# Format Preserving Encryption using Feistel Cipher

S.Vidhya
Ph.D Scholar
Department of Computer Science,
SCSVMV University
Kancheepuram, India.

K.Chitra, Ph.D.
Assistant Professor,
Govt. Arts College
Melur
Madurai, India

## ABSTRACT
This paper presents a Format preserving encryption algorithm using Feistel Cipher. Cryptography is a useful technique to transmit large amount of data in a secured way through an internet. In Cryptography, Encryption is used to convert the original information (Plain text) to unreadable intelligent form (Cipher text). Format Preserving Encryption is used to maintain the length and format of the cipher text as plaintext after encryption.

## General Terms
Format Preserving Encryption ( FPE )

## Keywords
FPE, Format Preserving Encryption, Data type Preserving Encryption, Block cipher.

## 1. INTRODUCTION
Today we transmit much secret information through the internet such as credit card number. There are many possibilities for tracing the information. Cryptography is used to avoid it. It is a tool for secret writing. In Cryptography, Encryption converts the original information such as plaintext into unreadable secret information such as cipher text. Cipher is an algorithm used for encryption and decryption. Format Preserving Encryption means both plaintext and cipher text having same length and format.

In all the algorithms the encrypted value is not same as plaintext in length and format. The encrypted value requires modification to the database and also changes of queries related to the database. It is very tedious process.

## 2. ENCRYPTED VALUE IN DATABASE
After encryption process the schema will be changed according to store the encrypted value. I give an example to encrypt credit card number in stored in the data base.
Create a Customer_detail a table which contains credit card details for customers. Our task is to protect this data by encrypting the column, which contains the credit card number.

**Table 1. Database before Encryption**

| ClientID | ClientName | CreditCardNum |
|---|---|---|
| 1 | R.V.Keerthi | 1234-5678-9789-0124 |
| 2 | V.R.Rajkumar | 1234-5671-9988-7766 |
| 3 | R.V.Kabilan | 3456-7898-9789-0124 |

Using Electronic Code Book(ECB) mode to encrypt our database column. This mode does not require any initialization vector. This mode requires our input should be multiple of 8 bytes.

**Table 2. Database after Encryption**

| ClientID | ClientName | Encrypted CreditCardNum |
|---|---|---|
| 1 | R.V.Keerthi | 0BDC16E6A777C535C49F67688C6D4E21D3F36088C206C85A |
| 2 | V.R.Rajkumar | 0BDC16E6A777C535264AF5FD1E8BD570DDD44E842A72C00B |
| 3 | R.V.Kabilan | 5408551E9C4A0F8FC49F67688C6D4E21D3F36088C206C85A |

After completing all the encryptions, our database schema will be changed to store the encrypted value. The length and data type of the credit card number column is changed after encryption. The corresponding queries which handle the credit card number will also be changed.

## 3. FPE AND HISTORICAL CIPHERS
Most of our earlier classical encryption techniques support FPE. Two basic methods of classical encryption are substitution and transposition.

### 3.1. Substitution cipher
In this technique each element of the plaintext is replaced by another element. The substitution ciphers such as Caesar cipher, Mono alphabetic cipher, Poly alphabetic cipher etc, were supporting FPE. In all the cipher the length and format of plaintext and cipher text are same.

### 3.2. Transposition cipher
This cipher is also called as permutation cipher. In this cipher the plaintext is shuffled without changing the original letters. So that the length and elements of both plaintext and cipher text are same. The only difference is the position of the elements.
The historical ciphers could easily break because the computational functions were not complicated. The historical ciphers were only basic to the modern ciphers.

## 4. FPE AND MODERN CIPHERS

The modern ciphers are classified into two types. Symmetric key encryption and Asymmetric key encryption. In symmetric key encryption the same key is used for both encryption and decryption. But in Asymmetric two separate keys such as public key and private keys are used. DES, Triple DES, AES and Feistel network are best example for modern ciphers. The ciphers are more secured and cannot be easily broken.

The main draw back in modern ciphers is the length of the cipher text. For example encrypting a single digit number using AES and 128 bit key, the cipher text is 32 digits hexadecimal number. 128 bits are required to store 32 digits hexadecimal number. The cost of altering the database is too high. The queries related to the data base will also be changed. The graphical user interface could not support it.

## 5. EXISTING FPE TECHNIQUES

Black and Rogway suggested three practical methods for FPE such as Prefix method, Cycle walking method and Feistel network.

### 5.1 Prefix Method

Prefix method uses AES or 3DES algorithm. For example encrypting 16 digits credit card number applying AES algorithm to each digit and store the digit and encrypting values in the table. The table is sorted according to the encrypted value and the corresponding original digits are used as a cipher text. The technique is useful only for small range of plaintext.

