Eng. & Tech. Journal, Vol. 29, No. 6, 2011

# Proposal to Complex DES Security Using Diffie Hellman Injection

**Shatha habeeb Jafar***

Received on: 2/1/2011
Accepted on: 7/4/2011

**Abstract**

Data Encryption Standard (DES**)** is based on a round of starters, from the results of the use of multi-stage permutation and replacement to the more complex algorithm which adopts the symmetric key. Diffie- Hellman is based key generation algorithm puts a shared secret key between two parties A and B, which depends on the prime number.

This research suggest a technique it is objective is the blending between the two encryption methods DES and Diffie Hellman to make DES more safe and secure. That by propose two options first one include injection the encryption DES after the seventh round with Diffie-Hellman just as key distribution algorithm then the results of the last back to the eighth round to complete the encryption process of DES. The second include injection the encryption DES after the eighth round with Diffie-Hellman just as key distribution algorithm to generate key the results of the eighth round will be encrypted using stream cipher then back to the ninth round to complete the encryption process of DES.

**Keywords**: - DES, Diffie-Hellman, Cipher, Encryption, Key exchange.

## أقتراح تعقيد أمنية DES باستخدام دافي هلمن

**الخلاصة**

يعتمد تشفير البيانات الموحدة (DES) على الدورات باستخدام التقليب متعددة المراحل التي تعتمد على المفتاح المتماثل و DH التي تعتمد على توليد مفتاح سري مشترك بين طرفين A,B والذي يعتمد على عدد اولي.

يشير هذا البحث الى تقنية الهدف منها هو المزج بين طريقتين التشفير DES وDH لجعل DES أكثر آمنة وموثوقة. ذلك من خلال اقتراح خيارين الأول يعتمد على ادخال DH على مفتاح DES بعد االدورة السابعة في الدورة الثامنة والعودة لإكمال عملية تشفير DES. والثانية تشمل الحقن التشفير DES بعد الدورة الثامنة مع DH لتوليد مفتاح وتشفير نتائج الدورة الثامنة باستخدام طريقة تشفير ثم العودة إلى الدورة التاسعة لإكمال عملية تشفير DES.

## 1- Introduction

The data encryption standard (DES) is the most widely used symmetric cipher, the use multiple stage of permutation and substitution results in more complex algorithm, which increases the difficult of cryptanalysis. DES algorithm [1,2,3 and 4], see figure (1):

Step 1: Create 16 subkeys, each of which is 48-bits long.

Step 2: Encode each 64-bit block of data.

The DES encryption algorithm involves five functions:

1. An initial permutation (IP).

* **Computer Science Department, University of Technology, Baghdad**



https://doi.org/10.30684/ etj.29.6.15
University of Technology-Iraq, Baghdad, Iraq/2412-0758
This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0

2. A complex function called $f_k$, which involves both permutation and substitution operations and depends on a key input.
3. A simple permutation function that switches (SW) the two halves of the data .
4. The function $f_k$ again.
5. A permutation function that is the inverse of the initial permutation ($IP^{-1}$).

Diffie-Hellman key exchange offers the best of both worlds -- it uses public key techniques to allow the exchange of a private encryption key. Let's take a look at how the protocol works, from the perspective of Alice and Bob, two users who wish to establish secure communications. We can assume that Alice and Bob know nothing about each other but are in contact. With Diffie-Hellman Key Exchange here

Are the nine steps of the process, [5, 6, 7, 8 and 9], see figure (2):

1. Communicating in the clear, Alice and Bob agree on two large positive integers, $q$ and $g$, with the stipulation that $n$ is a prime number and $g$ is a generator of $q$.
2. Alice randomly chooses another large positive integer, $X_A$, which is smaller than $q$. $X_A$ will serve as Alice's private key.
3. Bob similarly chooses his own private key, $X_B$.
4. Alice computes her public key, $Y_A$, using the formula $Y_A = (g \wedge X_A) \bmod q$.
5. Bob similarly computes his public key, $Y_B$, using the formula $Y_B = (g \wedge X_B) \bmod q$.
6. Alice and Bob exchange public keys over the insecure circuit.
7. Alice computes the shared secret key, $k$, using the formula $k = (Y_B \wedge X_A) \bmod q$.
8. Bob computes the same shared secret key, $k$, using the formula $k = (Y_A \wedge X_B) \bmod q$.
9. Alice and Bob communicate using the symmetric algorithm of their choice and the shared secret key, $k$, which was never transmitted over the insecure circuit.

