A SIMPLIFIED 48-BIT KEY GENERATION SCHEME FOR DMDC

Mylene J. Domingo[1], Bobby D. Gerardo[2]
[1]Technological Institute of the Philippines
[1]Quezon City, Philippines
[1]mgj16@yahoo.com/mjdomingo@ust-ics.mygbiz.com
[2]Institute of Information and Communications Technology
[2]West Visayas State University
[2]Lapaz, Iloilo City, Philippines
[2]bgerardo@wvsu.edu.ph

ABSTRACT

Information security is a challenge today. Protecting information from availability, privacy and integrity has become a very hard task. Because of the existence of very good crackers, there is a demand in providing a stronger encryption technique. Many of the information stored are highly confidential. Because of its confidentiality, researchers tried to develop various encryption algorithms. One of these algorithms is the DES which is used as an encryption technique for the hash function DMDC. On this paper, I have developed a new key generation scheme with the use of 48 bits conversion from 64 bit input. I have introduced a new table in converting given bit to 48 bits by dropping the 1st and the 8th bit. Shifting operation will also be employ.

General Terms: *Algorithm, Security*

Keywords: *Information security, Encryption, Decryption, Cryptography*

INTRODUCTION

Security on information is a very important aspect of our society, from personal, home, academe, business or enterprise [1]. Transmitting data over the network using either physical cables or wireless communication are not protected by intruder. Data transmitted over the unsecured network is susceptible for eavesdropping, illegal activities such as illegal retrieval and modification [2]. In view of this, we must use efficient techniques in securing data transmitted over the network.

Cryptography is field of study where secret messages are securely transmitted form one party to another. To do this, the system needs to receive an original text or message which is known as a plaintext. This plaintext needs to be encrypted which is known as cipher text before sending to the intended recipient. On the other hand, the recipient needs to decrypts the text to read the original message.

Cryptography is considered not only a part of the branch of mathematics, but also a branch of computer science [3]. There are three main forms of cryptosystems: Symmetric Encryption System, Asymmetric Encryption System and Hash Functions [4].

There are so many symmetric block ciphers available: Data Encryption Standard (DES), Triple DES, and International Data Encryption Algorithm (IDEA), RC5, RC6, and AES algorithm [5].

Numerous studies are conducted on Asymmetric encryption. Asymmetric encryption uses a same key pair for public key and private key. According to Sison et al [6], both the private and public key are managed by the sender and the receiver. With this anyone may convert the clear text to cipher text(encryption process) a message for A using his public key but only A can decrypt (conversion of cipher text to clear text) the message using his secret key and only A can encrypt the message that will decrypt with A's public key. On the other hand, a symmetric encryption uses only one symmetric key (e.g. series of numbers and letters) and some shifting of characters (bits) to alter the message. The same key is use for both encryption and decryption so the symmetric key must be known for both sender and the receiver.

Every algorithm has merits and demerits and thus being not sufficient to answer the security of information. Through the years researchers are trying to create a better solution which will remove the demerits of each algorithm. In this paper a simplified 48 key generation scheme for DMDC, which is a Hash Function with the use of DES under Symmetric Encryption System, will be developed.

According to [7], in cryptography and information security, hash functions are considered as the "Swiss army knife". They are used in countless protocols and algorithms. Hash functions accept a variable-sized message as input and output a small fixed-sized string. Message authentication is the major use or function of the hash function and the security depends on the cryptographic strength of the hash function. Message authentication is a procedure to verify that received messages come from the alleged source and have not been altered [8].

REVIEW OF RELATED LITERATURE

The Data Encryption Standard (DES) is a block cipher involving 64-bit data encryption with 56-bit key, which was adopted by the U.S. National Institute of Standards and Technology in 1976[9] DES is a symmetric key algorithm that uses the same key for encryption and decryption. DES encryption algorithm was proposed in the year 1977. It encrypts 64 bits blocks with a 56 bit key. It uses 16 rounds of iteration; each round uses swapping, permutation, substitution and XOR operations [5].

