# Implementation of Encryption Data Table by Using Multi-Keys

**Maitham Ali Naji**

***Abstract*— The paper presents an encryption application that is able to work with data access table. In this paper the Caesar method is developed to generate one key to each record. The length of the key is computed from first word of record. The record after encryption will be stored in separate line in text file that separate each field by semicolon, this process will continue until the end of table.***

***Index Terms*— Caesar Cipher, Database Encryption, Text File, and Visual Basic.**

## I. INTRODUCTION

Encryption is a process of encoding a message so that its meaning is not obvious [1]. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a difference form [2].

Cryptography is the science of using mathematics to encrypt and decrypt data .Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptanalysis is the science of analyzing and breaking secure communication [3].

Conventional database security solutions and mechanisms are divided into three layers; physical security, operating system security and DBMS (Database Management System) security [4].

Typically DBMS provides two ways to achieve security access control and data encryption. Access control is a relatively older way to protect sensitive data. However, access control by itself is not sufficient. An adversary who gains access to the database files can access sensitive data, thus, bypassing the access control mechanism. As a result, it is necessary to encrypt data in the DBMS [5, 6].

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet [7], while the current system the number of shifting (key) characters is variable to each record in the table to increase the probability of broken message in addition the key is included with the message therefore the decryption algorithm can get the key from the cipher text.

Manuscript received on May, 2014.

**Maitham Ali Naji,** Power Engineering Department, College of Electrical and Electronic Techniques Baghdad / Iraq

## II. LITERATURE SURVEY

Several database encryption methods have been proposed in the literature. The one presented in [8] is based on Chinese - Reminder theorem, where each row is encrypted using different sub-keys for different cells. This schema enables encryption at the level of rows and decryption at the level of cells.

Data is valuable assets of an organization. So its security is always a big challenge for an organization. In recent times security of shared databases was studied through cryptographic viewpoint. A new framework was proposed in which different keys are used by different parties to encrypt the databases in assorted form that was named as mixed cryptography database (MCDB) [9].

## III. THE SYSTEM'S FLOWCHARTS

The system capable of encrypting any table in the database, the program will ask the user to specify the database name and table name (record source) properties to the data control object. As shown in Fig. 1.

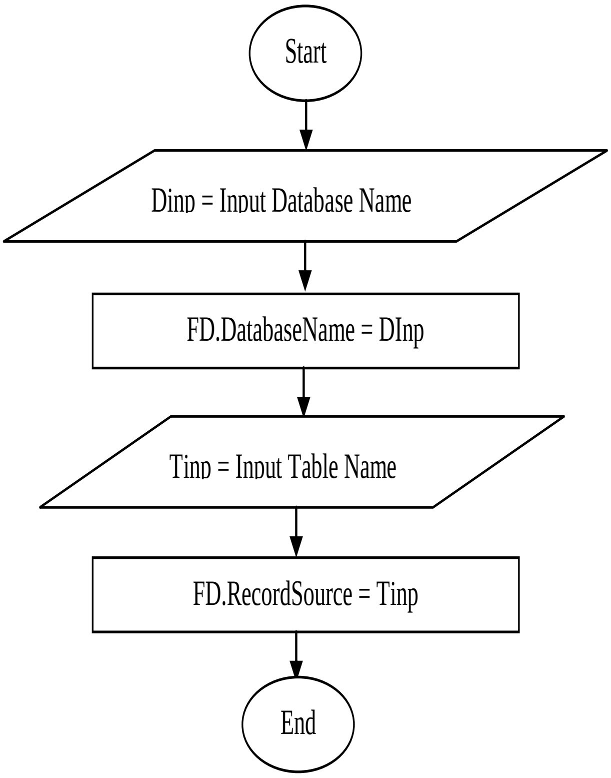
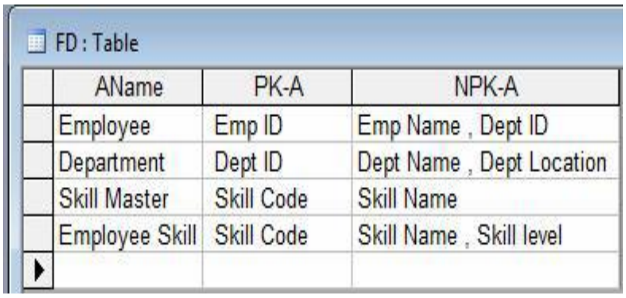


Fig.1 Assign Database Name & Table Name to Data Control Object

In our implementation we assume the database name is "FD.MDB" and the table name is "FD" as shown in table (1). The FD table will be an input to the system.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.*

Table (1): FD Table



FD : Table

| AName | PK-A | NPK-A |
|---|---|---|
| Employee | Emp ID | Emp Name , Dept ID |
| Department | Dept ID | Dept Name , Dept Location |
| Skill Master | Skill Code | Skill Name |
| Employee Skill | Skill Code | Skill Name , Skill level |
| | | |

The record set of the Data object control has a table collection properties like (fields number, records number,.., etc), the system will extract fields number from field property in record set as shown in Fig. 2.

