Implementation of Converting Text File to Data Access Table by Using Multi-Keys

Maitham Ali Naji

Abstract— The aim of this paper converts encrypted text file to access data table. The system infers the   number of fields from the number of semicolon in any line of text file. The program will create the database and its table by Data Access Object (DAO), the key of Decryption will be extracted from the first word in each line. The Caesar method is used to produce plain text to data table.

Index Terms— Caesar cipher, Caesar deciphering, Database Engine, DAO hierarchy, DAO programming, Scripting objects, and Visual Basic.

———————————————————— u ————————————————————

1 Introduction

The translation of encrypted text or data into original text or data (called plaintext), also called deciphering [1]. An encryption algorithm tells the sender how to process the plaintext using the key, thereby producing the cipher text that is actually transmitted. An encryption scheme also specifies a decryption algorithm, which tells the receiver how to retrieve the original plaintext from the transmission while possibly performing some verification, too. Finally, there is a key-generation algorithm, which produces a key that the parties need to share [2]. Caesar Cipher is or was probably the very first encryption methodology. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on [3]. The previous paper encrypt access table to text file, the key for each record is differ from other record. This paper is decryption system of previous paper.

2 Literature Survey

The basic technological meaning of Transparent Data encryption is encoding or encrypting databases on networks, hard disk and/or on any backup media to provide highly configurable, transparent, safe and secure environments for application development. Microsoft SQL Server 2008 uses this technology to encrypt database content stored on any network, disk or backup medium along with process of creation of a Master Key. This involves creation of key, protection by the certificate and ways to set the database to use in Microsoft SQL Server 2008 encryption. This study investigates what Microsoft SQL Server 2008's configurable environment has to offer in terms of data safety, security and application development for developers. [4]

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). [5]

3 Database

The Database object is the most important object we will be dealing with because it allows us to interface with the database.   To look at the structure of a database, we need first look at the objects, collections, and properties that exist in our DAO hierarchy. Fig 1. shows the relevant structure and properties [6,7].

I-TableDefs

TableDefs is a collection of TableDef objects. The TableDef is a representation of the Oracle/Visual Basic tables in the database we have opened and have access to.

II-Fields

Of more interest than the table names are the fields that exist in the table. Each TableDef object contains a Fields collection, which in turn contains one or more Field objects. The most important properties are (name, size, source field, source table, type and value).

III-Indexes

Just as you can look at the various fields you have in a table, you can also view the indexes on it. Each TableDef object can have an associated Indexes collection with one or more Index Object in it. The most important properties are (fields, foreign, name, primary and unique).
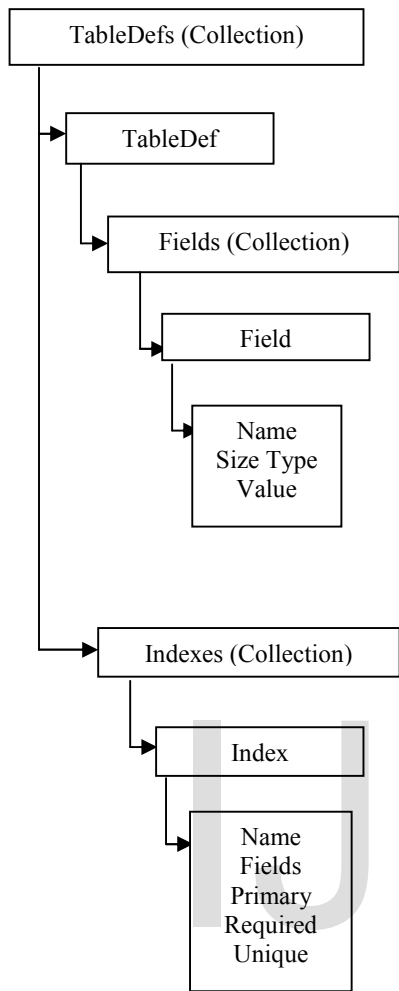
Fig 1. The Tabledefs Collection Hierarchy [6]