DMDC is a hash function that takes the input of arbitrary length and then output it to a fixed length of code such as 18, 32, 64 or 128 bits. Message digests are used to ensure the integrity of data. This can be achieved by breaking the given input to a sequence of fixed equal size of blocks using DES [5]

Message Digest is used for many applications. A related application is what we called password verification. Plain text scoring of password can result in massive security breach if someone will be able to access the database. Employing hash digest to each password may be used to reduce this danger. In authenticating the identity of the person accessing the system, the hash code will be compared to the stored hash. In case the user forgot his/her password, there will be no way to generate the same password but instead the user will be given another code. The code is usually generated by putting or concatenating with other characters before the actual hashing process.

PROPOSED KEY GENERATION SCHEME OF DMDC

DMDC hash function

According to [5] DMDC algorithms key generation scheme makes use of 64 bit input to Permutted Choice 1 (PC-1) to produce 56 bits. Will perform shifting on the left and on the right groupings of bit, then the output will be used as an input to Permutted Choice 2 (PC-2) table to form 48 bits that will be used in the computation of the message digest.

In this section, a simplified key generation scheme will be discussed.

Enhanced key generation scheme

- The proposed key generation scheme requires 64-bit input. This will be converted in binary to input in the Table1 64 bit values.
- Drop the first bit and eight bit of the given 64-bit.
- Last bit will be use as parity bit and the first bit will be saved in a temporary register.
- Create a table that will accept the 48-bit key after dropping the first and last bit. Input to the Modified Permutted Choice (modified PC-1)
- Use shifting function to provide additional security.
- Input values in the row/column wise permutation.

TABLE 1: Comparison of the Present DMDC with the Proposed DMDC

Present DMDC	Proposed DMDC
Use Table2: Existing PC-1 (56 bits)	Use Table4: Modified-PC1(48 bits)
Divide the 56 bits into 2 groups	Divide the 48 bits into 2 groups
Perform shifting once on each group	Perform shifting once on each group
Concatenate two groups	Concatenate two groups
Use Table3 Permutted Choice (PC-2) 48 bits	48 bit will then be input in Table5 Row wise permutation or Table6 Column wise permutation (these will be the value for K
48 bit will then be input in Table5 Row wise permutation or Table6 Column wise permutation (these will be the value for K	

Table 1 shows the comparison of the key generation scheme of the present key generation scheme of the present DMDC to the proposed DMDC. The table shows that instead of using two tables in converting 64 bits to 48 bits, the proposed scheme will only use one table for the conversion.

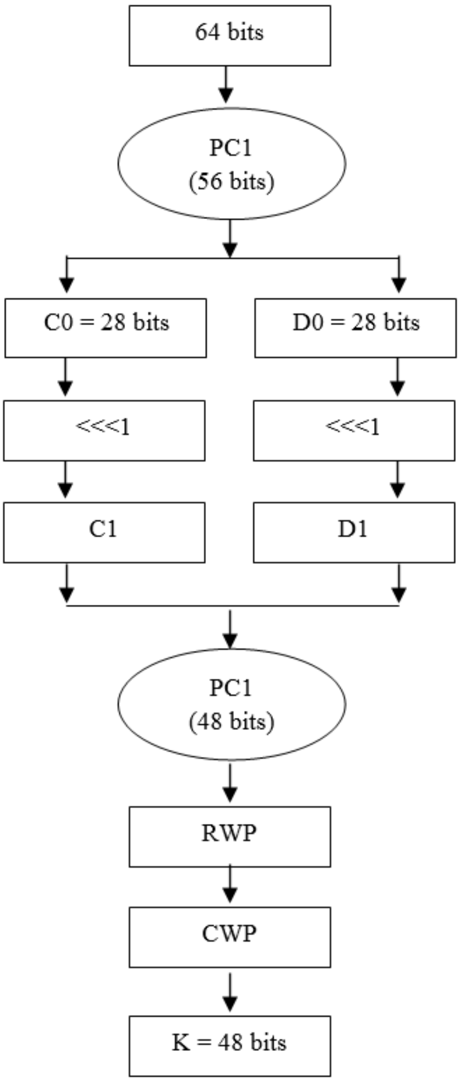


Figure 1: Existing Key Generation Scheme

Figure 1 shows the steps in 48-bit key generation using existing scheme. The 64-bit input key is initially reduced to 56-bit by ignoring every eight bit using Table2 Permutted Choice (PC-1).

After the 56-bit key was extracted, they are divided into 28-bit halves and loaded into two working registers (C0 and D0)

The halves in registers are shifted one or two depending on the number of rounds (C1 and D1)

After bit shifting, 56-bit input will be used as input in Table3 Permutted Choice 2 (PC-2) which produces the 48 bit key output.