The flowchart in Fig. 2 has nested loop, the main loop repeated until the end of FD table, in each iteration take one record and the content of AName field is stored in an array by using Split function [10].

The Caesar's key length will be generated by computing the length of first word as shown in table (2). The number of iteration of the second loop is determined by number of fields in each record. The field's data and the key of the record will be sent to Caesar function to obtain cipher text.

Table (2): Key Length for Each Record

| Word1 | Word2 | | Key Length |
|---|---|---|---|
| Employee | | … | 8 |
| Department | | … | 10 |
| Skill | Master | … | 5 |
| Employee | Skill | … | 8 |

The cipher fields are added in variable (N) that separate each field to other by semicolon symbol (";") as shown in Fig. 2. Finally the encrypted record will be stored in text file in separate line. This process is continued until the end of table.

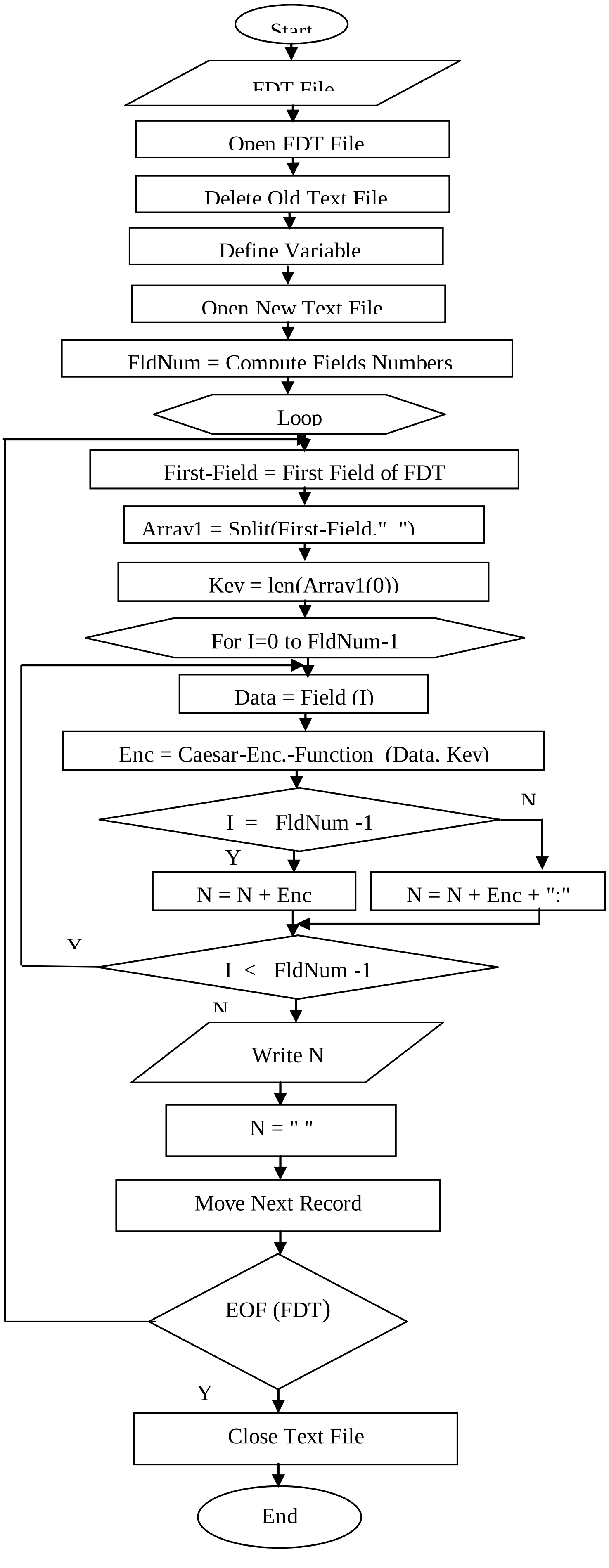


Fig. 2 Creating Text File

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

The Caesar function shown in Fig. 3 start by computing the length of the data to make iteration according to the length, each time the program gets single character by using built in Mid function [10].

