International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 5 (March 2013) PP: 12-15

Enhancement of Prefix Chiper in Format Preserving Encryption

S.Vidhya[1], Dr.K.Chitra[2]
[1]Ph.D Scholar , Department of Computer Science and Applications, SCSVMV University, Kancheepuram, India.
[2]Assistant Professor, Department of Computer Science, Govt Arts College, Mellur, Madurai, India.

Abstract: ***"Security, like correctness, is not an add-on feature."-- Andrew S. Tanenbaum***
The above quote (taken from Cryptography Quotation page) is trying to say that security is not something extra, but it is something essential. Nowadays most sensitive information is transferred through the internet. Cryptography is very useful for network security. It consists of Encryption and Decryption. Using Encryption the plaintext is converted to unreadable Ciphertext. Format preserving encryption (FPE) means during encryption process the format and data type of the plaintext will never change . FPE is a string encryption scheme that made minimum changes to the plaintext. Black and Rogaway constructed three main techniques for format preserving encryption such as prefix cipher, cycle walking and Feistel network with cycle walking. I examine the prefix cipher model and add some enhancement in this model to propose a new method PREFIX - II .

Keywords:*Analysis of FPE, Data type preserving encryption, Format preserving encryption, FPE, Prefix cipher.*

I. Introduction

Encryption is a useful technique that converts the plaintext into unreadable ciphertext. During encryption the plaintext may be expanded or the data type may be changed. For example if the 16 digit credit number is encrypted using AES encryption scheme then the cipher text is 128 bits. It is a hexadecimal number. The length of the plaintext is increased as well as the data type is also changed. It needs lots of work and cost.

Table -1 : Database before Encryption

CustomerID	CustomerName	CreditCardNumber
1	N.S.Velu	1234-5678-9789-0124
2	S.Ushadevi	1234-5671-9988-7766
3	S.Dhivya	3456-7898-9789-0124

Using the Electronic code book (ECB) mode to encrypt an above database. This mode does not require any initial vector (IV). The plaintext should be multiples of 8 bytes.

Table – 2: Database after Encryption

CustomerID	CustomerName	EncryptedCreditCardNumber
1	N.S.Velu	0FDC19E6A777C539C49F67688C6D4E21D3F36066A506C85A
2	S.Ushadevi	0EDC27E6A777C835264AF4CE8BE570FFF44E842A72C00B
3	S.Dhivya	8408551E9C4A0F8FB49F67688C6C4E21D3F36088C206C85A

After encryption the length and data type of the credit card number field is changed. The queries and front end design related to that field will also be changed.

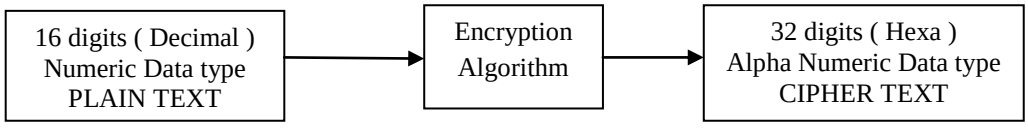


Fig. 1. Credit card number encryption using Normal Encryption Algorithm

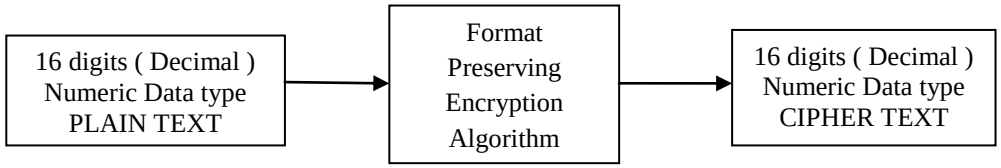


Fig. 2. Credit card number encryption using FPE Algorithm

Format preserving encryption is a preferable technique which encrypts the plaintext into ciphertext without changing the length and data type. When the FPE encrypts the N digit plaintext the output is also the N digit ciphertext.

