast. The proposed system exhibits efficient confusion and diffusion properties. Use of discrete Logarithmic approach and Modular arithmetic operations can further improve the efficiency of the system. The System can be further improved by using improved random number generator and effective round functions. The proposed block-size of 256-bits ,32 rounds and variable –length key provides effective security.

VIII.REFERENCES

[1] http://en.wikipedia.org/wiki/caesar_cipher

[2] http://en.wikipedia.org/wiki/Data_Encryption_Standard

[3] http://en.wikipedia.org/wiki/Vigen%c3%A8re_Cipher

[4] http://en.wikipedia.org/wiki/RSA_(algorithm)

[5] http://en.wikipedia.org/wiki/Feistel_Cipher

[6] Yumnam Kirani Singh-“A Simple fast and Secure Cipher”-ARPN Journal of Engineering and applied Sciences-Vol.6,No.10,October 2011

[7] Simar Preet Singh, Raman Maini-“Comparision of Data Encryption algorithms”-International Journal of Computer Science and Communication-Vol.2, No.1, January-June 2011, PP 125-127.

[8] Hari Krishan Soni, Dr. Sanjeev Sharma and Prof.SantoshSahu-“A New method in Symmetric Encryption for block cipher module: A Bit shifting Approach”-IJCA Special Issue on “Network Security and Cryptography”, NSC, 2011.

[9] Rohan Rayarikari, Sanket Upadhyay and Deeshen Shah-“ An Encryption Algorithm for Secure data Transmission “- IJCA (0975-8887) Volume 40, No.7, February 2012.

[10] Sanjay Basu and Uptal Kumar Ray-“Modified Playfair Cipher using Rectangular Matrix”-IJCA (0975-8887) Volume 46-No.9, May 2012.

[11] Jonathan Katz, Yehuda Lindell-“Introduction to Modern Cryptography”- Chapman & Hall/CRC, Taylor & Francis Group.

[12] Raj Jain-“The art of Computer Systems Performance Analysis “-John Wiley & Sons, Inc.

[13] William Stallings-“Cryptography and Network Security”-Third Edition.

[14] Dr.V.U.K Sastry and K.anup Kumar-“A Modified Feistel Cipher Involving Modular arithmetic Addition and Modular Arithmetic Inverse of a Key Matrix’-International Journal of advanced Computer Science and applications(IJACSA), Vol.3, No.7, 2012.

[15] Dr.V.U.K Sastry and K.Annup Kumar-“A Modified Feistel Cipher Involving a Pair of Key Matrices, Supplemented with XOR Operation, and Blending of the Plaintext in each round of the Iteration Process”-International Journal of Computer science and Information Technologies (IJCSIT), Vol.3(1), 2012, 3133-3141.

[16] Dr.V.U.K.Sastry and K.Annup Kumar-“A Modified Feistel Cipher Involving Key Based Substitution, Shifting of Rows, Key Based Mixing of Columns, Modular Arithmetic Addition and Shufling”-International Journal of Engineering Research and Applications (IJERA), Vol2, Issue 5, September-October 2012, pp 237-245.

[17] G.A.V.Rama Chandra Rao, P.V.Lakshmi and N.Ravi Shankar-“A New Modular Multiplication Method in Public Key Cryptosystem”-International Journal of Network security, Vol.15, No.1, pp 23-27, Jan 2013.

[18] Dr.V.U.K Sastry and K Annup Kumar-“A Block Cipher Obtained By Blending Modified Feistel Cipher and Advanced Hill Cipher Involving A Single key Matrix-International Journal of Engineering Research and Applicatio(IJERA), Vol.2, Issue 5, September-October 2012.