4 The System's Flowcharts

The system passes through five stages to produce plain table, as shown in fig 2.
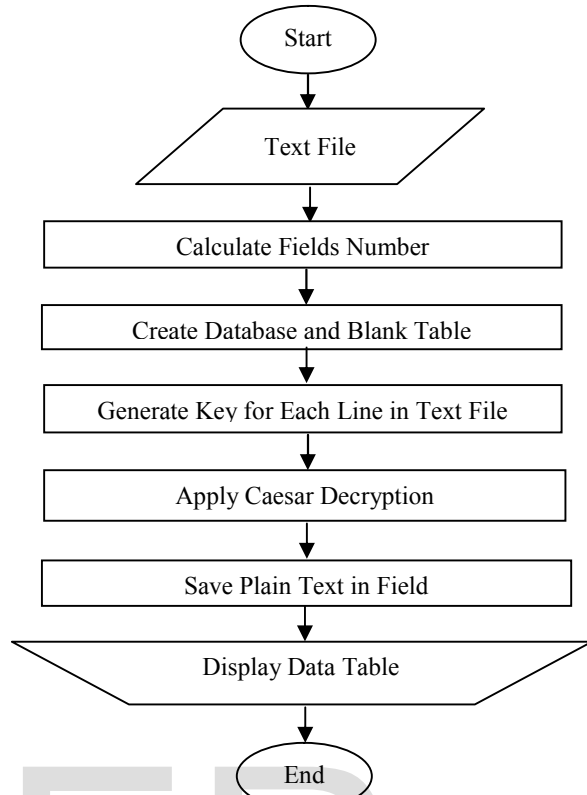

Fig 2. Text File Decryption Diagram

In previous paper, the author convert access table to cipher text file by using Caesar method base on fixed keys in which the key was variable to each record, as shown in fig 3.
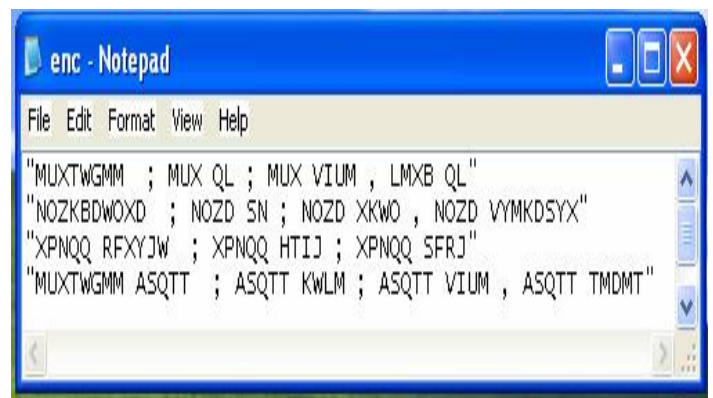

Fig 3. Access Table Encryption

The text file will be an input to the current system. The program is implemented with visual basic 6, so we need to add an object that deal with text file, this object called