Finally the 48-bit key output will be inputted in the Table5 Row wise permutation and Table6 Column wise permutation thus resulting to the K as the output in the key generation scheme.

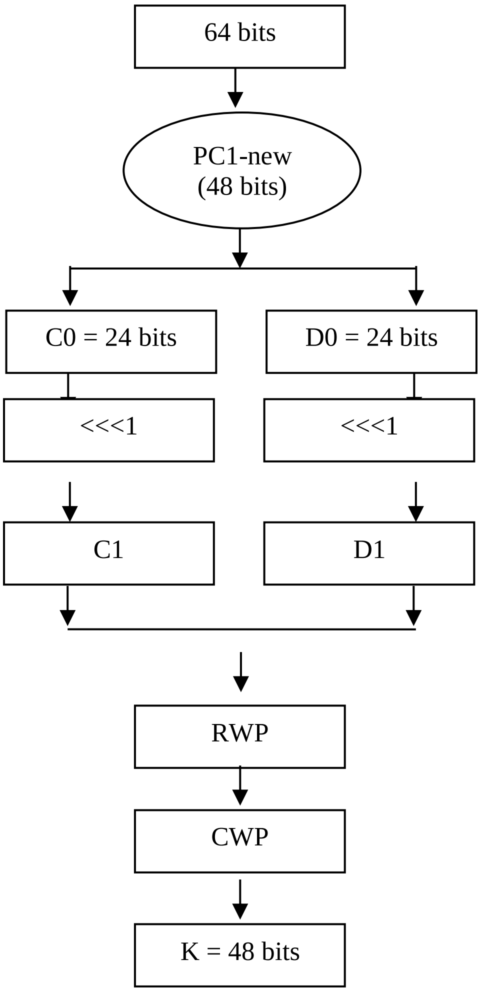


Figure 2: Proposed Key Generation Scheme

Steps in 48-bit key generation using propose scheme as depicted in Figure 2 are as follows:

The 64-bit input plaintext is reduced by dropping the first and eight bit using modified PC-1 table. The eight bit will be used as a parity bit while the first bit is saved in a temporary register

After the 48-bits are extracted, they are divided into 24-bit halves and loaded into two working registers.

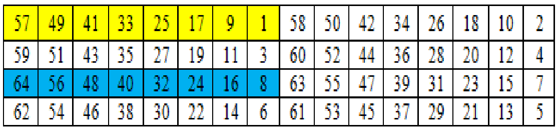
The halves in registers are shifted once.

The two halves is combined.

Finally the 48-bit key output will be inputted in the Table5 Row wise permutation and Table6 Column wise permutation thus resulting to the K as the output in the key generation scheme.

SIMULATION AND TESTING RESULTS

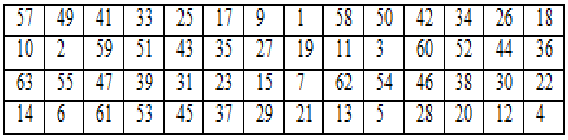
Table 1: 64-bit values



57	49	41	33	25	17	9	1	58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3	60	52	44	36	28	20	12	4
64	56	48	40	32	24	16	8	63	55	47	39	31	23	15	7
62	54	46	38	30	22	14	6	61	53	45	37	29	21	13	5

Table 1 shows the 64-bit input before dropping the first (with yellow color) and eight bit (with blue color)

Table 2: Existing Permutted Choice 1 (PC-1)



57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Table 2 shows the Permutted Choice 1 (PC-1) after dropping the eight bit, from 64-bit input to 56-bit output [5]

Table 3: Permutted Choice 2 (PC-2)

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Table 3 shows the Permutted Choice 2 (PC-2), converting 56 bits to 48 bits [5].

Table 4: Modified Permutted Choice 1 (PC-1)

58	50	42	34	26	18	10	2	59	51	43	35
27	19	11	3	60	52	44	36	28	20	12	4
63	55	47	39	31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37	29	21	13	5

Table 4 shows the Modified Permutted Choice 1 (PC-1) that directly convert the 64-bit input to 48 bits by dropping the every first and eight bit as also shown in Table1.

