SURVEY OF FORMAT PRESERVING ENCRYPTION

S.Vidhya[1] , K.Chitra[2]

[1] Ph.D Scholar, Department of Computer Science, SCSVMV University, Kanchipuram, India.
[2]Assistant Professor, Govt.Arts College, Melur, Madurai, India

Abstract

Cryptography is a technique used to transmit data in a secured way through the internet. Encryption is the process of converting information from its original form (called plaintext) into an encoded, unreadable form (called cipher text). Format preserving encryption (FPE) refers to a set of techniques for encrypting data such that the cipher text has the same format as the plaintext. A format-preserving encryption scheme is applicable for many real-life applications. FPE is a good encryption scheme that allows for encryption with minimal modifications to the original plain text. I examine the FPE model constructed by Black and Rogaway.

Keywords – Analysis of FPE, Data type preserving encryption, Format preserving encryption, FPE, Survey of FPE

I.Introduction

"Security, like correctness, is not an add-on feature."--Andrew S. TanenbaumThe above quote (taken from Cryptography Quotation page) is trying to say that security is not something extra, but it is something essential. Encryption and decryption are the methods used to transmit messages and other sensitive documents and information. During the last few years, format-preserving encryption (FPE) has developed as a useful tool in applied cryptography. The goal is this: under the control of a symmetric key K, deterministically encrypt a plaintext X into a cipher text Y that has the same format as X .

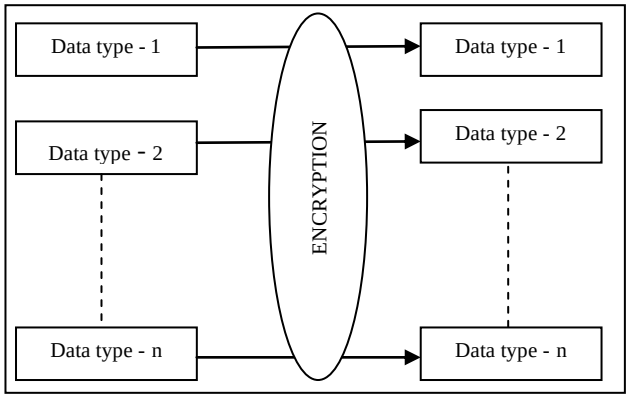

Fig.1 Format Preserving Encryption

The another names for FPE are Data type Preserving Encryption (DPE) and Feistel Finite Set Encryption Mode (FFSEM). There are many names to indicate theFPEtechnique. The main aim of all the techniques is to get back the same size, and data type as the original plain text is being encrypted. Transmitting sensitive data securely over the multi-system environments with minimum changes [1].

II.Fpe Importance

During Encryption and Decryption there is a need for changing the database to store the encrypted text. The main disadvantage in normal encryption method is the cost of modifying the existing databases and applications to process an encrypted information. These costs are related with two important criteria. First, sensitive information like credit card numbers is frequently used as primary key in databases, so changes of this field by encrypting data may require significant schema changes. Second, applications are related to specific data format; encryption will require a format change. In format preserving encryption there is no need to alter the database. A database field which contains a sixteen digits credit cannot store the DES generated cipher text. A Front end program cannot read it [2]. A Graphical User Interface would not display it. The normal encryption should provides lot of facilities for changes in data format throughout an application program and physical database schema. The main aim of FPE is to encrypt the data without the need to modify all of the systems that use that data; such as database field, queries, and all the application program.

A. Fpe Uses

1. Encrypt all types of data including numeric and Alpha numeric
2. Reduce changes to database or application schemas . The data is suitable for the existing data base field.
3. It supports referential integrity
4. Enables encryption of primary and foreign keys
5. It also supports reversible and non-reversible data masking

Iii. Fpe Mechanism

FPE security mechanism needs to be strong with the following limitations:

1. The attackers familiar with format and type of data in the database.

2. Data cannot be extended. If the FPE algorithm encrypts an N-digit number, the output also an N-digit number.[3]

The FPE algorithm should be satisfied the above mentioned conditions.