II. Importance of FPE

- The modification to the database, application program and front end is minimized.
- The cost of modifying the database and the application program is also reduced.
- Most of the encrypted fields are used as an index of the table, FPE does not change the index.
- Referential integrity of the database is also maintained.
- In FPE both production database and test database are same.

III. FPE and MODERN CIPHERS

All the historical ciphers such as Caesar cipher, Monoalphabetic cipher, Poly alphabetic cipher etc, were supporting FPE. In all the cipher the length and data type of the plaintext and cipher text are same.The modern ciphers are mainly classified into two types. Symmetric key encryption and Asymmetric key encryption. In symmetric key encryption the single 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 the best example for modern ciphers. The ciphers are more secured and it is very difficult to break.

The main drawback in modern ciphers is the length of the cipher text to be produced. 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 modifying the database is too high. The queries related to the data base will also be changed. The graphical user interface such as visual basic could not support it.

IV. 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: The prefix method uses AES or 3DES algorithm. For example encrypting 16 digit credit card number applying an 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 plain text.

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 an acceptable range. The duration for ciphering is not deterministic.

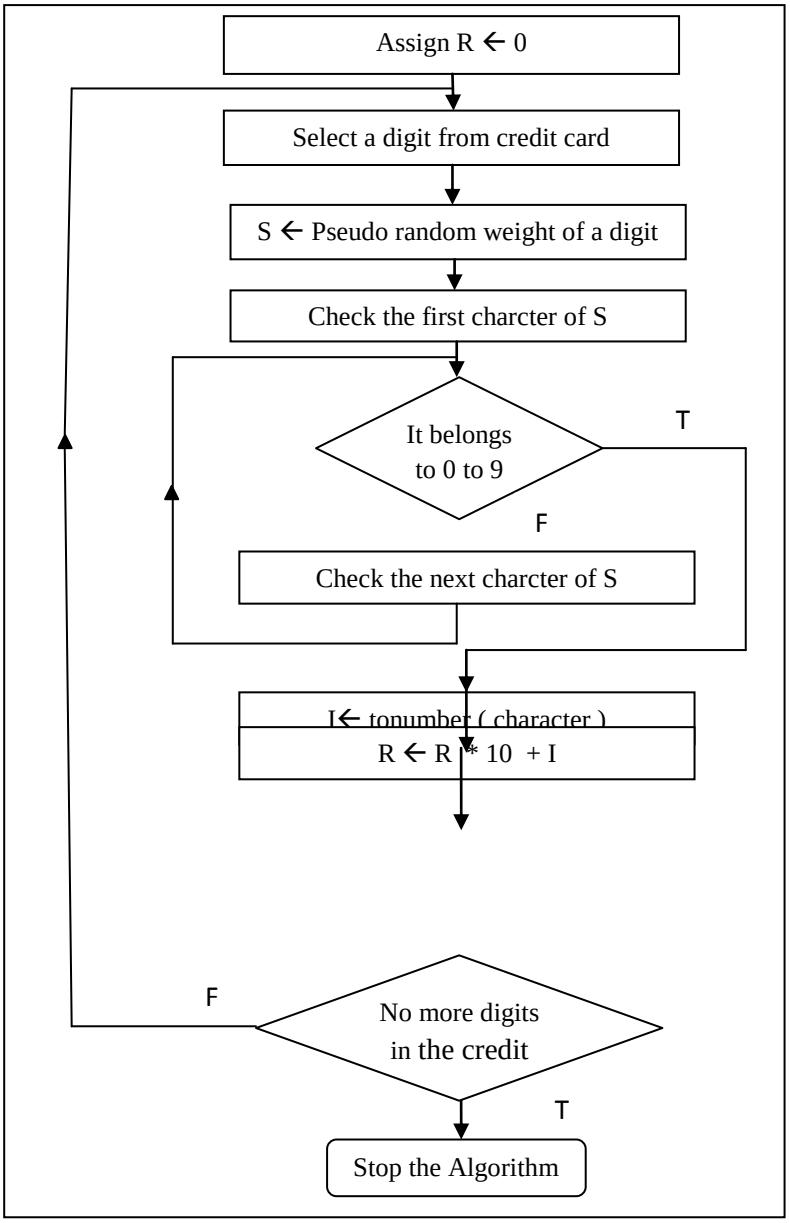
5.3 Feistel and cyclic method: The Feistel + Cycle construction is the combination of Two main techniques. First, the Feistel network that is constructed for the size of the given plaintext. This network used to encrypt the data. The cycle-walking technique is applied to the cipher text to provide the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