### 5.2 Cycle walking Method

The cycle walking works by encrypting the plaintext by repeatedly applying AES or 3DES until the cipher text becomes in acceptable range. The duration for ciphering is not deterministic.

### 5.3 Feistel and cyclic method.

The Feistel + Cycle construction is the combination of two main techniques. First, the Feistel network that is constructed for the size of the given plaintext. This network used to encrypt the data. The cycle-walking technique is applied to the cipher text to provide the cipher text in appropriate range. The performance depends upon the number of rounds used in the network.

## 6. FPE USING FEISTEL NETWORK

I propose a new technique using Feistel network for FPE. The existing technique uses the combination of Feistel and cycle walking but I use only Feistel network and number conversions. This technique simplifies the encryption process and also reduce the number of iterations. The main advantage in Feistel network is the size of the input can be changed. The sub keys are generated at each round. It is more secured and very flexible for implementing FPE.

In this section I provide encryption of 16 digits credit card number using Feistel network. After encryption the cipher text is also a 16 digits decimal number.

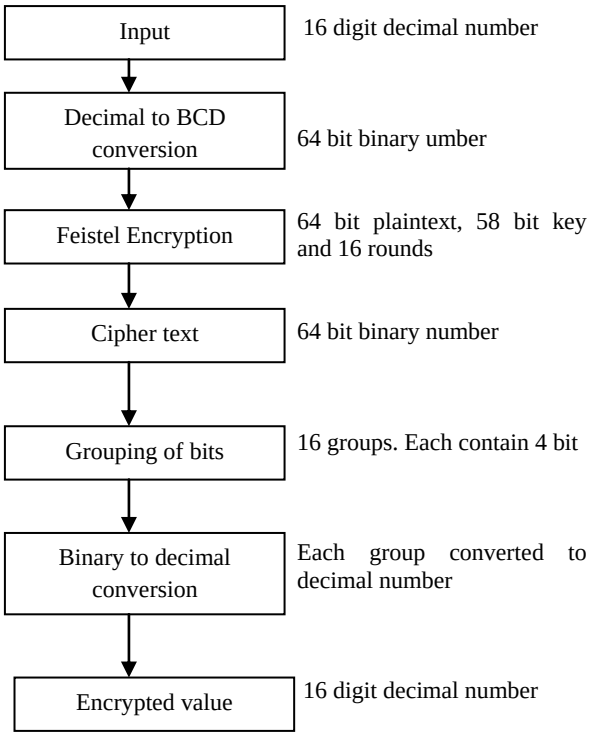


**Fig 1: FPE using Feistel network**

### 6.1 Decimal to BCD Conversion

The number of input bits for Feistel network is 64. Using BCD conversion each digit in credit card number is converted to 4 bit binary number.

Credit card number : 1234567897890124
BCD Conversion 0001001000110100
0101011001111000
1001011110001001
0000000100100100

### 6.2 Feistel Encryption

The input for Feistel encryption is data block and key. The input is divided into two halves and applied to number of rounds. Each round performs the following function.

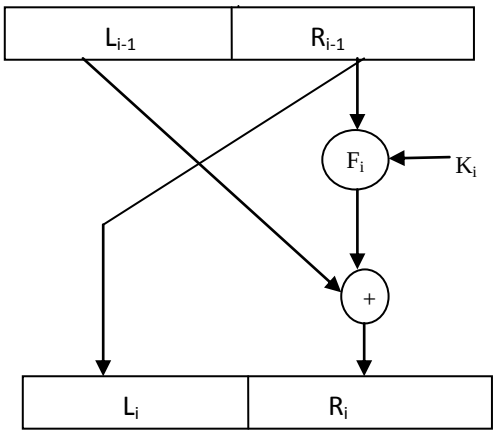


**Fig 2: Single Round in Feistel cipher Structure**

Li-1 and Ri-1 - Input for Round i
Li and Ri - Output of Round i
Fi - Round Function
Ki - Subkey
And
Li= Ri-1
Ri= F(Ri-1,ki) ⊕Li-1
Partitions input block into two halves process through multiple rounds and each round perform a substitution on left data half based on round function of right half and sub key then have permutation swapping halves.

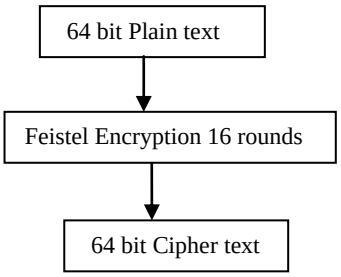


**Fig 2: Feistel cipher Encryption**

Each round the sub key $K_i$ is generated. In each round right half R is never changed. The left half L goes through the round function which depends upon the sub key $K_i$.

