ANALYSIS OF WEAK KEYS ON DES ALGORITHM

Soe Soe Mon[1], Khin Aye Thu[2], Thida Soe[3]

[1] Author, Lecturer, Faculty of Computer Systems andTechnologies, University of Computer Studies, Hinthada, Myanmar
[2] Author Lecturer, Faculty of Computer Systems andTechnologies, University of Computer Studies, Hinthada, Myanmar
r [3] Author Lecturer, Faculty of Computer Systems andTechnologies, University of Computer Studies,, Hinthada,, Myanmar

ABSTRACT

A cryptographic system is to be implemented in an information processing system. Many of IT applications will be realized as embedded systems, which reiy on security mechanisms.There is a particulariy simple relationship between the operations of decipherment and encipherment. One of the application of cryptographic methods to protect information-processing system is Data Encryption Standard (DES).If cryptography is to be used to protect communications between a terminal and host processor;the key is very important.DES has a 56-bits keys. The security of an algorithm rests in the key; using a cryptographically weak process to generate keys, the whole system is weak. Some encryption algorithms have weak-keys, specify keys that are less secure than the other keys. This system analyze weak-keys on Data Encryttion Standard such as weak-keys, semi-weak keys and possible weak-keys depend on DES algorithm.

Keyword: *Data Encryption Standard (DES), Cryptography, Private-key, Public-key, Permutation, deciphermant, enciphermant, Weak-keys, Semi-weak key.*

1. INTRODUCTION

Cryptography is the art and science of keeping messages, and it is practiced by cryptographers. It is used to protect information to which illegal access is possible and where other protection measures are inefficient.The popularity of the internet as a medium for personal and private communications and its push into commerce,the need for strong encryption and public key standard has become increasingiy urgent and received wide spread attention.It is of great interest in computer science , mainly because of the applications to the internet are so important these days.

Cryptography has become a center of in many departments like computer science, mathematics and electrical engineering. At the same time, that has made important advancaes over the last years. Many of these advances are widely used today.Cryptography is widely recognized that data security will play a central role in the design of IT systems.A cryptograpgicsystem is to be implemented in an information processing system.There is a particularly simple relationship between the operations of decipherment and encipherment.

1.1 Historical Background

Cryptography involves the study of mathematical techniques that allow the practitioner to achieve or provide the following objectives.

- Con-dentitiality is a service used to keep the content of information accessible to only those authorized to have it. This service includes both protection of all users data trnsmitted between two points over a period of time as well as protection of trace from analysis.

- Intrgrity is a service that require computer system access and transmitted information be capable of modification only by authorized users.Modification includes writing, changing, changing the status, deleting, creating and delaying or replaying of transmitted messages.

- It is important to point out that integrity relates to active attacks and it is concerned with detection rather than prevention.Morever, intregrity can be provited with or without recover.

- Authentication is a service that is concerned with assuring that the origin of a message is correctiy identified.That is, information deliver over a channel should be authenticated as to the origin, date of origin, data content, to me sent, etc.For these reasons this service is subdivided into two major classes entity authentication and data origin authentication.Notice that the second class of authentication implicity provides data integrity.

- non- repuditation is a service which prevents both the sender and the receiver of a transmission from denying previous actions.

- These security services are provided by using cryptographic algorithms.There are two major classes of algorithms in cryptography: Private-Key or Symmetric algorithms and Public-Key algorithms.

1.2 Private-Key algorithms

Private-key or Symmetric algorithms where the encryption and decryption key is the same or where thre decryption key can be calaulated from the encryption key and vice versa.The main function of these algorithms, which are also called secret-key algorithms, is encryption of data,often at high speeds.Private-key algorithm require the sender and receiver to agree on the key prior to the communication taking place.The security of privatr-key algorithms rests in the key, the key means that anyone can encrypt and decrypt messages.Therefore, as long as the communication needs to remain secret, the key must remain secret. There are two types of symmetic-key algorithms which are mmonlydistinguished:block cipher and stream cipher.Block ciphers are encryption schemes in which the message is broken into strings of fixed length and encrypted one block at a time. Stream ciphers operate on asingle bit of plaintext at a time.

