Indonesian Journal of Electrical Engineering and Computer Science
Vol. 17, No. 3, March 2020, pp. 1499~1505
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v17.i3.pp1499-1505

Methods for database ciphering

Maitham Ali Naji[1], Dalal Abdul mohsin Hammood[2], Nuha Abdul Razzaq Yahya[3]
College of Electrical and Electronic Engineering Techniques, Middle Technical University (MTU), Iraq

Article Info

Article history:

Received Jun 13, 2019
Revised Aug 3, 2019
Accepted Sep 4, 2019

Keywords:

Caesar cipher
Data access object
Database security
Text file
Vigenere cipher

ABSTRACT

In this paper Caesar and Vigenere methods have been used for table ciphering. Each record has unique and independent keys to the next record to get high security. The cipher text stored in script file that separates the content of fields by semicolon. The second part is the process of creating a new database using the Object called Data Access Object (DAO) and then create table and it is fields. The program gets plaintext of the table by applying the decryption rules of two methods.

Corresponding Author:

Maitham Ali Naji,
College of Electrical and Electronic Engineering Techniques,
Middle Technical University (MTU), Iraq.
Email: maitham_naji@mtu.edu.iq

1. INTRODUCTION

Typical database security divided to three levels; physical security, operating system security and Database Management System (DBMS) security [1]. Normally DBMS gives two methods to accomplish security access control and data encryption. Access control is an older method to protect important data, as a result access control is not enough to protect sensitive data, therefor data encryption methods are used to protect sensitive data in DBMS [2]. This paper applies Caesar and Viginere methods for database encryption and decryption.

Caesar is mono alphabetic cipher. The idea of Caesar method involves shifting the character in alphabet via three places to take other character in alphabet [3] for example A → D. Vigenere method is Poly alphabetic cipher. Vigenere includes the use more than one cipher alphabets. That is mean each character in alphabet has many cipher characters [4] for instance A → D, A → F and A → L.

Friedman calculates the frequency of English letter to determine whether the method is mono alphabetic or poly alphabetic cipher; this is done by accounting the index of coincidence (I) or repeat rate. Friedman notes according to the Greek study, the Value of (I) is changed between 0.038 and 0.065, If (I) near 0.065 means the method is mono alphabetic like Caesar and Affine methods otherwise the method is Ploy alphabetic cipher like Vigener[5]. That is mean Poly alphabetic more secure than mono alphabetic cipher.

2. DATABASE

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

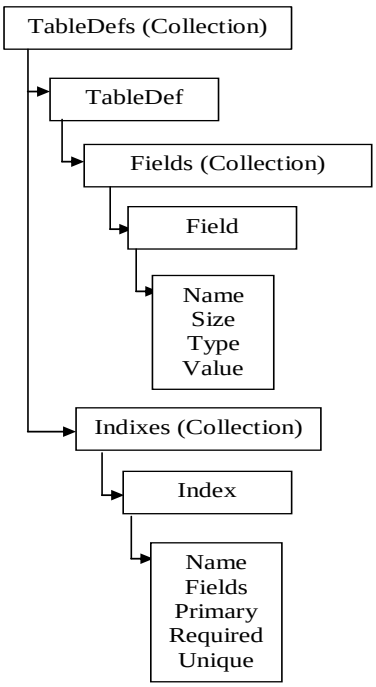

Figure 1. The tabledefs collection hierarchy [6]

2.1. TableDefs

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

2.2. Fields

Every TableDefs has one or more fields object. Each field contains many properties like (name, size, source field, source table, type and value).

2.3. Indexes

Every table may have one or more indexes.

3. RELATED WORK

The authors in this paper enhance affine ciphering and deciphering algorithms by using different keys length for each record [7].

The Author in [8] confirms that most application need database. Database may contain sensitive data that may be attack by third person. This paper discussed much kind of attacks on database and reviews some techniques for database security.

In [9] the author applies database security in any level of DBMS. The propose research contain four stages requirements collection, many level relational construction, DB analysis and logical construction. The propose system applies actions for analysing and developing a secure DB.

K. Kusnardi and D. Gunawan use Guillo-Quisquater protocol to allow server to authenticate user with zero knowledge (without knowing the user's password). Two login methods were used file-based certificate with key and local storage [10].

In [11] the user request access the data stored in desk computer through fingerprint biometric. The entropy value system generates fingerprint secret code when the user (authorized person) requests access. The fingerprint is verified with the database in the desk computer. If it is matched, then the computer can be accessed by the request person.