Plaintext: 0001001000110100
0101011001111000
1001011110001001
0000000100100100

Round 1 Example :
$L_0$ : 00010010001101000101011001111000
Ro : 10010111100010010000000100100100

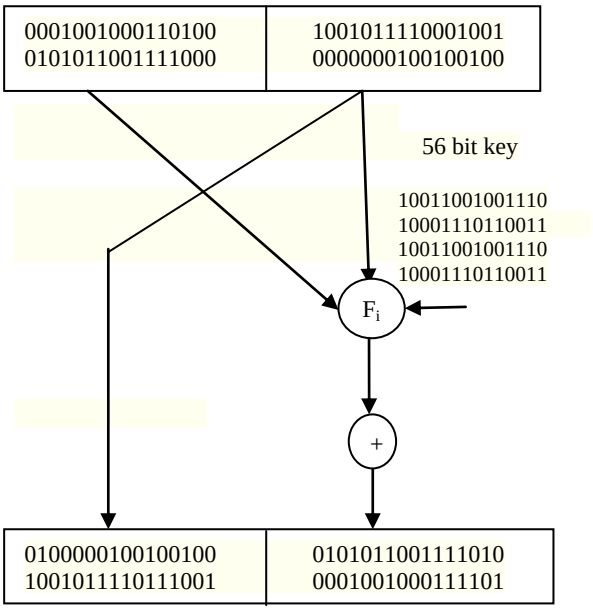


**Fig 3: Round1 in Feistel network structure**

For simplicity I never specify the round function The corresponding cipher text after Feistel network encryption is

Cipher text : 0100000100100100
1001011110111001
0101011001111010
0001001000111101

## 6.3 Binary to Decimal Conversion

The grouping of bits converted in to decimal digit which is suitable for data base field. If the decimal number is greater than 9 then subtract 9 from the digit to make it as single digit number.

Decimal conversion : 4 1 2 4 9 7 11 9
5 6 7 10 1 2 3 13
Reduced to single digit : 4 1 2 4 9 7 2 9 5 6 7 1 2 3 4
The final encrypted value is : 4 1 2 4 9 7 2 9 5 6 7 1 2 3 4

## 7. PERFORMANCE ANALYSIS OF FEISTEL NETWORK

- Feistel cipher uses product cipher that is combination of substitution and transposition. The final result is cryptographically more secured.
- The security in Feistel network depends on the key length and number of rounds. Large key length and more number of rounds increase the security.
- The round function should also complex to make more secured.
- Due to key length and sub key generated in each round the basic cryptanalysis method brute force attack cannot be applied.
- The decryption process is same as encryption. Only requirement is reversal of key schedule. The size of the code and the hardware implementation of Feistel network are very less compared to other cipher structure.

The following table shows the performance of the existing FPE techniques and fpe using feistel structure on a 2.34 Ghz Pentium IV with 1 GB memory running Microsoft Windows XP Professiona

**Table 3.Comparitive Table**

| FPE techniques | Input range | Number of encryptions | Time required in milli seconds |
|---|---|---|---|
| Prefix Method | Small range | Number of digits in an input | 760 ( 20 bit ) |
| Cycle walking Method | Plaintext should be equivalent to AES domain | Large number of encryptions | 1500 ( 64 bit) |
| Feistel+Cycle walking Method | Plaintext should be equivalent to AES domain | Large number of encryptions | 10500 (56 bit ) |
| Feistel cipher | Any range | Single encryption | 360 ( 64 bit) |

## 8. CONCLUSION

In many of our real life applications such as credit card number and social security number format preserving encryption plays a major role. Using Format preserving encryption the data base schema and applications related to the database will never changed. The cost and time for changing the data base is minimized. In future FPE will be achieved by making small changes in the existing block cipher implementation without adding number conversion.

## 9. ACKNOWLEDGEMENT

I express my profound gratitude and regards to my guide Dr.K.Chitra for his exemplary guidance. I thank almighty, my parents, my lovable husband and my kids for their constant encouragement.

## 10. REFERENCES

[1] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. Format-preserving encryption. SAC 2009. LNCS 5867,Springer, 2009.

[2] V. Hoang and P. Rogaway. On generalized Feistel networks. Conference version of this paper. CRYPTO 2010,Springer, 2010.

[3] J. Patarin. Security of random Feistel schemes with 5 or more rounds. CRYPTO 2004, LNCS 3152, Springer,pp. 106–122, 2004.

[4] Format Preserving Encryption Terence SpiesVoltage Security, Inc.

[5] M. Bellare, P. Rogaway, and T. Spies. The FFXmode of operation for format-preserving encryption(Draft 1.1). February, 2010. Manuscript (standards proposal) submitted to NIST.

[6] BPS: A Format-Preserving Encryption Proposal Eric Brier, Thomas Peyrin and Jacques SternIngenico, France