Scripting Objects [8]. The first stage the program will compute the number of semicolon plus one from the line of text file which presents the number of fields in table as shown in fig 4.
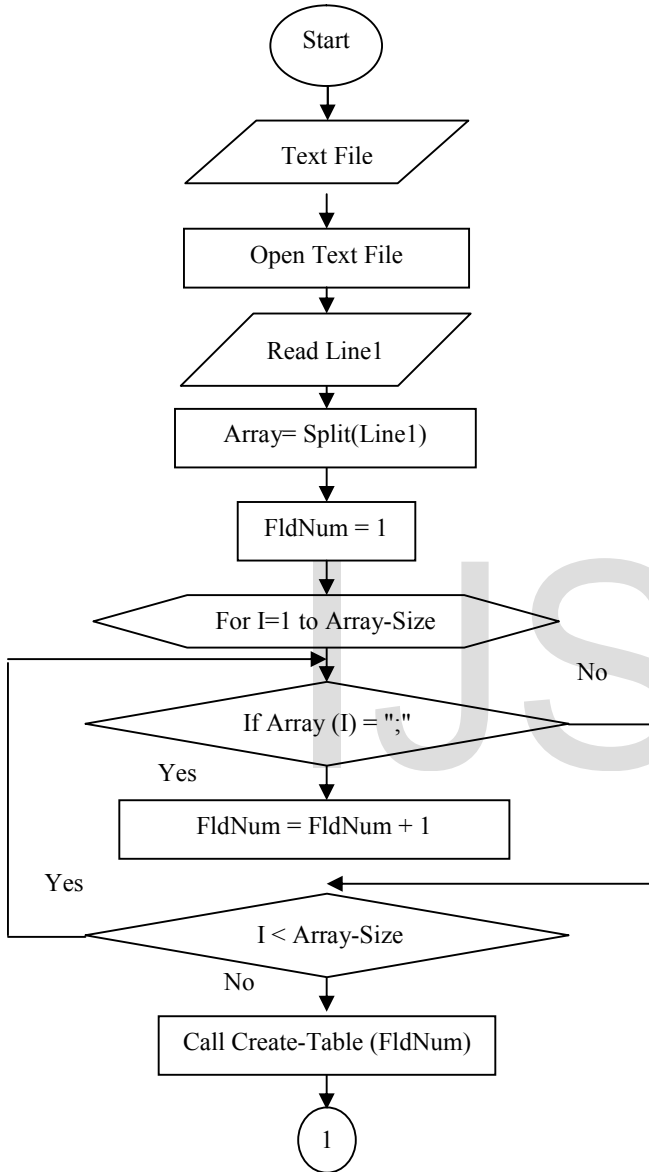

Fig 4. Fields Number Extraction

The above figure use "Split" built in instruction in order to convert the text line in an array [9]. In our example, the number of field will be 3. The second stage the fields' number will be passed to procedure called Create Table as shown in fig 5.
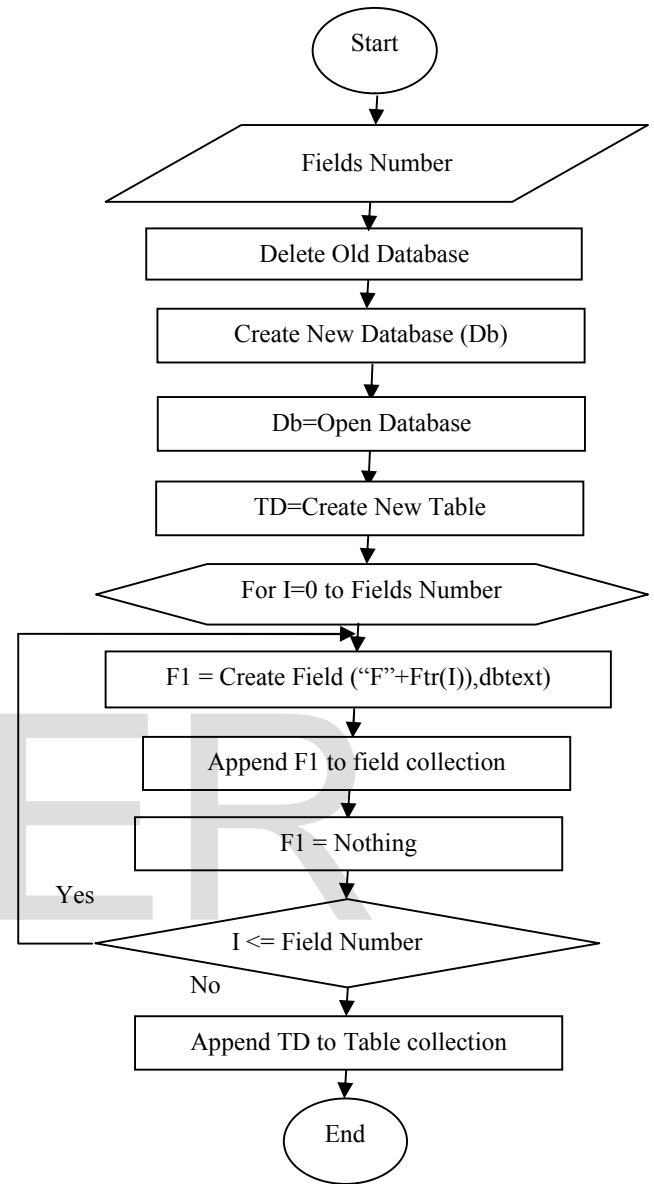