Picture Stream depending on Starting Late Various Fierce Key was proposed as a new Cipher technique [12]. A cluttered key-based scheme for image ciphering and deciphering, in which diminish measurements of each image pixel is processed using XOR or XNOR functions with a smidgen at a chance of introducing any of the two destined keys. The authors kept concentrate on three cornerstone components, as example rigid security, simple computations and without turning.

The authors in [13] proposed an image count to encode corresponding pixels from propelled pictures by pixel. Then such count can use stream assume to encode each image pixel using a novel logical course of limits known action to be the propose key. Such assessments adopted a similar key at each of the source and the destination. Other techniques of image encryption were also starting late proposed subject for substitution muddled.

In [14], they adopted S-encase pushed encryption standard (AES) theory for count reliant as an image encryption technique. They demonstrated (30) diverse S-boxes by different constant polynomials. All segments of the S-boxes were assigned to (0 to 255) numbers and they were also adjusted mapped. The assigning process used vital reference that depended on a related reference as one of the 30 S-boxes is going to be adopted in the process of byte substitution till completing scrambling of the entire picture.

According to the authors of [15], an estimation of image encryption is adopted, which accomplished using an outside key of 256-piece. In this technique, the pixel in the end of plain picture is considered to provide the parameters and the basic states of the cluttered systems for the essential S-box. The plain image is divided into social events in which each pixel is replaced by S-boxes. The image pixels are separated into couples of corresponding regarding image sections and adjacent lines that can be assembled over multiple social events. Over each these events, they make and use another S-box. Accordingly, the reviews between vertically adjacent pixels are distorted. After that, they use a comparable technique on divided parts to pound its modifications between adjacent pixels of the same level.

The authors of [16] illustrated that the count image ciphering which is under key stream support and non-direct substitution box was pre-determined. The authors considered the S-box for this circumstance as a round gathering with a head pointer, and individual pixels of the image are combined by an S-box segment due to the head pointer and the pixel regard, Head pointer is then changed with the prior substituted pixel. Yielded results illustrated that some ciphering techniques of S-box-just have some weakness against chosen plaintext ambushes.

According to Y. Zhang and D. Xiao [17] security issues of the image (S-box-simply) ciphering technique was purposely analyzed in addition to displayed a productive deciphering technique.

Recently, for figuring the turmoil, several techniques were conducted depend on Stream-Cipher branch of Cryptography. Traditional type of Stream-Cipher Cryptography has XORing as the cornerstone to make secure discretionary. Action number course was a subject to sliced maps (as an example Bernoulli Map, key guide, or Tent Map) with the original image to get the ciphered one. Such approach of Stream-Cipher is obviously vulnerable against the attacks of chosen plaintext. Their technique provided different stream-Cipher count, which was related to incredible S-box. Their proposed estimation adopted one S-box and a scattered enhancing technique. Individual bytes in the vector of spatial-domain picture are replaced depending on another S-box in order to get the vector of the Ciphered image. Their technique yielded safe results for picking plaintext strikes. In addition, this count is increasingly ensured as secured against customary type of stream Cipher [18]. A reliable ciphering technique must be rigid against different techniques of cryptanalysis and other attacks.

4. RESEARCH METHODS

This paper used modulo 35 instead of 26, where the order of alphabet from (0-25) and the order of digits from (26-35). The author assumes the database name is "Cust.MDB" and the table name is "Customer" as shown in Figure 2. The Customer table will be an input to the system. 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.

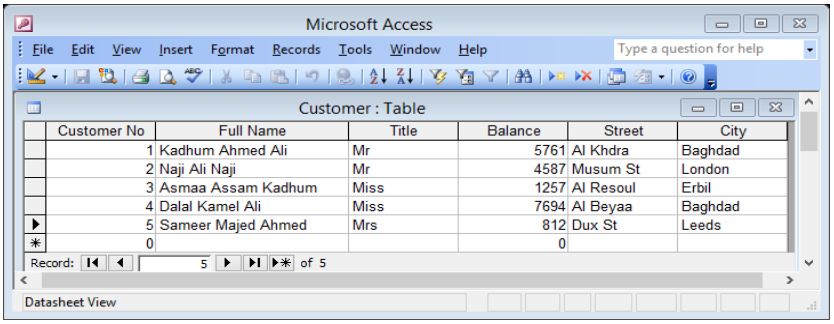

Figure 2. Original Customer Table

The Algorithm (1) has nested loop, the main loop repeated until the end of Customer table, in each iteration take one record while the second iteration take a field from record to accomplish Caesar and Vigenere encryption, the key of Caesar shown in Table 1, is calculated by sum the length of "Full Name" and "City" fields for each record, for example the key is applied on word “AL KHDRA” in “Street” field as shown in Table 2 and the encryption result of the “Customer” table shown in Figure 3, while the key of Vigenere method is extracted from "balance" field that saved in a text file as shown in Figure 4. The key of Vigenere is applied to Caesar cipher to produce Vigenere cipher text as shown in Table 3 and the result shown in Figure 5.