## 2- The Proposal System Design

The proposed system suggests two options to strength the DES algorithm these options will be explained in the following sections:

### 2-1 First Option

The first option to strength the DES encryption algorithm will divide the DES algorithm into three parts, see figure (3):

1. The first part consist the first seven iterations only, work just like traditional DES.
2. The second part consist the eighth iteration only but instead of using the traditional eighth subkey it will used a proposed alternate key extracted by Diffie-Hellman algorithm.
3. The third part consist the last eighth iterations, work just like traditional DES.

### 2-2 Second Option

The second option to strength the DES encryption algorithm will also divide the DES algorithm into three parts, see figure (4):

1. The first part consist the first eighth iterations only, work just like traditional DES.
2. The second part consist of taking the result of the eighth iteration and then encrypt it using stream cipher algorithm with key also obtained by Diffe-Hellman algorithm.
3. The third part consist the last eighth iterations, work just like traditional DES.

## 3- The Implementation of the Proposal System

The implementation of the proposal done by using VBv6, as mentioned in previous sections, the proposal aim to strength the DES algorithm using Diffie-Hellman (DH) algorithm, figure (5) display the DH algorithm for symmetric key generation and figure (6) display the DES algorithm which the proposal aim to strength it.

The implementation of the first proposal displayed in figure (7), where it presented in one form this form consists of three buttons, first one to the left will run the seventh iterations in DES, then the second button run the DH to generate the key of the eighth iteration in DES. Finally the button in the right side complete the eighth iterations.

The implementation of the second proposal displayed in figure (8), where it presented in one form this form consists of three buttons, first one to the left will run the eighth iterations in DES, then the second button run the DH to generate the key of the traditional stream cipher to encrypt the result of the eighth iteration in DES. Finally the button in the right side take the final result and complete the eighth iterations.

## 4- Conclusions

This research suggest a technique it is objective is the blending between the two encryption methods DES and Diffie Hellman to make DES more safe and secure. That by propose two options. And from that we conclude the following points:

1. The encryption of DES has some thing danger, that it is an algorithm depend on symmetric key, so if the key is discovered that will destroy the DES security.
2. DH just generate symmetric key need an encryption algorithm to be useful.
3. Using DH with DES make some level of DES encryption online.

Both of proposal make the DES more secure since it is security depend on more just it is symmetric key.

## References

**[1]-** S.Siva Sathya, T.Chithralekha and P.AnandaKumar, **"Nomadic Genetic Algorithm for Cryptanalysis of DES 16",** International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, 2010.

**[2]-** Seung-Jo Han, Heang-Soo Oh, Jongan Park, **"The improved Data Encryption Standard (DES) Algorithm",**E-mail : han7069@nown~1ri.nowcom.co.kr , 2006.

**[3]-**Limor Elbaz & Hagai Bar-El," **Strength Assessment Of Encryption Algorithms"** Discretix Technologies Ltd. Email: {limor.elbaz, hagai.bar-el}@discretix.com Tel: +972-9-8858810 www.discretix.com **,White Paper** October 2000.

**[4]** –Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, **"Data Encryption Standard (DES)**", Gaithersburg, MD (1999).

[5]- Rongxing Lu¤y, Xiaodong Linz, Zhenfu Caoy, Liuquang Qiny, and Xiaohui Liangy,"**A simple deniable authentication protocol based on the Diffie-Hellman algorithm**", International Journal of Computer Mathematics Vol. 00, No. 00, August 2007.

