Data Base Protection Using Proposed Block Cipher Algorithm

By
Dr. Hilal Hadi
Dr .Ahmed Tariq
Dr.Alaa Kadim

In
2010

Science Computer, University of Technology

Abstract:

The Cryptography is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure and modification. The Cryptographic systems are classified into two cryptosystems, private-key cryptosystem and public-key cryptosystem. Both are based on complex mathematical algorithms and are controlled by keys.

Sensitive data that exist within organization's databases is attacked with some methods by unauthorized persons who use this data in illegal operation. Intrusion operations cannot be completely controlled, but they are possible to reduce them through data protection. In this paper, we proposed a block cipher algorithm for personal data protection by using in the same time a secrete key as a cipher key and password.

حماية قاعدة بيانات بأستخدام خوارزمية تشفير كتلي مقترحة

د.هلال هادي د.احمد طارق

د.علاء كاظم

الخلاصة:

إنّ علم التشفيرَ هوعلمُ ودراسةُ طرق حماية البياناتِ في الحاسبةِ وأنظمةِ الإتصال من الكشفِ الغير مخوّل والتّغيير. إنّ انظمة التشفير تُصنّفُ الى نظامين رئيسية انظمة التشفيرذات المفتاح السري و انظمة التشفيرذات المفتاح المعلن وكلا النظامين مستندة على خوارزمياتِ رّياضيةِ معقّدةِ ويُسيطرُ عليها بالمفاتيح.

ان البيانات الحساسة الموجودة في قاعدة بيانات المؤسسات والمنظمات تهاجم ببعض الطرق من خلال اشخاص غير مخولين والذين يستخدمون هذة البيانات في عمليات غير قانونية. عمليات التدخل لايمكن السيطرة عليها بشكل متكامل ولكن من الممكن الحد منها من خلال حماية البيانات . في هذا البحث اقترحنا خوارزمية التشفير الكتلي لحماية بيانات الاشخاص(العملاء) والتي تستخدم في نفس الوقت المفتاح السري كمفتاح تشفير وكلمة مرور.

Keywords: *Cryptography, Encryption, Decryption, Database, Security.*

1. Introduction

Information security deals with several different "trust" aspects of information. Information security is not confined to computer systems, or to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form. Information systems security can be defined as:

Information securities are the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations **[1,2]** .Information security is related to the need of keeping information from falling into the wrong hands. Failure to follow good security practices may lead to unauthorized uses of information, to fraud and to identity theft. In contrast, businesses collect and share information about people for a variety of appropriate reasons: improving service, decreasing costs, reducing fraud, and targeting offers of goods and services. **[3,4]**.

2. Databse Security

The protect access to an organization’s sensitive data and digital assets. A large majority of any organization’s electronic digital assets are stored in off-the-shelf relational database products. Businesses and government organizations use this database for personnel information such as employee payroll and medical records for which they have responsibility for privacy and confidentiality. Database holds sensitive financial data, past and future, including trading records, business transactions, and accounting data. Strategic or classified information such as proprietary technical and engineering

data - even marketing plans - must be guarded from competitors and unauthorized internal access. Database also includes detailed customer information including financial accounts, credit card numbers, and the trusted data of business partners. **[5,6]**

3. Information Security Threats

Bad things can happen to an organization's information or computer systems in many ways. Some of these bad things are done on purpose (maliciously) and others occur by accident. No matter why the event occurs, damage is done to the organization. Because of this, all of these threats are called "attacks" regardless of whether there is malicious intent or not. There are four primary categories of attacks:

- Access
- Modification
- Denial of service
- Repudiation

Attacks may occur through technical means (vulnerability in a computer system) or they may occur through social engineering. Social engineering is simply the use of non-technical means to gain unauthorized access for example, making phone calls or walking into a facility and pretending to be an employee. Social engineering attacks may be the most devastating Attacks against information in electronic form have another interesting characteristic: information can be copied but it is normally not stolen. In other words, an attacker may gain access to information, but the original owner of that information has not lost it. It just now resides in both the original owner's and the attacker's hands. This is not to say that damage is not done; however, it may be much harder to detect since the original owner is not deprived of the information. **[7, 8]**.