1.3 Public-Key algorithms

Pubkic-key cryptography is based on the idea of separating the key used to encrypt a message from the one used to decript it.Any one that wants to send a message to party A can encrypt that message using public-key of A but only A can decrypt the message using her private key. In implementating a public-key cryptosystem, it is understood that public-key of A is publicy available to every one, including adversaries of A, it is impossible for anyone, except A, to derive the private-key.

2. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) also known as the Data Encryption Akgorithm (DEA) by the International Standards Organization (ISO), has been a world wide standard. In the early 1970s, nonmilitary cryptographic research was materialize. Almost no research papers were published in this field.Most people knew that the military used special coding equipment to communicate, but few understood the science of cryptography.

The National Security Agency (NSA) had considerable knowledge, but they did not even publicy admit their own existence.

In 1972, the National Bureau of Standards (NBS), now the National Institude of Standard and Technology (NIST), initiated a program to protect computers and communications data.As part of that program, they wanted to develop a single, standard cryptographic algorithm. A single algorithm could be tested and certified and different cryptographic equipment using it could interoperate. In May 15, 1973 Federal Register,the NBS issued a call for proposal for a public encryption algorithm.The algorithm must provide a high level of security.

2.1 Operation of DES Algorithm (DEA)

DES operates on a 64 bit block of plaintext. After an initial permutation, the block is broken into a right haif and a left half, each 32 bits long.Then there ar 16 rounds of identical operations, called function f, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm.In each round, the key bits are shifted, and then 48 bits are selected from the 56 bits of the key. The right of data is expanded to 48 bits via an expansion permutation, combined with 48 bits of a shifted and permuted key via an XOR, sent through 8 S-boxes producing 32 new bits, and permuted again.These four operations make up Function f. The out put of Function f is then combined with the left haif via another XOR. The result of these operations becomes the new right half; the old right half becomes the new left becomes the new left half. These operations are repeated 16 times, making 16 rounds of DES.

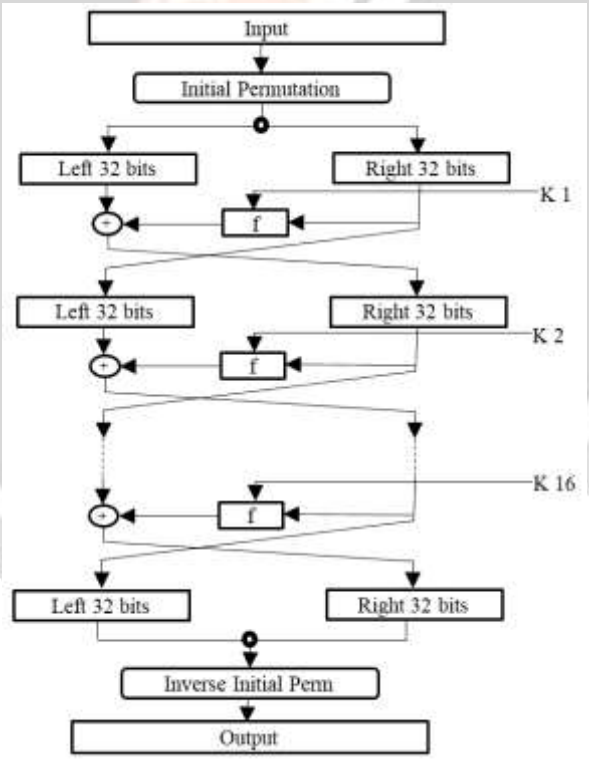

Fig -1: DES algorithm

2.2 Number of Rounds

After five rounds every ciphertext bit is a function of every plaintext bit and every key bit. After eight rounds the ciphertext was essentially a random function of every plaintext bit and every key bit.