Fig 5. Create Table Procedure

The procedure Create Table has the following sequence:

1- Delete old database.

2- Create new database.

3- Create new table.

4- Create new fields according to the field's number and add them to the collection as illustrate in fig 1.

5- Add table to the collection as illustrate in figure (1).

After the database and tables has been created the key of Caesar method will be generated for each line in text file. The key will be differ from one line to other, the key can extracted from the first word before first semicolon, so the key for text file are:

First line is "MUXTWGMM" = 8

Second line is "NOZKBDWOXD" = 10

Third line is "XPNQQ" = 5

Fourth line is "MUXTWGMM" = 8

The following flowchart has two nested loop the main loop will generate key for each line and add new record to the table. The second will assign decrypted data (plain data) to table's field. This process will be repeated until the end of text file. As shown in fig 6.
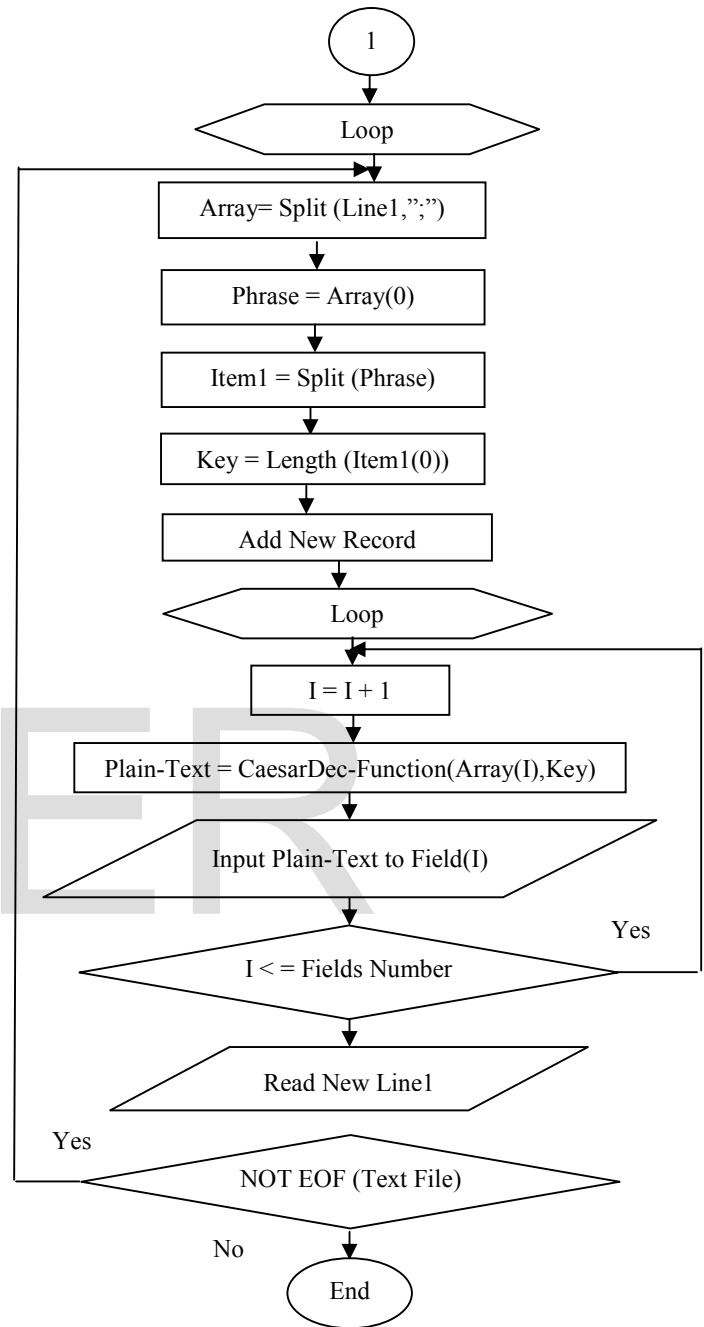