4. System platform

The platform is a foundation of the software solution and should be presented first. The core component will be indicted, piecing it all together in overall stage**.**

4.1 Registration Algorithm

In figure (1) show the major steps to registration

1. When the costumer wants to register in a system sends request to system administrator.
2. The administrator generate secret key(as password) and sent to login table used it to encryption and enter system
3. The costumer sends private data to data table in system ,the administer encrypt data by the proposed algorithm and put in there table

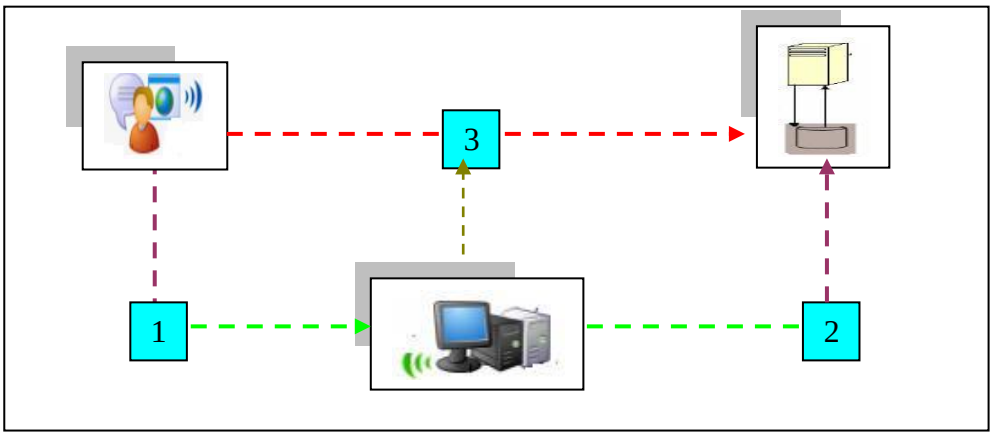


Figure (1) show the major steps to registration

4.1 Request Algorithm

In figure (2) show the major steps to request data:

1. The costumer enter system by security key (as password)
2. The administrator check password(as secrete key) in login table
3. Search private data for costumer in data table by secrete key and decrypt data by proposed block cipher and password method to display in clear to costumer

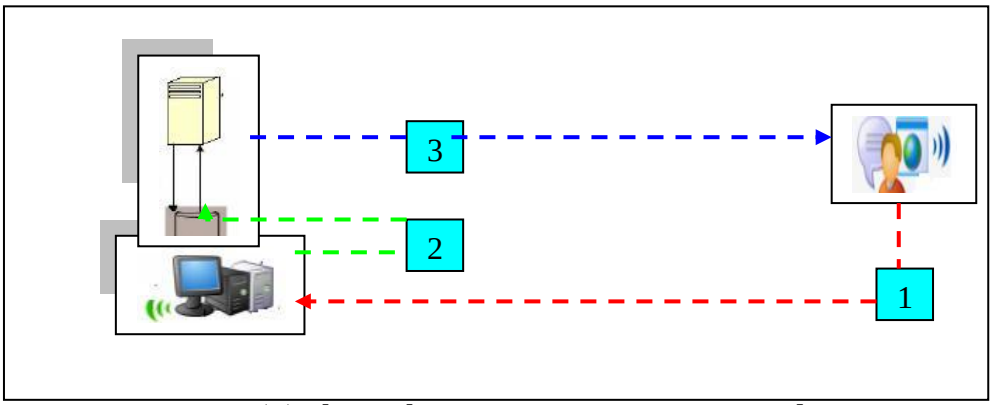


Figure (2) show the major steps to request data

4.3 Proposed Block Cipher Algorithm

Speed and complexity are two important properties in the block cipher. The block length of the block cipher controls these two aspects. In the same manner, the key complexity aspect acts as increasing the block length, which will cause increasing the complexity.