Algorithm(1) A pseudo-code for Creating Encryption Text Files

```
Begin
 Open database
 Open blank text file
 F= Get fields numbers from table
While (not end of table)
 Caesar-Key1 = length of Full Name Field
 Caesar-Key2 = length of city field
 Caesar-Key = Caesar-key1+Caesar-key2
 I=0
Loop
 Data = Field(I)
 I=I+1
 Caesar- Encryption = Call Caesar-Encryption-Fun. (Data, Caesar-Key)
 Vigenere-Key = length of balance field
 Vigenere- Encryption = Call Vigenere-Encryption-Fun. (Caesar-Encryption,Vigenere-Key)
Repeat Until (I=F)
 Print (Caesar-Text, Vigenere-Text, Vigenere-Key)
 Move Next Record
 End While
```

Table 1. Records Key Length

Full Name	Key1 Length	City	Key2 Length	Key1 + Key2
Kadhum Ahmed Ali	16	Baghdad	7	23
Naji Ali Naji	13	London	6	19
Asmaa Assam Kadhum	18	Arbil	5	23
Dalal Kamel Ali	15	Baghdad	7	22
Sameer Majed Ahmed	18	Leeds	5	23

Table 2. Caesar Encryption Example

Plain Text	A	L	K	H	D	R	A
Character Order	0	11	10	7	3	17	0
K=Key1+Key 2	23	23	23	23	23	23	23
(Character Order + K) Mod 35	23	34	33	30	26	5	23
Caesar Chiper Character	X	8	7	4	0	F	X

Table 3 Vigenere Encryption Example

Caesar Chiper	X	8		7	4	0	F	X
V1	23	34		33	30	26	5	23
Vigenere Key	5	7	6	1	5	7	6	1
V2	31	33	32	27	31	33	32	27
(V1+V2) Mod 35	19	32		25	26	24	2	15
Vigenere Chiper	T	6		Z	0	Y	C	P

The first step of Vigenere decryption process, the system calculates semicolon number in the line of text file which presents the number of fields in the table, in order to create blank database and table with field’s name. The first loop in algorithm (2) takes line from Vigenere cipher and Vigenere key that applies Vigenere decryption rule to obtain Caesar cipher for instance shown in Table 4. This process continues until the end of file. The second loop extract key length from Caesar text file and apply Caesar decryption rule to produce plan text for example shown in Table 5 and the final result shown in Figure 6.

Algorithm (2) A pseudo-code for Creating Plain Database

```
Begin
 Fields Number = Number of semicolons in each line
 Create and open Database

For I=0 to Fields Numbers
 Input Field Name
 Create Field in table collection
Next I

Loop
 V= Read line from vigenere text file
 Vkey= Read line from Vigenere Key text file
 Apply Vigenere –Decryption (V,Vkey)
 Write Decryption text (Caesar Text) in text file
 Repeat Until End Of File

 Loop
 C= Read line from Caesar text file
 Key1= Extract first key Length
 Key2= Extract Second Key Length
 Apply Caesar -Decryption
 Write Plain text in Database Table
 Repeat Until End Of File
 End
```

Table 4. Vigenere Decryption Example

Vigenere Chiper	T	6		Z	0	Y	C	P
V1	19	32		25	26	24	2	15
Vigenere Key	5	7	6	1	5	7	6	1
V2	31	33	32	27	31	33	32	27
(V1-V2)>0 F=(V1-V2) Mod 35 (V1-V2)<0 F=((V1-V2)+35) Mod 35	23	34		33	30	26	5	23
Caesar Chiper	X	8		7	4	0	F	X

Table 5. Caesar Decryption Example

Caesar Chiper	X	8		7	4	0	F	X
V1	23	34		33	30	26	5	23
K=Key1+Key 2	23	23		23	23	23	23	23
V2	31	33	32	27	31	33	32	27
(V1-V2)>0 F=(V1-V2) Mod 35	0	11		10	7	3		0
(V1-V2)<0 F=((V1-V2)+35) Mod 35							17	
Plain Text	A	L		K	H	D	R	A

5. RESULTS AND DISCUSSION

The system has been implemented in Visual Basic 6. The project has two main Commands "Table Encryption" and "Table Decryption". When the "Table Encryption" buttons is clicked the system requests the path and name of database and table name, the system will process the "Customer" table and generate Caesar file is called "Caesar". As shown in Figure 3.