Fig 6. Caesar Key Generation and Assign Data to Table's Field

The input parameters of Caesar decryption function shown in fig 7. are an item (field of record) and the key. The flowchart first extracts the length of the item in order to make iteration according to the length; in each iteration the program gets single character by using built in MID

function. The character is sent to user define function called Ord to give the order of character set for example (A has order 0, B = 1, … Z=25) also we built another function called Ch that give the character according to the order. These two functions programmed as a Modula in visual basic in order to be public to the project, after that the system will apply the following Caesar decryption equation as shown below.

Caesar-Formula = (Character-order – key) .. 1

   When the result of first equation is negative the system will apply the second equation.

C = 26 + Caesar-Formula ………………... 2

For example the length of key of first line is (8) and the order of letter (N) is (11) By applying equation (1), 11-8 = 3 by using Ch function the system will return the letter "D"

While the order of letter (B) is (1) and the key of second line in text file is (10) by applying the first equation 1-10 = -9

The result will be negative therefore the system will apply the second equation

C = 26 + (-9) = 17 = R

   This process will continue to convert the cipher text in each line to plain text by storing the character of plain text and the character space and coma in a list. Finally the flowchart has a loop to collect the decrypted character to produce plain text. As shown in fig 7.
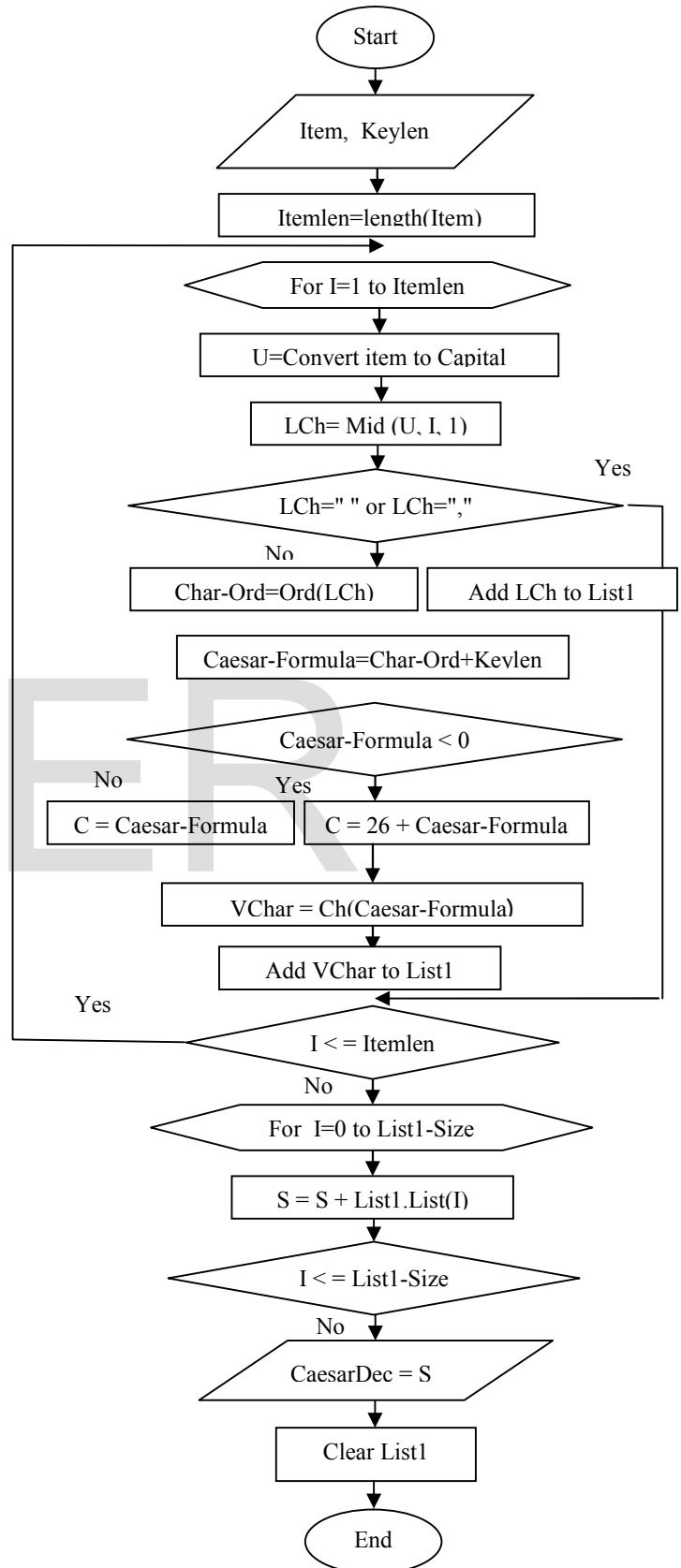
Fig 7. Caesar Decryption Function