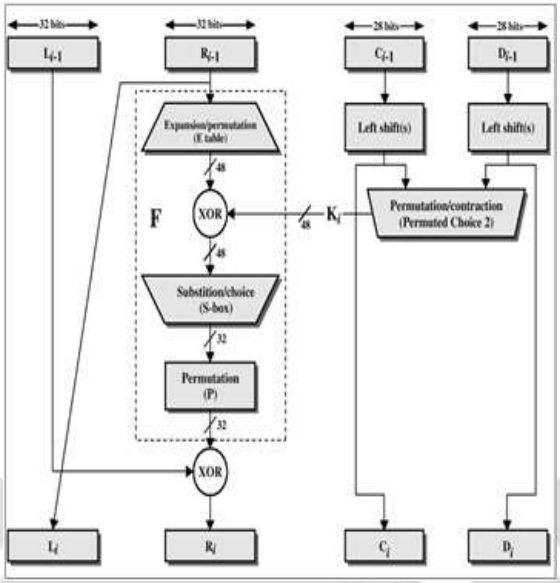

Fig-2: One round of DES

2.3 The Permutation

The initial permutation occurs before round 1, it transposes the input block as describe in Table-1.

Table-1: Initial Permutation

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

After being shifted, 48 out of 56 bits are selected. Because this operation permutes the order of the bits as well as selects a subset of bits, it is called a compressing permutation describe in Table-2.

Table-2: Compression Permutation

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

The expansion permutation changes the order of bits as well as repeating certain bits describe in Table-3.

Table-3: Expansion Permutation

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

2.4 The S-box Substitution

The 48 bits are divided into eight 6 bits sub-blocks. Each separate block is operated on by a separate S-box.The first block is operatde on by S-box 1,the second block is operated on by S-box 2, and so on.

Table-4: Selection Function S-boxes

		Column														
Box	**Row**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
								S_1									
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
								S_2									
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
								S_3									
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
								S_4									
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
								S_5									
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
								S_6									
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
								S_7									
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
								S_8									
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

2.5 The P-box Permutation

Finally, the result of the P-box permutation is XORed with the left half of the initial 64 bits block. Then the left and right halves are switched and another round begins.

Table-5: P-box Permutation

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

2.6 The Final Permutation

The final permutation is the inverse of the initial permutation. Note that the left and right are not changed after the last round of DES; instead the concatenated block $R_{16}L_{16}$ is used as the input to the final permutation. There is nothing going on here; exchanging the halves and shifting around the permutation would yield exactly the same result.This is so that the algorithm can be used to both encrypt and decrypt.

Table-6: Final Permutation

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

2.7 Descryption of DES

DES is symmetric algorithm. the same algorithm and key are used for both encryption and decryption. It is a block cipher and it encrypt data in 64 bit blocks.A 64 bit block of plaintext goes in one end of algorithm and a 64 bit block of ciphertext comes out of other end.It use the 56 bits key length. The key is usually expressed as a 64 bits number, but every eight bit is used for parity checking and is ignored. These parity bits are the least significant bits of key bytes. The key can be any 56 bit number and can be changed at any time. A handful of numbers is considered weak-keys, but they can easily be avoided all security rests within the key.

After all the substitutions, permutations, XORs, and shifting round, the description algorithm is completely different and just as confusing as the encryption algorithm. On the contrary, the various operations were chosen to produce a very useful property. The same algorithm works for both encryption and decryption.

3. KEY MANAGEMENT

In order to realize the increased security potential of DES, key management will need to assume primary importantce. Cryptanalysts often attack both symmetric and public-key cryptosystems through their key management.The security of an algorithm rests in the key. If we are using a cryptographically weak process to generate keys, then the whole system is weak.

DES has a 56 bit key. Implemented properly, any 56 bit string can be the key; there are 2^{56} (10^{16}) possible keys. These poor key generation procedures have made its DES ten thousand times easier to break than a proper implementation. The number of possible keyys with various constraints on the input strings. The time required for an exhaustive search through all of those keys, given a million attempts per second. There is a very time differential between an exhaustive search for 8 byte keys and exhaustive search of 4,-, 5-, 6-, 7-, and 8 byte keys.