[6]- Rescorla, E., "**Diffie-Hellman Key Agreement Method**", RFC

2631, IETF Network Working Group, http://www.ietf.org/rfc/rfc2631.txt ,2006.

[7]- RSA Laboratories,"**FAQ About Today's Cryptography**, http://www.rsa.com/rsalabs/faq/index.html , Version 4.1, RSA Security Inc., 2000

[8]- Costas Christoyannis, "**What is Diffie-Hellman**", http://www.hack.gr/users/dij/crypto/overview /diffie.html ,2006.

[9]- Levy, Benjamin, "**Diffie-Hellman Method for Key Agreement**", http://apocalypse. org/pub/u/seven/diffie.html ,2006.

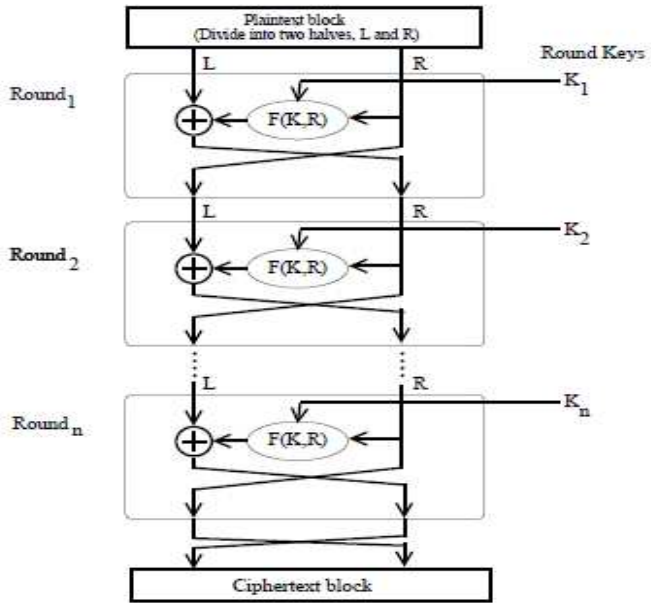


**Figure (1): DES Algorithm**

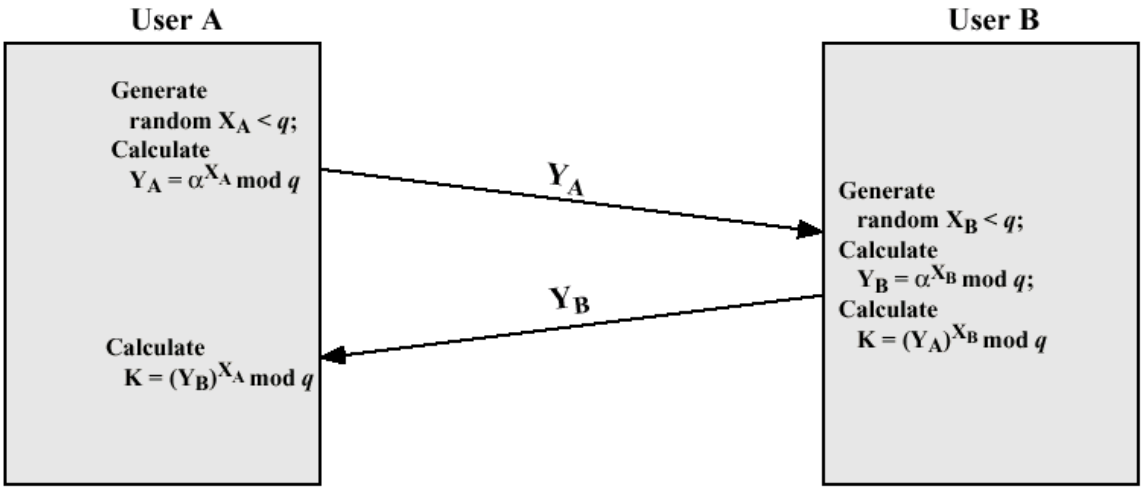


**Figure (2): Diffie-Hellman diagram**

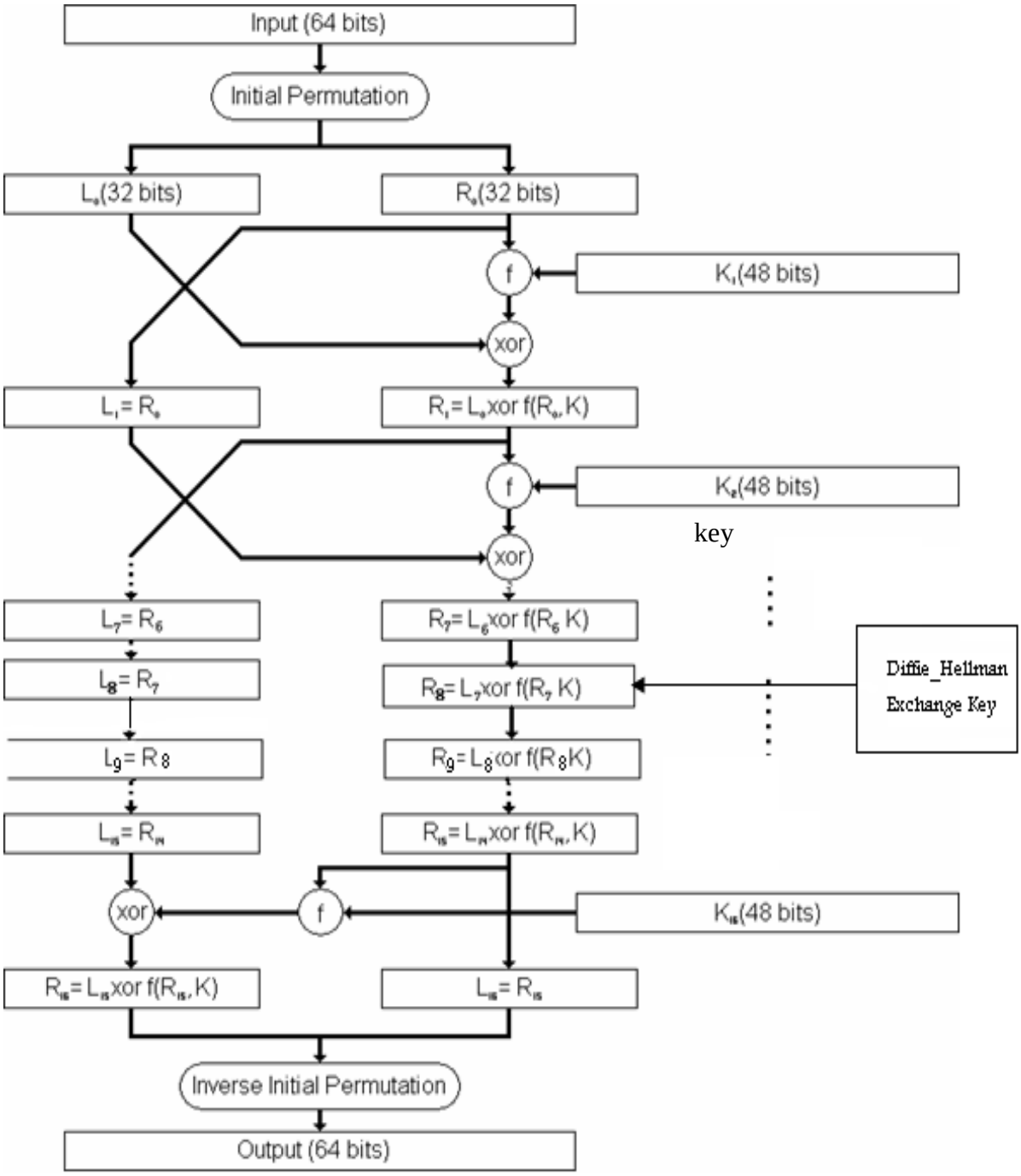


**Figure (3): The first option to strength DES**

***Will describe the first option in the sender side***

***Algorithm(1)***

| ***Input : plaint text and key DES with DH*** |