Table 5: Row wise permutation

5	11	17	23	29	35	41	47
1	7	13	19	25	31	37	43
3	9	15	21	27	33	39	45
6	12	18	24	30	46	42	48
2	8	14	20	26	32	38	44
4	10	16	22	28	34	40	46

Table 5 shows the Row wise permutation that will be use after the shifting operation.

Table 6: Column wise permutation

11	35	5	47	17	41	29	23
7	31	1	43	13	37	25	19
9	33	3	45	15	39	27	21
12	46	6	48	18	42	30	24
8	32	2	44	14	38	26	20
10	34	4	46	16	40	28	22

Table 6 shows the Column wise permutation that will be use after the shifting operation.

Illustrative Example:

Let the input plaintext

M = 5f18ac31a84eac45

Table 7: Conversion of input(M) to its binary equivalent.

Given Key	Binary Equivalent	Index
5	0101	4
F	1111	8
1	0001	12
8	1000	16
A	1010	20
C	1100	24
3	0011	28
1	0001	32
A	1010	36
8	1000	40
4	0100	44
E	1110	48
A	1010	52
C	1100	56
4	0100	60
5	0101	64

Using result in the above conversion, binary will be input in the modified permuted choice (PC-1)

Table 8: Permutted Choice 1 (PC-1) result

1	0	1	0	0	0	0	1	0	1	0	1
1	1	0	0	0	0	0	0	1	0	1	1
0	0	1	0	0	0	0	1	1	1	1	0
0	1	0	1	0	1	1	1	0	1	1	1

C0 = A15C0B   D0 = 21E577

Table 9: Result after Shifting

0	1	0	0	0	0	1	0	1	0	1	1
1	0	0	0	0	0	0	1	0	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0
1	0	1	0	1	1	1	0	1	1	1	0

C1 = 42B817   D1 = 43CAEE

Combine C1 and D1 to get K

K = 42B81743CAEE

Table 10: RWP/CWP output

0	1	0	1	0	0	1	1
0	1	1	0	0	1	1	1
0	1	0	0	0	1	1	1
0	1	0	1	0	1	1	0
1	0	0	1	1	1	0	0
0	0	0	1	0	1	0	1

Final Result of key generation scheme for

K = 536747569C15

CONCLUSION AND RECOMMENDATION

Information transmitted over the network is rapidly increasing. Securing information transmitted over the network is vulnerable to attacks by different intruders like hackers. We should develop different techniques on how to safeguard information against these attacks.

The simplified 48-bit key generation scheme is just another way of illustrating decryption process in DMDC. It involves modifications of table in order to obtain the equivalent 48-bit decrypted text from 64-bit plaintext. This would be a new algorithm that can be used for the hashing technique.

In comparing the existing key generation of DMDC to the proposed key generation scheme, converting 56-bit key to 48-bit key using PC-2 table is eliminated and PC-1 table is modified. But will provide the same security as compare with the existing scheme. The modified scheme can be used as a reference for other researcher to explore and create a better encryption technique that will only deal with lesser tables and conversion.

REFERENCES

[1] P. Rakers, L. Connell, T. Collins, D. Russel, “Secure Contactless Smartcard ASIC with DPA Protection”, IEEE 2000 Custom Integrated Circuits Conference.

[2] S. Han, H. Oh, P. Jongan, “The improved Data Encryption Standard (DES) Algorithm” 1999”

[3] S. Bhati, A. Bhati, S.K. Sharma, “A New Approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm” 2012

[4] V. Gupta, G. Singh, R.Gupta, “Advance cryptography algorithm for improving data security” 2012

[5] M. Rhee, “Internet Security, Cryptographic principles, algorithms and protocols” 2003

[6] A. Sison, B. Gerardo, B. Tanguilig III, Y. Byun, “An improved Data Encryption Standard to Secure Data using Smart Cards” 2011 Pages 113-118

[7] D. Gligoroski, “Cryptographic hash function Edon-R’” May 20-22, 2009 page 1-9

[9] Q. Yu, C. Zhang, X. Huang, “An RC4-Based Hash Function for Ultra-Low Power Devices” April 16-18, 2010 V1-323-V1-328

[8] A. Valizadeh, M. SahebZamani, B. Sadeghian, F. Mehhpour, B. Najafi, “A High Performance Reconfigurable Implementation of DES-LikeAlgorithms” 2004

[9] G. Gong, S. Golomb, “Transform Domain Analysis of DES”, 1999