Iv. Existing Fpe Techniques

Cryptographers John Black and Phillip Rogaway proposed three techniques for FPE [4]. All the techniques are based on secured block ciphers (AES). This section provides analysis of three FPE techniques.

1.Prefix cipher
2.Cycle Walking
3. Feistel Network

A. Prefix Cipher

In prefix cipher FPE algorithm each integer in a plaintext is assigned by pseudo random weights. The weights are calculated by using AES or 3DES block cipher to each integer.

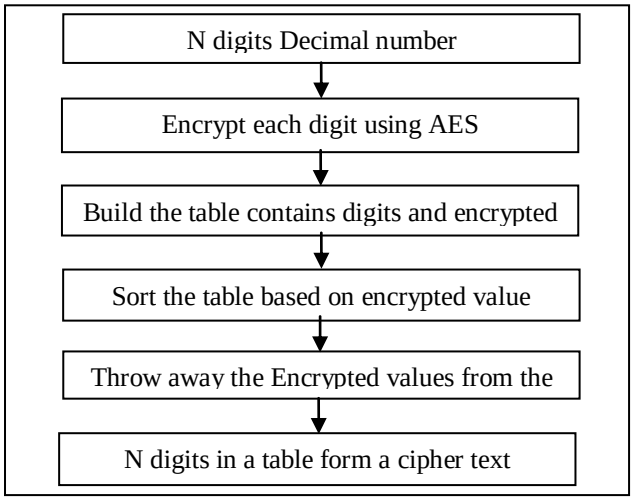

Fig.2 Prefix Cipher

This method is applicable only for small length of plaintexts. For larger plaintext, the entries in the the lookup table and the required number of encryptions to create the table is too big. To build the table, AES or 3DES algorithm is used to encrypt the digits in the plaintext. The table contains input digitand the encrypted value, then sort by the encrypted value. The tiny domain X = {0, 1, 2, 3, 4} having just five possible plaintexts. = {0, 1, 2, 3, 4} having just five possible plaintexts. Under the control of a key K , say having 128 bits, compute Y(0)=AESK (0), Y(1)=AESK (1),Y(2)=AESK (2), Y(3)=AESK (3), Y(4)=AESK (4), and Y(5)=AESK (5). Use the relative ordering of Y(0),Y(1),Y(2),Y(3),Y(4) and Y(5) to determine the desired permutation [5].Suppose we want to encrypt set of 8 digits. Applying AES algorithm for each digit to build the table which contains digits and encrypted value. Sort the table based on encrypted value. The 8 digit number is 34567812.

TABLE I. ENCRYPTED VALUE BEFORE SORTING

Digit	AES encryption of digit
3	49d68753999ba68ce3897a686081b09d
	19ad2b2e346ac238505d365e9cb7fc56
5	9b82998964728141405e23dd9f1dd01b
6	d45efc5268a9afeac1d229e7a1421662
7	b9322f19c62b38e9bed82bd3e67b1319
8	a524c76df94fdd98f7d6550dd0b94a93
1	7346139595c0b41e497bbde365f42d0a
2	3063b6df0a2cdbb0851251d2c669d1bf

TABLE 2. ENCRYPTED VALUE AFTER SORTING

Digit	AES encryption of digit
4	19ad2b2e346ac238505d365e9cb7fc56
2	3063b6df0a2cdbb0851251d2c669d1bf
3	49d68753999ba68ce3897a686081b09d
1	7346139595c0b41e497bbde365f42d0a
5	9b82998964728141405e23dd9f1dd01b
8	a524c76df94fdd98f7d6550dd0b94a93
7	b9322f19c62b38e9bed82bd3e67b1319
6	d45efc5268a9afeac1d229e7a1421662

In this example encryption of 3 is 4, encryption of 4 is 2 and encryption of 2 is 6.

Prefix Cipher Performance

It needs N AES calls to encrypt N digits number. For example to encrypt 16 digits credit card number it needs 16 AES calls. It is not a efficient scheme. The this method is interesting for small values of |M| but is completely unpractical otherwise since$2^{|M|}$time and memory are required in order to start using the cipher[5]. The Prefix method having a very slow key generation and a very fast encryption . The needs more amount of time to build the table, and the memory to hold the table.