Table-7: Number of Possible Keys of Various Key Spaces

	4- Bytes	5-Bytes	6-Bytes	7-Bytes	8-Bytes
Lowercase letters(26)	460000	$1.2x\ 10^7$	$3.1x\ 10^8$	$8.0x\ 10^9$	$2.1x\ 10^{11}$
Lowercase letters and digits(36)	1700000	$6.0x\ 10^7$	$2.2x\ 10^9$	$7.8x\ 10^{10}$	$2.8x\ 10^{12}$
Alphanumeric characters(62)	$1.5x\ 10^7$	$9.2x\ 10^8$	$5.7x\ 10^{10}$	$3.5x\ 10^{12}$	$2.2x10^{14}$
Prinable characters(95)	$8.1x\ 10^7$	$7.7x\ 10^9$	$7.4x\ 10^{11}$	$7.0x10^{13}$	$6.6x\ 10^{15}$
ASCII characters(128)	$2.7x\ 10^8$	$3.4x\ 10^{10}$	$4.4x\ 10^{12}$	$5.6x10^{14}$	$7.2x10^{14}$
8-bit ASCII characters(256)	$4.3x\ 10^9$	$1.1x\ 10^{12}$	$2.8x10^{14}$	$7.6x10^{16}$	$1.8x10^{14}$

Table-8: Exhaustivew Search of Various Key Spaces

	4- Bytes	5-Bytes	6-Bytes	7-Bytes	8-Bytes
Lowercase letters(26)	5 seconds	12 seconds	5 minutes	2.2 hours	2.4 days
Lowercase letters and digits(36)	1.7 seconds	1 minutes	36 minutes	22 hours	33 days
Alphanumeric characters(62)	15 seconds	15 minutes	16 hours	41 days	6.9 years
Prinable characters(95)	1.4 minutes	2.1 hours	8.5 days	2.2 years	210 days
ASCII characters(128)	4.5 minutes	9.5 hours	51 days	18 years	2300 days
8-bit ASCII characters(256)	1.2 hours	13 days	8.9 years	2300 years	580000 days

3.1 Random Keys

Some encryption algorithms have weak-keys: specific keys that are less secure than the other keys. DES has only 16 weak-keys out of 2^{56}, so the odds of generating any of these keys are incredibly small. It has been argued that a cryptanalyst would have no idea that a weak key is being used and therefore gains no advantage from their accidental use. It has also been argued that not using weak keys give a cryptanalyst information. However, testing for the few weak keys is so easy that is seems imprudent not to do so. Generating keys for public-key cryptography system is harder, because often the keys must have certain mathematical properties.

3.2 Weak Keys

The initial value is split into two halves, each half is shifted indenpendently. If all the lines are either 0 or 1, then the key used for any cycle of the algorithm is the same for all cycles of the algorithm. This can occur if the key is entirely 0s or if one half of the key is entirely 1s and the other half is entirely. Also, two of the weak keys have other properties that make them less secure. The four weak keys are shown in hexadecimal notation in Table-9.

Table-9: DES Weak Keys

Weak Key Value (with parity bits)				Actual Key
0101	0101	0101	0101	0000000 0000000
1F1F	1F1F	0E0E	0E0E	0000000 FFFFFFF
E0E0	E0E0	F1F1	F1F1	FFFFFFF 0000000
FEFE	FEFE	FEFE	FEFE	FFFFFFF FFFFFFF

3.3 Semi-weak Keys

Additionally, some pairs of keys encrypt plaintext to the identical ciphertext other words, one key in the pair can decrypt message encrypt with the other in the pair. This is due to the way in which DES generates sub-keys; instead of generating 16 different sub-keys, these keys generate only two different sub-keys. Each these sub-keys is used eight times in the algorithm. These keys are called semi-weak keys, and are shown in hexadecimal notation in Table-10.

Table-10: DES Semi-weak Keys

01FE	01FE	01FE	01FE	and	FE01	FE01	FE01	FE0
1FE0	1FE0	0EF1	0EF1	and	E01F	E01F	F10E	F10
01E0	01E0	01F1	01F1	and	E001	E001	F101	F10
1FFE	1FFE	0EFE	0EFE	and	FE1F	FE1F	FE0E	FE0
011F	011F	010E	010E	and	1F01	1F01	0E01	0E0
E0FE	E0FE	F1FE	F1FE	and	FEE0	FEE0	FEF1	FEF

3.4 Index of Coincidence

The index of coincidence (IC) measures the variation in the frequencies of letters in the ciphertext. If the period of cipher is one (1), that is substitution has been used, there will be considerable variation in the letter frequencies of IC will be high. As the period increase, the variation is gradually eliminated and IC is low.