|---|
| ***Output : encrypt text*** |
| ***Process***<br>***Begin***<br>***Step one:*** the sender and receiver must be both on line<br>***Step two:*** both of them receive the encryption key from third party certification<br>***Step three:*** the sender encrypt the plaintext by only the first seven iterations.<br>***Step four:*** notify the receiver that the time for online Diffe-Hellman key distribution.<br>***Step five:*** apply the DH algorithm and both of them have the same key.<br>***Step six:*** return to DES algorithm and continue to encryption with the eighth iteration using the DH key instead of the traditional eighth subkey which will be omitted.<br>***Step seven:*** take the resulted encryption and entered it to the last eighth iteration as in traditional.<br>***Step eighth:*** send the encrypted text to the receiver.<br>End |

***Will describe the first option in the receiver side***

***Algorithm(2)***

| ***Input : ciphertext and key DES with DH*** |
|---|
| ***Output :plaintext*** |
| ***Process***<br>***Begin***<br>***Step one:*** the sender and receiver must be both on line<br>***Step two:*** both of them receive the encryption key from third party certification<br>***Step three:*** the receiver decrypt the ciphertext by only the last eighth iterations.<br>***Step four:*** the receiver already was notified by the sender in the time for online Diffe-Hellman key distribution. And they apply the DH algorithm and both of them have the same key.<br>***Step six:*** return to DES algorithm and continue to decrypt with the eighth iteration using the DH key instead of the traditional eighth subkey which will be omitted.<br>***Step seven:*** take the resulted decryption and entered it to the first seven iteration as in traditional.<br>***Step eighth:*** read the decrypted text.<br>End |