Prefix Cipher Optimization

Encrypt the elements using AES and storing only the first 32 bits or 64 bits in the table instead of storing entire 128 bits as a cipher text. The table is sorted using 32 bit elements, and if two entries in the table are same, re-encrypt and compare the entire encrypted value. This Optimization makes the intermediate table smaller, and lowers the amount of copying required during the sort.

B. Cycle Walking

The Cycle-walking construction works by encrypting the plaintext with an existing block cipher (AES or 3DES) repeatedly until the cipher becomes in acceptable range If we have a plaintext X, create an FPE algorithm from the block cipher by repeatedly applying the AES OR 3DES until the result is satisfying required FPE range.

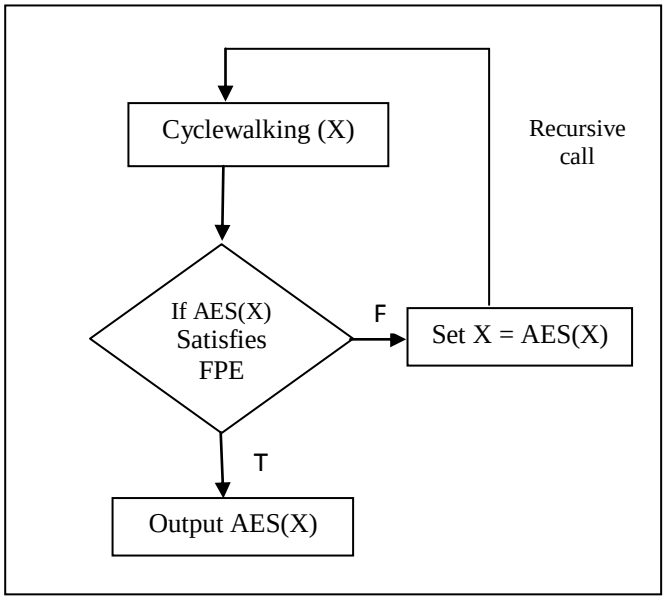

Fig. 3 Cycle Walking

```
CycleWalking FPE(x)
 {
  if AES(x) is an element of M
    return AES(x)
  else
    return CycleWalking FPE(AES(x))
 }
```

The recursion is guaranteed to terminate.

1) Cycle Walking Performance

The larger the difference is between the size of the cipher text and the size of the required FPE output range. [6]. It needs too many iterations. For example if we want to encrypt 64 bits input. The standard block cipher such as AES produces 128 bits cipher text as output. To maintain FPE, AES is repeatedly applied until the higher order 64 bits becomes zero. when plaintext is much smaller than AES domain, that large number of iterations are required for each operation.

C**. Feistel Network**

The Feistel + Cycle construction is the combination of two main techniques. First, the Feistel network that is generated 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. In Feistel network the sub keys are calculated at each round, The pseudo random values generated by AES algorithm are used as a sub key. Like cycle walking repeatedly executing the Feistel network until the required FPE range is reached.

1) Feistel Mechanism

The standard version of a Feistel network works like this. Assume that X has an even number of bits. Partition it in to a left-hand side L and a right-hand side R. Take the right hand side R and apply to it some key-dependent round function. Next xor together the already-mentioned left-hand side L and the processed right-hand side R∗ to get the new right hand side R'.. The old right-hand side becomes the new left-hand side L'. . This is round-1 of the classical Feistel network, mapping a left and right side, (L, R), to a new left and right side, (L',R'). Each round the round function will differ [5]. We can use any number of rounds. The round function performs the following operation to calculate the new L and R values:

R' = L XOR f(R)

L' = R

Feistel structure to encipher a 5-digit number, say the number 23456. To encode a 5-digit number needs 16 bits are required. Converting 23456 as a 16-bit binary number, getting 0101101110100000. F is a round function. Superscript specifies round number and subscript specifies key value. Here I never specify the round function.