In this paper, a proposed block cipher algorithm will be presented. Which includes non-linear function(S-box) with new random key generators to generate all keys and a new approach for S-box are used in this algorithm.

On the other hand, the proposed algorithm is designed to work with blocks of data consisting of 256-bits with 256-bits key. It converts a block with 32-bytes (plaintext or cipher text) to square array of 16x16 bits length, and then splits this array to four 8x8 bits arrays.

In decryption, the key must be accomplished by using the same key that is used in encryption. A block to be enciphered is subject to an initial permutation ***IP***, then to a complex key-dependent computation and finally to an inverse permutation $\boldsymbol{IP}^{-1}$.

The proposed algorithm cipher system is designed in relation to the class of Feistel cipher algorithm with some added points which cannot be considered as a difference because the main concepts are used but the structure is changed to increase the computational complexity, the block diagram of the proposed block cipher is shown in figure (3).

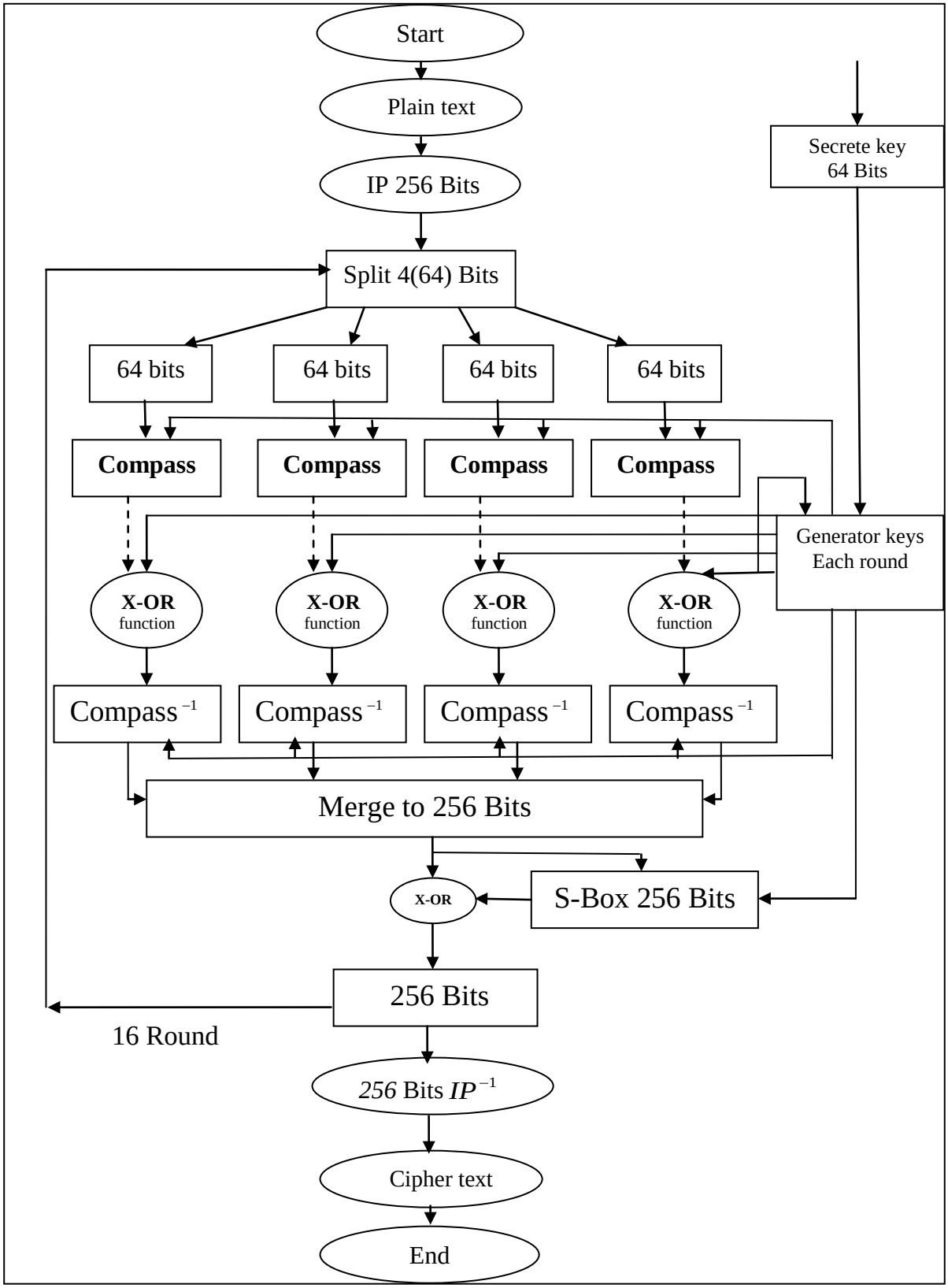


Figure (3) Block Diagram of Proposed Block Algorithm

Encryption Algorithm

INPUT:

M=m1...m256 (plain text)

K =k1...k256 (secret key)

OUTPUT:

C=c1...c256 (cipher text)

Begin

Generate master key as 256 bit from secret key using LFSR function, and given to generator function;

Use the IP permutation;

Split the plaintext into four arrays (64 bit), each of those 8x8 bits;

For i=1 **to** 16 **do**

Begin

Compute compass function for each part.

X-OR function with secret key for each part.

Compute Compass^{-1} function for each part.

Merge four parts to 256 bit.

Compute the S-Box function for output Merge.

X-OR output S-Box with merge.

End For

Use the IP^{-1} permutation.

End