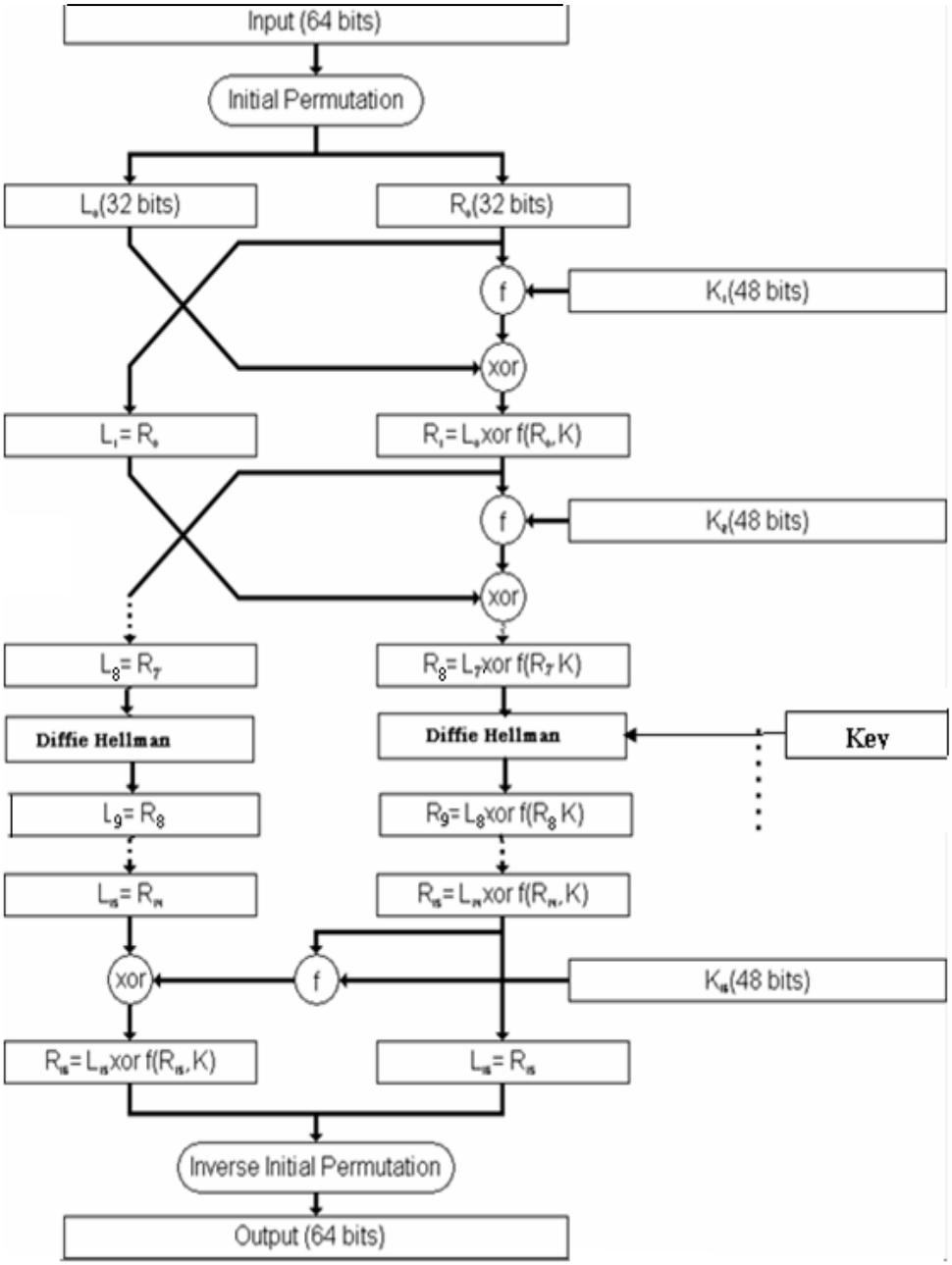


**Figure (4): the second option to strength DES**

***Will describe the second option in the sender side***

***Algorithm(3)***

| ***Input : plaintext and key DES with DH*** |
|---|
| ***Output :ciphertext*** |
| ***Process*** <br> ***Begin*** <br> ***Step one:*** the sender and receiver must be both on line <br> ***Step two:*** both of them receive the encryption key from third party certification <br> ***Step three:*** the sender encrypt the plaintext by only the first eighth iterations. <br> ***Step four:*** notify the receiver that the time for online Diffe-Hellman key distribution. <br> ***Step five:*** apply the DH algorithm and both of them have the same key. <br> ***Step six:*** return to DES algorithm and take the result of encryption from the eighth iteration and encrypt it with the stream cipher using the DH key. <br> ***Step seven:*** take the resulted encryption and entered it to the last eighth iteration as in traditional. <br> ***Step eighth:*** send the encrypted text to the receiver. |

***Will describe the second option in the receiver side***

***Algorithm(4)***

| ***Input : ciphertext and key DES with DH*** |
|---|
| ***Output :plaintext*** |
| ***Process*** <br> ***Begin*** <br> ***Step one:*** the sender and receiver must be both on line <br> ***Step two:*** both of them receive the encryption key from third party certification <br> ***Step three:*** the receiver decrypt the ciphertext by only the last eighth iterations. <br> ***Step four:*** the receiver already was notified by the sender in the time for online Diffe-Hellman key distribution. And they apply the DH algorithm and both of them have the same key. <br> ***Step six:*** return to DES algorithm and take the result of decryption after the last eighth iteration and decrypt it with same stream cipher using the DH key. <br> ***Step seven:*** take the resulted decryption and entered it to the first eighth iteration as in traditional. <br> ***Step eighth:*** read the decrypted text. <br> End |