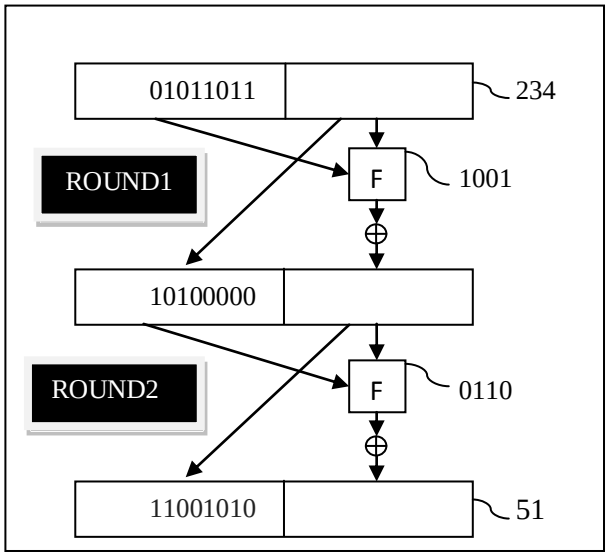

Fig . 4 Feistel Network

The initial left-hand side L; the next 10 bits are the initial right-hand side R . The 10-bit numbers that result from each round function have been randomly generated in the figure

4; I specify only 2 rounds of Feistel network. We can use any number of rounds. Encrypting 5 digit number we get 5 digit number as a output.

1) **Feistel + Cycle Method**

In an above example there is a possibility for getting 6 digit number as output. At that time keep rechipering until get the 5 digit output. This method is called cycle walking. Repeatedly applying the Feistel network until we get the desired output.

2) Feistel + Cycle Method Performance

The generalized Feistel has been the most widely used method to build FPE scheme. The main advantage in Feistel network is the size of the input can be changed. The Feistel + Cycle construction's performance is dependent upon the number of rounds used and the specific PRF (Permutation Round Function) that is used in the round function. For any plaintext that is smaller than the block size of the PRF, the performance is essentially i*r*cost(PRF), where r is the round count and i is the average number of times the cipher cycles to get an acceptable output[7].

V. Comparative Study

The following table shows the performance of the FPE techniques on a 2.34 Ghz Pentium IV with 1 GB memory running Microsoft Windows XP Professional.[6]

TABLE III. COMPARATIVE TABLE

ECHNIQUE NAME	NUMBER OF BITS ENCRYPTED	TIME REQUIRED IN MILLI SECONDS
Prefix cipher (using AES -256)	20	760
Cycle Walking (using 3DES)	64	15000
Feistel + Cycle (using AES-256)	56 (32 Rounds)	10500

The prefix method works on only small data set. The Cycle-walking construction, like the Prefix method, is quite simple, but works on a limited class of sets. The performance of the Feistel + Cyclic method is based on number of rounds constructed and round function PRF used in the network.

VI. Conclusion

Most of our real life applications such as credit card number and social security number require format preserving encryption. Using Format preserving encryption the data base schema and applications will never changed. The cost and time for modifying the data base is reduced. An individual technique alone is not secured For better security we use combination of more than one techniques and also increase the number of permutations at the time of encryption. In future FPE will be applied to all the data types.

References

[1] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. *Format-preserving encryption*. Full version of this paper. 2009.

[2] H. E. Smith and M. Brightwell. *Using Datatype-Preserving Encryption to Enhance Data Warehouse Security.* NIST 20th National Information Systems Security Conference, pp.141, 1997.

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

[4] J. Black and P. Rogaway. Ciphers with Arbitrary Finite J. Black and P. Rogaway. *Ciphers with Arbitrary Finite Domains.* RSA Data Security Conference, Cryptographer's Track (RSA CT '02), Lecture Notes in Computer Science, vol. 2271, pp. 114-130, Springer, 2002.

[5] *A Synopsis of Format-Preserving* Encryption Phillip Rogaway March 27, 2010

[6] *Format Preserving Encryption* Terence SpiesVoltage Security, Inc.

[7] 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.