Decryption is similar to the encryption algorithm, except the number round and keys order to compute the plaintext M.

4.3.1 Compass Function

This function is called compass function because it can replace a location of a bit from input depending on secret key.

Compass function receives 64(8x8) bit and returns 64(8x8) bit without any change in the size, the process of it cuts the first 4 bits from the input and if the first bit is 1, it replaces location 2 with location 4 depending on the secret key, otherwise those bits are stilling as they are. The same thing is done to the second four bits by replacing location 2 with 4 when the second bit is 1.This process is continued until the last 4 bit is reached.

4.3.2 S-BOX and S^{-1}-BOX Function

S-box function is a 256-bit input and output. The 256 bits input is ordered as 16x16 matrices. The sixteen rows are performed in the process to sixteen rows output.

4.4 The Proposed Algorithm versus DES

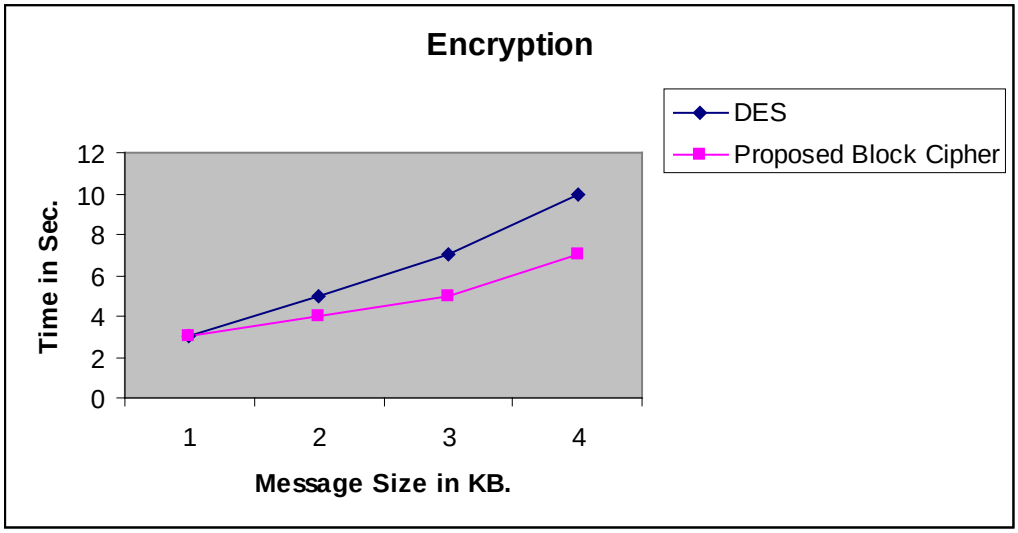
In this part, we will try to find out some aspects of evaluation concerning speed, complexity and resistance against know attack as a comparative study with DES block cipher system. The speed of the proposed algorithm and DES algorithm is un equivalent .The S-box function of DES is an 8-tick time consuming function because there are 8 s-boxes which work serially .In the proposed algorithm ,the s-box takes 1-tick time consuming function because there is 1 S-box which works in parallel-wise each of rows to calculate the output. This algorithm is programmed in Visual basic.Net on P4 with CPU 1.7G.B and RAM 512G.B.Then they are applied to massages that have different sizes. The plaintext of 1K is then taken and encrypted and the running time of its operation is computed. Then the 2K, 3K, and 4Kare taken and the running time of encryption and decryption of each message is calculated. The following table explains the running time in Sec.