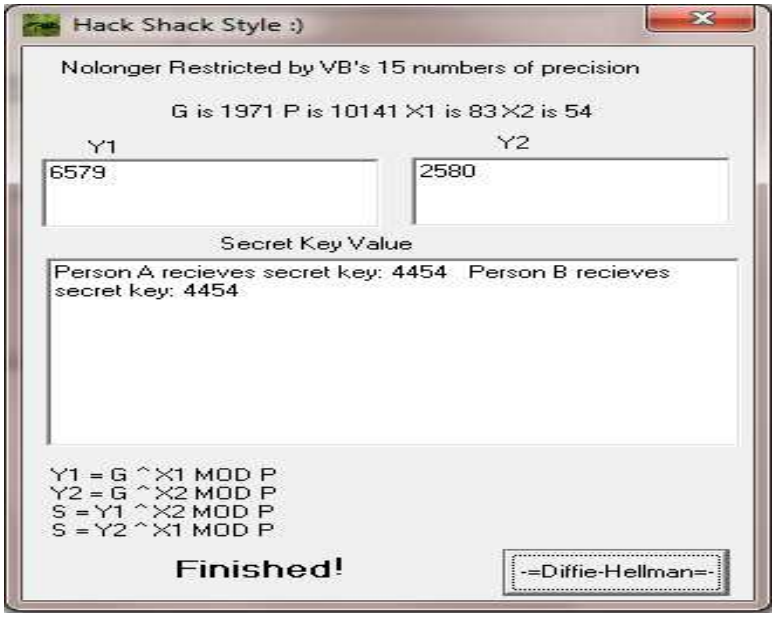


**Figure (5): DH algorithm.**

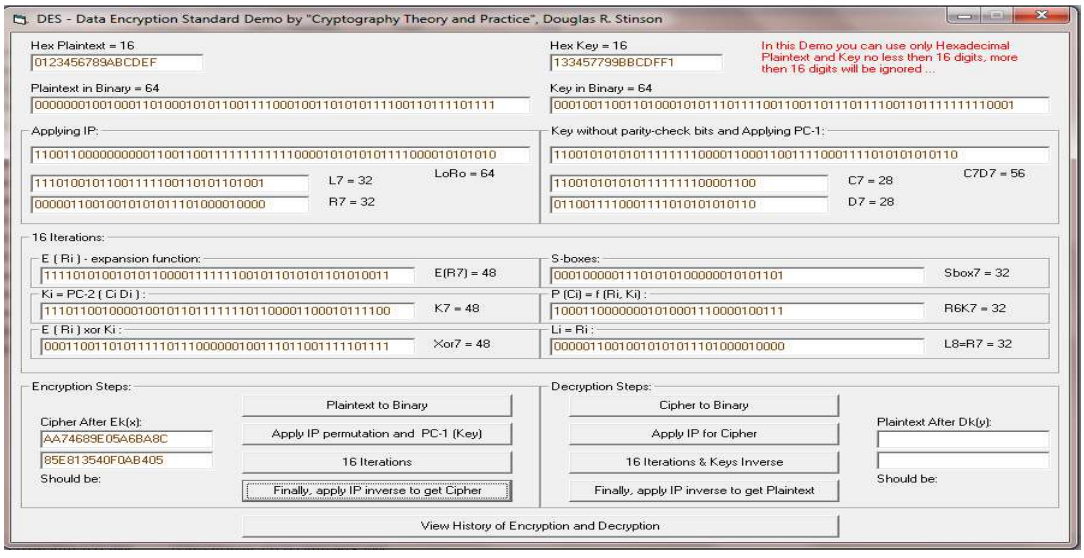


**Figure (6): DES algorithm.**

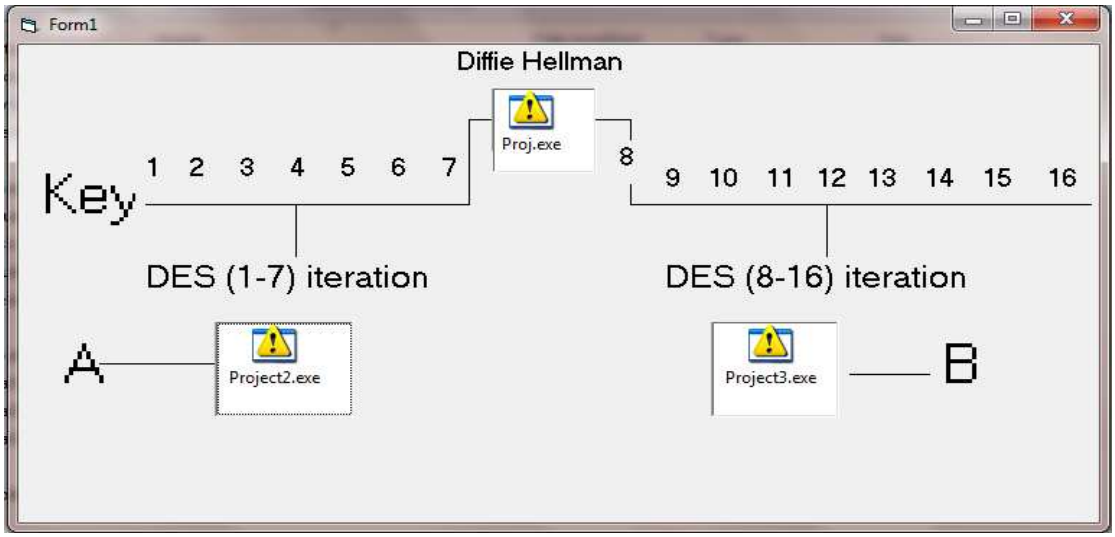