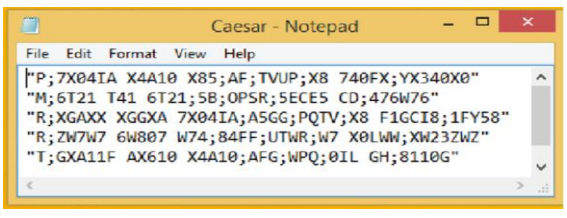

Figure 3. Caesar encryption file

The Caesar encryption file and Vigenere keys file processed by vigenere encryption program. The system takes row from Vigenere key file and row of Caesar file to produce cipher text by vigenere method. The process will be continued until the ends of two files in which the results saved in text file called "Vigenere" as shown in Figure 5.

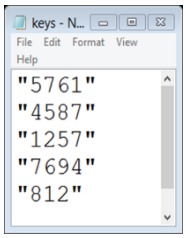

Figure 4. Vigenere KEY FILE

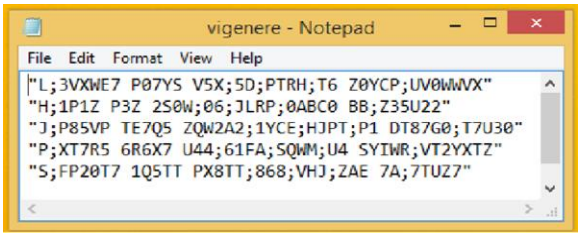

Figure 5. Vigenere encryption file

The deciphering is done by click on "Table Decryption" button. The first step the system allows the user input fields name. The second step the application processes Vigenere text file with Vigenere key file to produce Caesar cipher as shown above. Finally the programs produce plain database from the output as shown in Figure 6.

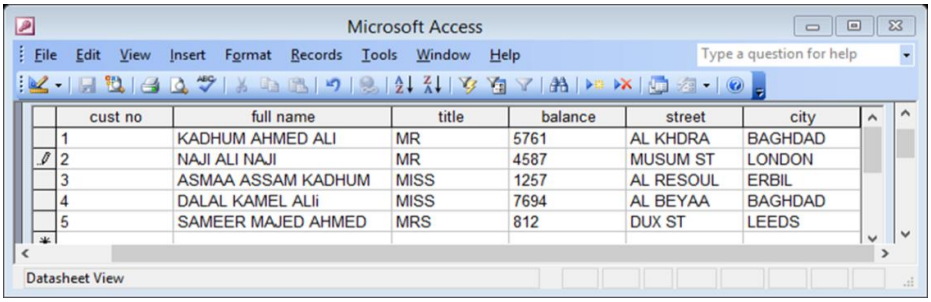

Figure 6. Plan table with fields name definition

In [19-20] the author use Caesar method with one key for each record, it means only 26 possibilities which make Caesar a very week code to break. In [7] use Affine method to produce cipher database. Affine cipher is a mono-alphabetic cipher, uses a mathematical function with two keys (a, b) for encryption, where each letter in the plaintext is substituted by a number [21-22]. The possible key combinations for Affine cipher are 12*26-1=311, Therefor an Affine cipher is highly insecure [23]. In addition the table loss has field's name as shown in Figure 7. The Vigenère Cipher was the biggest step in cryptography for over 1000 years. The idea of switching between cipher texts alphabets as you encrypt was evolutionary, and an idea that is still used to make ciphers more secure [24-25]. The current system achieves two powerful points in comparison with affine paper [7]; first the user can input the field name when the system creates the table as shown in Figure 6. Second the proposed system use Vigenere method which is more secure than Affine, and use modulo 35 instead of 26 which increase the probability to break encryption code.