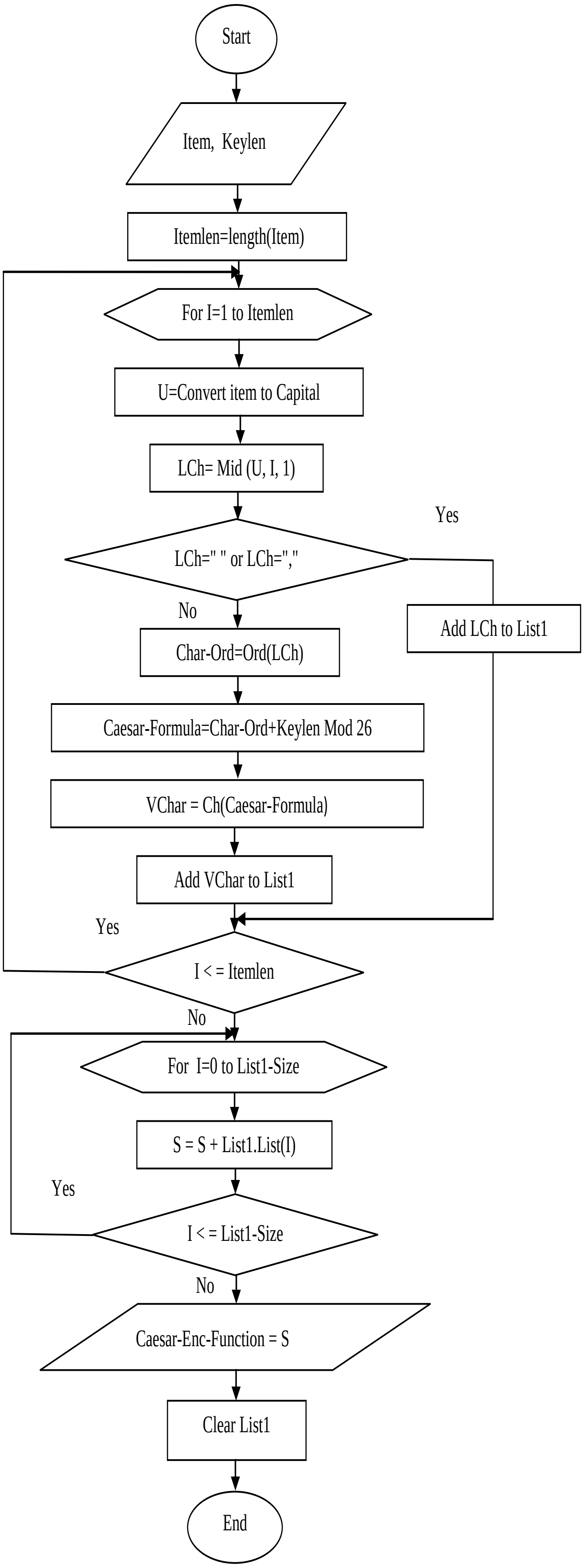


Fig.3 Caesar Function

The character is sent to **Ord** function to get the order of character. A new order is obtained from the Caesar formula.

Caesar formula = (Character-order+ key) mod 26.

The order of character "E" = 4 and the key of first record is 8.

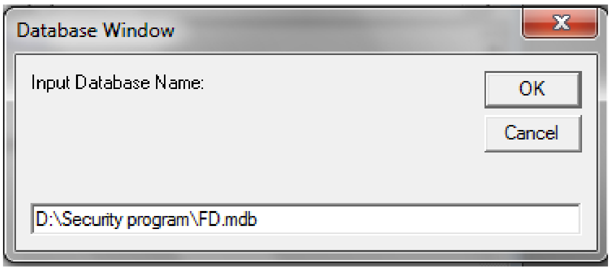
E(4+8) mod 26 =12

The **Ch** function gets character according to its order for the above example the output of Caesar equation is (12) and by using Ch function, the character "E" will be converted to "M" character.

The Ord and Ch functions are programmed as a Module in visual basic in order to be public to the project. This process will continue to convert the plain text of each field to cipher text and storing the character of cipher text in a list, and then the items of list will be collected to produce cipher text.