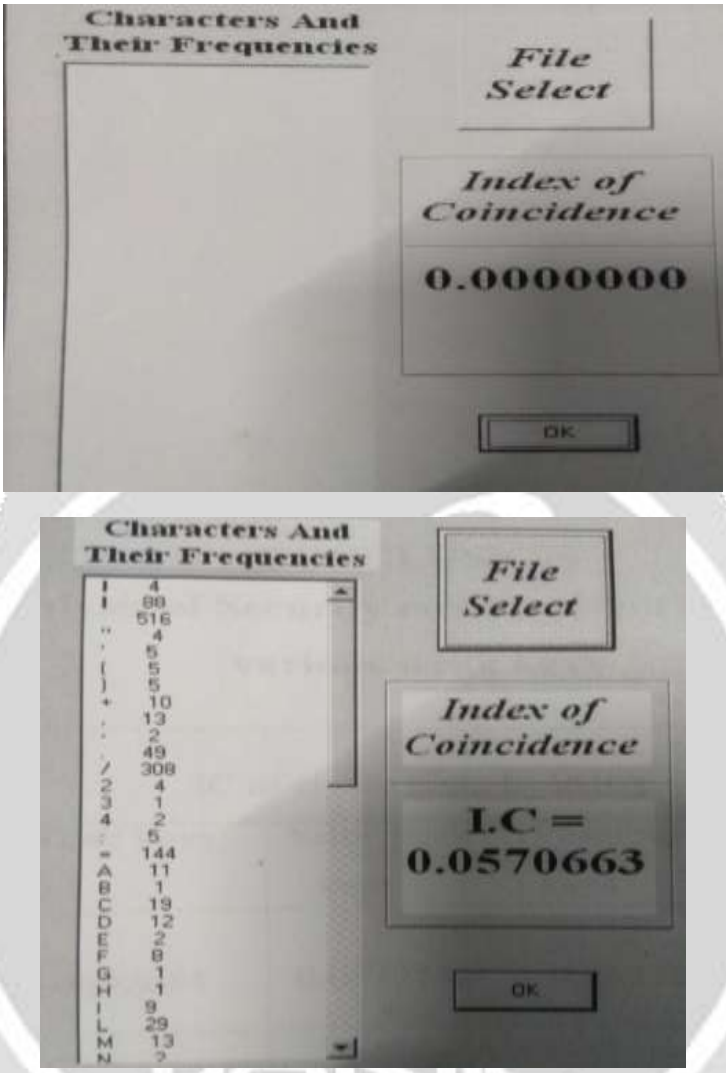

Fig-3 Index of coincidence

3.5 Analysis of Security Measurement by Using Various Weak Keys

Table-11

No: of Char	IC of ciphertext by using			
	Weak keys	Semi Weak keys	Possible weak keys	Good keys
100	0.0692681	0.0672143	0.0622681	0.0511352

1000	0.0837392	0.0816967	0.0737392	0.0666356
5000	0.1085228	0.1042984	0.1035228	0.1018173
10000	0.1127397	0.1097133	0.1068397	0.1040372

4.CONCLUSIONS

This paper has investigated the cryptographic method for data security during transmit and store. With conventional encryption, a fundamental requirement for two parties to communicate securely is that they share a secret key. The security of an algorithm rests in the key. If we are using a cryptographically weak process to generate keys, then the whole system will be weak. So, we must avoid from weak key for security of communication between both sides.

5.ACKNOWLEDGEMENT

I would like to express my gratitute to my parents , for their tender care of my life. I also wish to thank all my teachers.

6.REFERENCES

[1]. Bruce Schneier, E-mail Security, How to Keep Your Electronic Message Private, John Wiley and Sons, Inc., 1995

[2]. Bruce Schneier, Applied Cryptography, Protocols, Algorithms and Source code in C, John Wily and Sons, Inc., 1995

[3]. Aifred J.Menzes, Paul C. van Oorschot, Scoot A. Vanstone Handbook of Applied Cryptography, 1997 by LLC

[4]. Michael J. Young, Mastering Visual C, Sybex Inc., 1998

[5]. Smith, R.E., Internet Cryptography, Addision Wesley Longman, Inc., 1999.

[6]. dorothy Elizabeth Denning, Cryptography and Data Security.