**Figure (7): The implementation of the first options.**

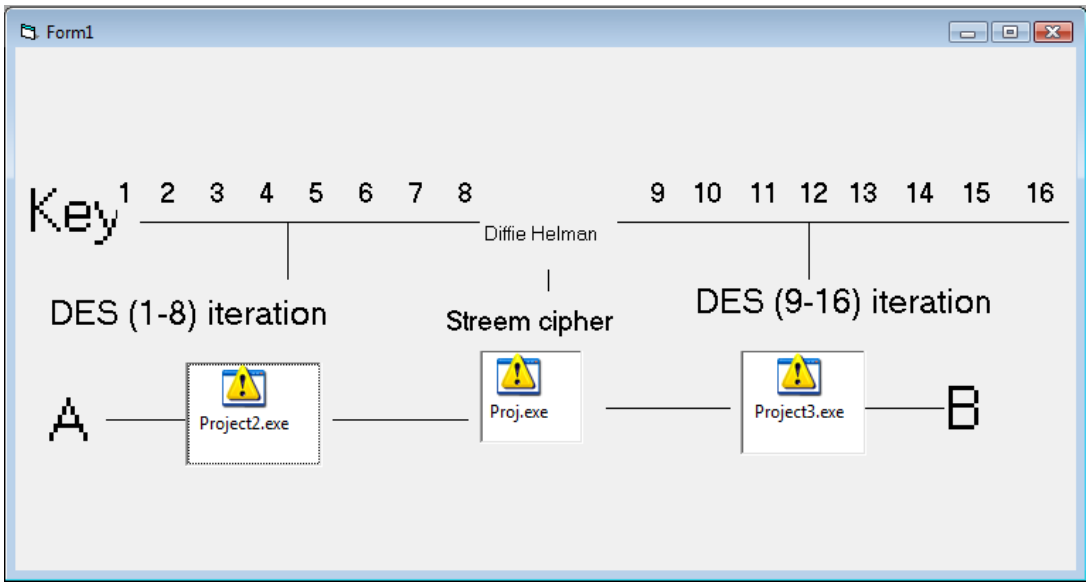


**Figure (8): The implementation of the second options.**