V. Prefix - II Ciphering

The main drawbacks in prefix ciphering is the time required to build the table which contains the pseudo random weight of each digit and the memory required to store the table. The pseudo random weight contains 32 digit hexadecimal number. Each table contains 16 entries.I propose some modifications to the Prefix method to develop new algorithm PREFIX – II. In PREFIX – II method instead of storing the 32 digit hexadecimal number in a table , select one numeric digit from it and discard the remaining digits. For all the 16 digits repeat the same process. At the end of the encryption process the cipher text contains exactly 16 digit decimal number which is same as plain text. The PREFIX – II method mainly contains three steps.

i. Generate pseudo random weighted for each digit.
ii. Select one digit from the weight.
iii. Adding the digit to cipher text.

Repeat the above three steps for all the digits. Finally we get 16 digit numeric cipher text.



5.1 Pseudo Random Weight: Using modern cipher AES to calculate pseudo random weight. The AES generates 128 bit ciphertext that is 32 digit hexadecimal number. Store the hexadecimal number in a string S which contains 32 characters. For each digit in the plain text the same string is used. Each iteration it receives new value. Initialize the variable R to 0.

5.2 Select A Digit: Examine the string by checking each character. Starting from the first character check whether it belongs to the digits 0 to 9. If the condition is true store a character and stop the checking process. Otherwise repeat the process until finding a character. Convert a character into the number data type and store it in a variable I.

5.3 Generate A Ciphertext: Multiply the R by 10 and adding I to the product. Store the result in the variable R.. At the end of the sixteenth iteration the variable R contains final cipher text.

5.4 Example:

7 - **1**2d76795b5e818b38be9813260ab0c5f --- 0 * 10 + 1 = 1
3 - **2**03c3c515ae6101c4858fe07ecb78ec0 --- 1 * 10 + 2 = 12
5 - d**9**9851ff58a9bf03d717ff6601639795 --- 12 * 10 + 9 = 129

In an above example for simplicity I consider only 3 digits. Repeat the same process for all the 16 digits we get the 16 digit credit card number as as cipher text.

VI. Prefix – II Method Performance

The PREFIX – II algorithm is very simple to implement. There is no need to build and store the table for each digit like prefix method. The time and memory requirement is reduced. It involves only simple arithmetic operations like addition and multiplication. It is also applicable for large values. The encryption and decryption is very fast. In prefix method, for 16 digits nearly 700 milliseconds are required to build the table. This time is reduced in PREFIX – II method.

VII. Conclusion

Format preserving encryption is useful for many of our real life applications such as credit card number and social security number. Using Format preserving encryption the database schema, queries and application programs related to the database will never change. The cost and time for changing the database is minimized. In future FPE will be achieved by making small changes in the existing block cipher implementation without adding extra work.

VIII. Acknowledgement

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

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] Format Preserving Encryption Terence SpiesVoltage Security, Inc.
[4] 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.
[5] Information security management Hnadbook, volume 6 by Harold F.Tipton, Micki Krause nozaki
[6] A new integer FPE scheme based on Feistel Network (Jia, Z Liu, J Li, Z Dong, X you advances in Electric and Electronic, 2012 Springer.