Customer Table

F1	F 2	F 3	F 4	F 5	F 6
1	Kadhum Ahmed Ali	Mr	5000	Al Khdra	Baghdad
2	Naji Ali Naji	Mr	4500	Musum St	London
3	Asmaa Assam Kadhum	Miss	13000	Al Resoul	Erbil
4	Dalal Kamel Ali	Miss	7700	Al Beyaa	Baghdad
5	Sameer Mohammed Ahmed	Mrs	900	Dux St	Leeds

Figure 7. Table without fields name [7]

6. CONCLUSION

The system provides three levels of security. The first and second level use Caesar and Vigenere methods. Where the Caesar method is used different key lengths in each record, but the disadvantage each character in record has one cipher character. For this reason, the system has been strengthened with Vigenere method since each character has more than one cipher characters. The final level is converting table to text file.

REFERENCES

[1] Fernandez EB, Summers RC, Wood C, "Database Security and Integrity", Addison-Wesley, Massachusetts, 127, 1981.
[2] S. Mossayebi, "A Concrete Security Treatment of Symmetric Encryption in a Quantum Computing World" Ph.D. Thesis, University of London, 2015.
[3] W. Stalling, "Cryptography and Network Security Principles and Practices"; Printice Hill publishing, 792, 2005.
[4] A. Menezes, P. Van Oorschot, and S. Vanstons, "Handbook of Applied cryptography", CRC press 2001.
[5] William Friedman, "Cryptanalysis of the Vigenère Cipher: The Friedman Test", Chris Christensen, spring 2015.
[6] N. Snowdown, "Oracle Programming with Visual Basic"; SYBEX Inc,USA,495, 1998.
[7] Maitham A. Naji, Dalal A. Hammood; "Implementation and Enhancement Affine Cipher of Database", *Journal of Engineering Sustainable Development* Vol. 20, No. 4, P 264 – P 276, July 2016.
[8] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2017.
[9] W. Ch. Alisawi, Alaa Abdul AlMuhsen Hussian, Wasan A. Alawsi, Estimate Model of System Management for Database Security, *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, Volume 14, No. 3, 2019.
[10] Kevin Kusnardi, Dennis Gunawan, Guillou Qusiquater Protocol for User Authentication Based on Zero Knowledge, *Telecommunication Computing Electronics and Control*, Volume 17, No. 2, 2019.
[11] A. Amali Mary Bastina, N. Rama, Biometric Identification and Authentication Providence Using Fingerprint for Cloud Data Access, *International Journal of Electrical and Computer Engineering (IJECE)*, Volume 7, No. 1, 2017.
[12] Yen, J. C., & Guo, J. I., Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. IEE Proceedings-vision, image and signal processing, 167-175, 2000.
[13] Kaushik, Akhil, Satvika Khanna, Manoj Barnela, and Anant Kumar. "Stream Encryption Standard for Digital Images." International Journal of Computer and Electrical Engineering, no. 2, 240, (2011).
[14] W. De, Z. Yuan-Biao, "Image encryption algorithm based on S-boxes substitution and chaos random sequence", Conf. Comput. Model. Simulation, ICCMS 2009, pp. 110–113, 2009.
[15] X. Wang, Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos", Nonlinear Dyn., Vol. 75, No. 3, pp.567 -576, 2013.
[16] X. Zhang, Z. Zhao, J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer", Signal Process. Image Commun., Vol. 29, No. 8, pp. 902–913, 2014
[17] Y. Zhang, D. Xiao, "Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack", Nonlinear Dyn., Vol. 72, No. 4, pp. 751–756, 2013
[18] Elsharkawi, Abdelfattah, Ragab M. El-Sagheer, Haitham Akah, and Hatem Taha. "A Novel Image Stream Cipher Based On Dynamic Substitution." Engineering, Technology & Applied Science Research, no. 5, pp 1195-1199, 2016.
[19] M., A., Naji, "Implementation of Encryption Data Table by Using Multi-Keys" IJSCI, India Vol. 4 Issue 2, pp 14-17, 2014.
[20] M., A., Naji., "Implementation of Converting Text File to Data Access Table by Using Multi-Keys" IJSER, USA Vol. 4 Issue 12, pp 1090-1096, 2013.
[21] "A decent overview of the affine Cipher", http://www.math.sunysb.edu/~scott/Book331/Affine_enciphering.html
[22] "Cryptanalysis of the Affine Cipher", https://crypto.stackexchange.com/questions/50991/affine-cipher-cryptanalysis
[23] http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-affine-cipher/
[24] "Vigenere Cipher", https://crypto.interactive-maths.com/vigenegravere-cipher.html
[25] "Classical Cryptography, Vigenere Cipher", https://www.cs.uri.edu/cryptography/classicalvigenere.htm.