5-The Implementation

The system has been implemented by Visual Basic 6 as shown in fig 8.

Fig 8. Main Form Window

The command button "Decryption" is executed by click event. The system will take the input from Text file shown in above fig 3. The program will create database as shown in fig 9, when the database executed the user select option button "Open Database" to see blank table named "FDT" that has a field according to the number of semicolon plus one as shown in fig 10.

Fig 9. Create Database

Fig 10. Create Blank Table

The text file will be decrypted line after line and the result will store in records. As shown in fig 11.
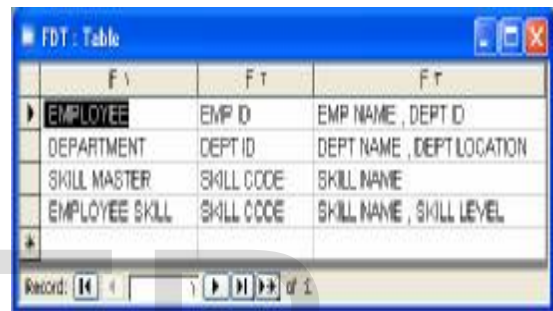

Fig 11. Decryption Text File to Access Table

6- Conclusions

Many points can be concluded from this paper:

1- The system can generate table with unlimited number of field.

2- The key of decryption is variable in each line and it is included with text file.

3- The intruder cannot expect the text file is an access table.

4- The speed of decryption is too high because the system passes through one process.

7-References

[1] Stalling W., "Cryptography and Network Security Principles and Practices"; Prentice Hill publishing, p36-38, 2005.

[2] "Symmetric Encryption", http://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf. (URL link)

[3] Somdip Dey,"SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted", on line documents http://arxiv.org/ftp/arxiv/papers /1205 /1205.4279.pdf. (URL link)

[4] Dr. Anwar Pasha Abdul Gafoor Deshmukh; Dr. Anwar Pasha Abdul afoor Deshmukh; Transparent Data Encryption- Solution for Security of Database Contents; (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[5] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Page(s): 163 – 170, Conference on; Publication Year: 2009.

[6] Snowdow, N, "Oracle Programming with Visual Basic"; SYBEX Inc,USA,495, 2002.

[7] Dr. A, Aziz, Dr. A. Saluman, "Database Programming" Shwaa for Scientific and Publishing",Surya,235, 1999.

[8] P. Evangelos, "Mastering Visual Basic 6", SYBEX In, USA, 1062-1069, 2000.

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