## IV. THE IMPLEMENTATION

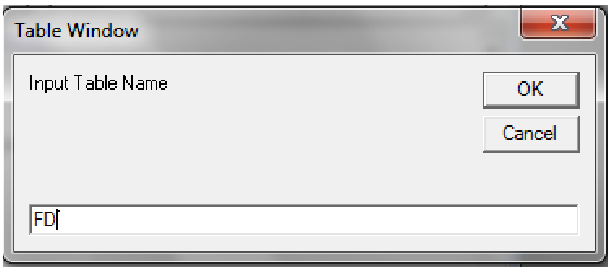
The system has been implemented by Visual Basic 6. When the system is executed an input box are appeared to input the database and table names as shown in Figs. 4,5.



Input Database Name:

D:\Security program\FD.mdb

Fig. 4 Input Database Name



Input Table Name

FD

Fig. 5 Input Table Name

The main window shown in Fig. 6 will appears after the database name and table name are assigning to data control.

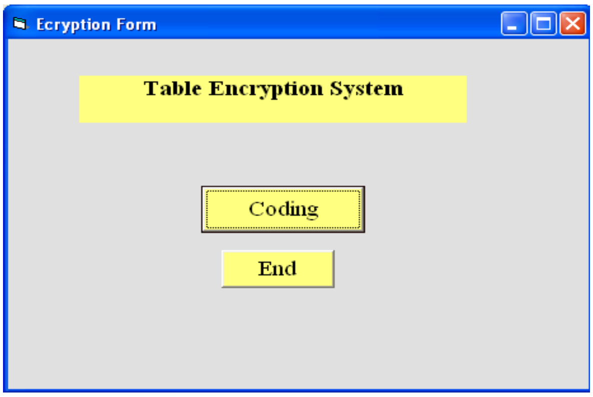
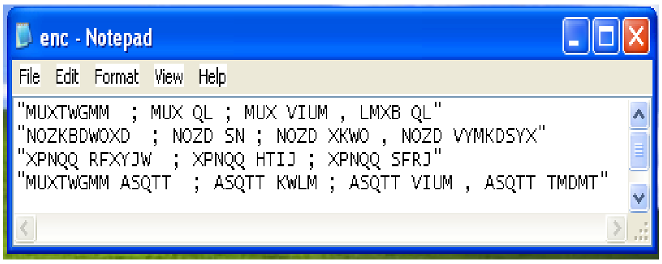


Fig. 6 Main Form Window

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

The command button "Coding" is executed by click event. The system will take the input from FD shown in table (1) and make a process to encrypt it. The result will be store in text file called "enc" as shown in Fig. 7.



```
"MUXTWGMM  ; MUX QL ; MUX VIUM , LMXB QL"
"NOZKBDWOXD  ; NOZD SN ; NOZD XKWO , NOZD VYMKDSYX"
"XPNQQ RFXYJW  ; XPNQQ HTIJ ; XPNQQ SFRJ"
"MUXTWGMM ASQTT  ; ASQTT KWLM ; ASQTT VIUM , ASQTT TMDMT"
```

Fig. 7 Convert FD Table to Text File

## V. CONCLUSION

Three points can be concluded from this paper. First the Caesar method is developed by generating different keys and the keys are included with cipher text. The second point, the speed of encryption is very high. Finally the current system reduces the storage space.

## VI. FUTURE WORK

The Text file may be sent through transmission medium to destination party, therefore the destination should have decryption system.

The decryption system converts encrypted text file to access data table, this can be done by determining and creating fields number from semicolon number and then create the database and it is table by using Data Access Object (DAO).

The system can be developed to encrypt all objects in the database.

## REFERENCES

[1] Lee, K, H., "Basic Encryption and Decryption", on line document http://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/Kwang.pdf

[2] Freeman J., Neely R., and Megalo L., "Developing Secure Systems", IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45, 1998.

[3] "The Basics of Cryptography", on line documents ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

[4] Fernandez EB, Summers RC, Wood C, "Database Security and Integrity", Addison-Wesley, Massachusetts, 127, 1980.

[5] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption", In Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997.

[6] O. Goldreich, "Foundations of Cryptography", Cambridge University, Press, 2003.

[7] Stalling W., "Cryptography and Network Security Principles and Practices", Printice Hill publishing, PP. 36, 2005.

[8] Davida GI, Wells DL, Kam JB; "A Database Encryption System with Sub-keys". ACM Trans. Database Syst. 6, PP. 312-328, 1981.

[9] Kadhem, H.; Amagasa, T.; Kitagawa, H.; "A Novel Framework for Database Security based on Mixed Cryptography", Internet and Web Applications and Services. ICIW '09. Fourth International Conference on; Publication, 163 –170, May 2009

[10] VB Help, "Microsoft Developer Network (MSDN)", 2001.