Table (1) Total Time of the Proposed Block Cipher

Message Size	**Operation**	**DES In Sec**	**Proposed** In Sec
1K	Encryption	3	3
	Decryption	4	2
2K	Encryption	5	4
	Decryption	5	4
3K	Encryption	7	5
	Decryption	8	6
4K	Encryption	10	7
	Decryption	9	7

Curves are used to explain the differences in time .They have been illustrated in figures (4) and (5) below.

The complexity of any block cipher depends on key length or block length .unless there is a special attack to break through. In the DES, the length is appropriate key 56 bits so we need $(2^{64})^{16}$ trials to find the correct key for brute force attack. On the other hand, the complexity of the proposed algorithm is $(2^{256})^{16}$ because the key is 256 bits length.



Figure(4) Encryption Time

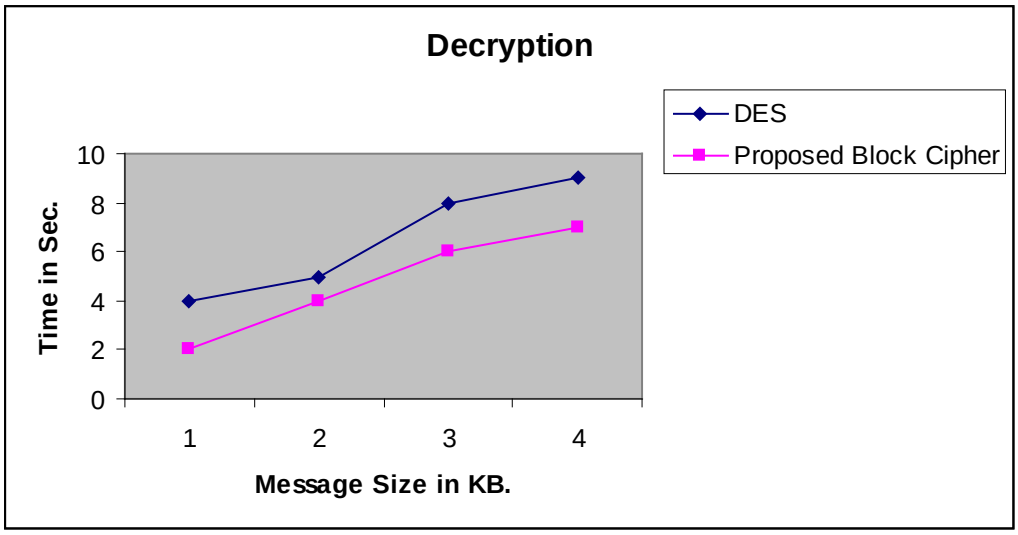


Figure (5) Decryption Time

5. System Implementation

When the proposed system is implemented in VB.NET, it has many pages that are used to access to clear data staring from the main page to last page

In executing the application, the user can enter to the system but must use the secrete key as password. When the user enters in a special place, the administrator checks in login table and enters to the next page to display data or exit when not found. Figure (6) and (7) shows the password.

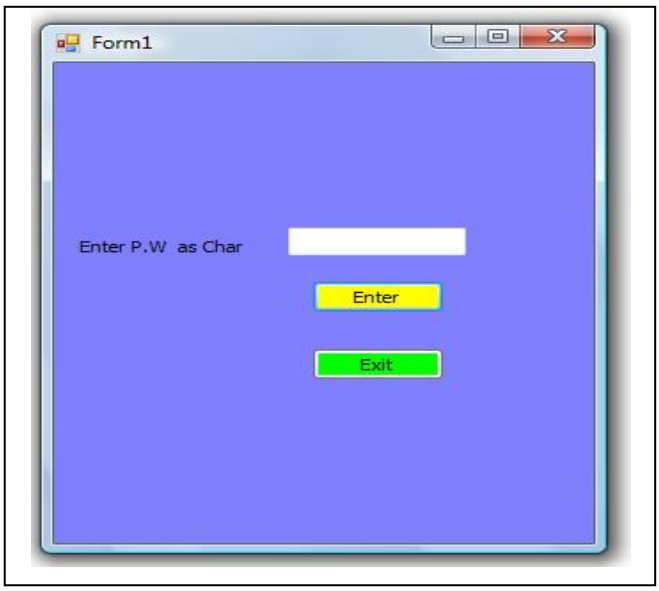


Figure (6) Main Page in Proposed System

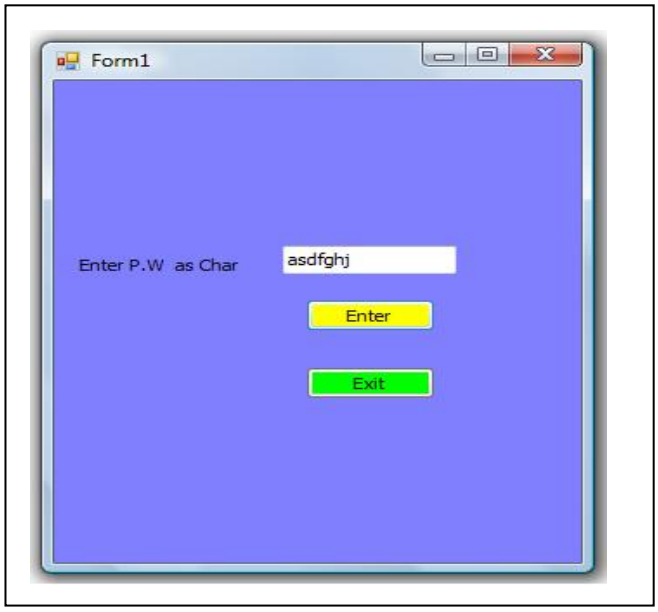


Figure (7) Enter to System by password

The display page displays the data for costumer, but the data is ciphered by the proposed block cipher .To display the data in clear the costumer must reenter the password as secret key, when the secret key (as password) is reentered, the system it is uses the same algorithm to decrypt data and display it clearly, .Figure (7) explains cipher and plain data.

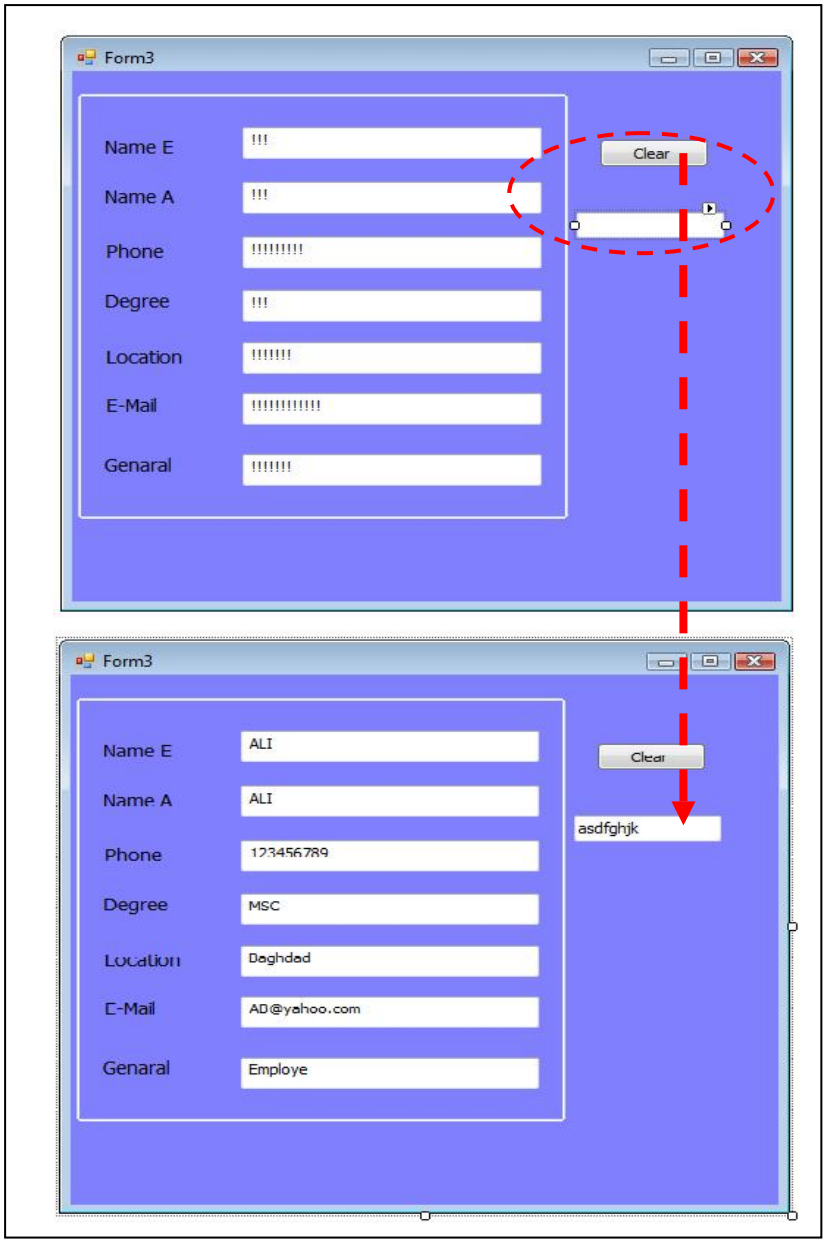


Figure (8) display data in clear

6. Conclusion

1. The attacker used multi ways to introducer the data in database by legal or illegal methods for introducer.
2. The proposed method is more complexity other methods, be cause of the length of cipher is longer than the original methods.

3. When programming application in modern language can use in multi environments and distribute.

References

1. Daniel, J., H. Kevin, and J. Andrew. "***Information Security: Why the Future Belongs to the Quants***." , IEEE Security and Privacy. IEEE, 24-32. 2003.

2. Wikipedia the Free Encyclopedia:***''Information Security Booklet''***, Federal Financial Institutions Examination Council, http://en.wikipedia.org/wiki/Information_security, *July 2006.*

3. Alaan W., "***Prepared Statement before the House Subcommittee on Commerce***",Trade and Consumer Protection, For a Good summary of these surveys, www.cdt.org/privacy/ccp/security1.shtml, May 8, 2001.

4. Paul, O., A. Annie, and B. David. "***The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information***." IEEE Security and Privacy. Piscataway, NJ, USA : IEEE Educational Activities Department, 15-23. 2007.

5. Gerald V. "**Data Base Management System**", second edition, McGraw Hill Companies, 2002.

6. Sudarshan S ,"**Data Base System Concept**" ,third edition ",McGraw Hill,1998.

7. Richard C., "***Why is Information Security Important***", Keynote Address to the Federal Trade Commission, http://www.cdt.org/privacy/ccp/security1.shtml, May 20, 2002.

8. Wegman M. and Carter L., " ***New Hash Functions and Their Use in Authentication and Set Equality***, . Journal of Computer and System Sciences, 22(3):265–279, Jun 1981.