

Double Way Protection of Triple Data Encryption Standard Algorithm

Dr. M. Jaya Kumar¹, Mr. R. Nandha Kumar²

Assistant Professor, Department of Information Technology, SNMV College of Arts and Science, Coimbatore^{1,2}

Abstract: Cryptographic algorithms are used as fundamental techniques for assuring confidentiality and integrity of data used in financial transactions and for authenticating entities involved in the transactions. Secure data transmission via Internet or any public network, there is no alternative to cryptography. It is widely used by governmental and intelligence agencies around the world to safe transmission of any format of messages-online or offline. No data online is secure unless use any type of cryptography to send your messages. Cryptographic algorithm development is a never-ending race as the cryptanalysts are also getting smatter with the advent of higher computer power of decoding secret codes.. This research will concentrate on increasing the complexity of block cipher encryption. Secure key based Treble Data Encryption Standard algorithm (STDES) is based on secure keys of Static IP address. STDES algorithms ensure the improved encryption performance, high secure and less encryption, decryption time. STDES algorithm is highly secure while improving the efficiency of cryptography algorithm.

Keywords: Secure key, Static IP address, Encryption, Decryption, Permutation, S-box.

1. INTRODUCTION

Cryptography has been long in use by governments, military sector and other areas for security purpose. Cryptography is used in the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics and computer science [1][2]. Cryptography has wide range of applications such as ATM cards, computer passwords, and electronic commerce. Cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key [3]. Networks are admiring day by day in our life. The widespread for using Internet makes the need for protection of user data. Encryption algorithm plays an important role for information security. Encryption is the process of transforming plain text data into the cipher text (secure data) in order to reveal its meaning. TDES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods recorded the weaknesses of TDES, which made it an insecure block cipher [4][5]. We proposed secure key based Treble Data Encryption Standard algorithm is included the function of key Static IP address to manipulate. This kind of algorithm used other security improvement in identified dispatcher; recipient geo location is high securing in the cryptography algorithms.

2. TRIPLE DATA ENCRYPTION STANDARD (DES)

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits[6]. The Triple DES then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three

times. Hence the name Triple DES, The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES, also known as 3DES. Consequently, Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse [7]. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

If consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

- Encrypt with K1
- Decrypt with K2
- Encrypt with K3

Decryption is the reverse process:

- Decrypt with K3
- Encrypt with K2
- Decrypt with K1

Setting K3 equal to K1 in these processes gives us a double length key K1, K2. Setting K1, K2 and K3 all equal to K has the same effect as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be compatible with a system using single-DES. DES operates on a 64 – bit block of plaintext [8]. After an

initial permutation the block is broken into a right half and left half, each 32 – bits long. Then there are 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 finishes off the algorithm. DES operates on a 64 – bit block of plaintext [9][10]. After an initial permutation the block is broken into a right half and left half, each 32 – bits long. Then there are 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 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 [11]. The right half of the 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.

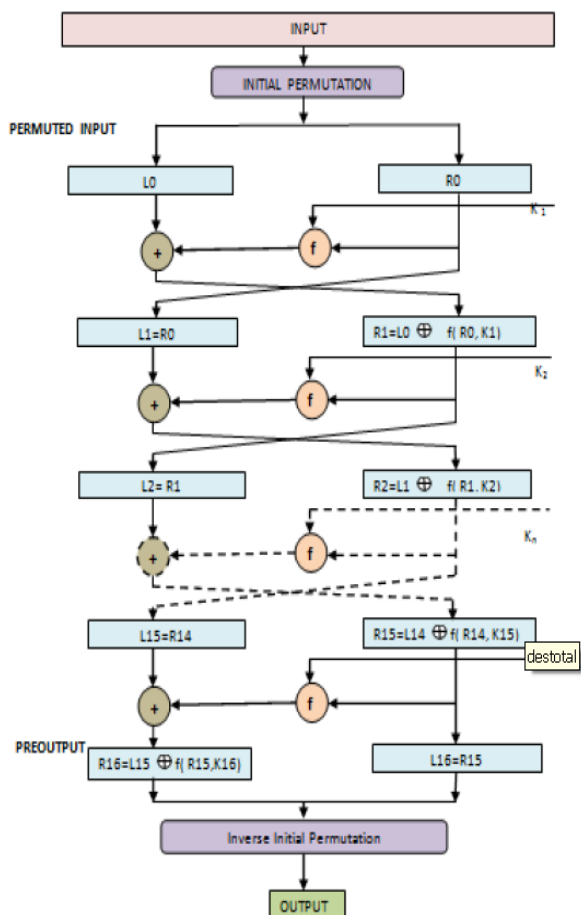


Figure-1 Enciphering computation

3. STATIC IP ADDRESS BASED TRIPLE DATA ENCRYPTION STANDARD

STDES is a block cipher--meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**.

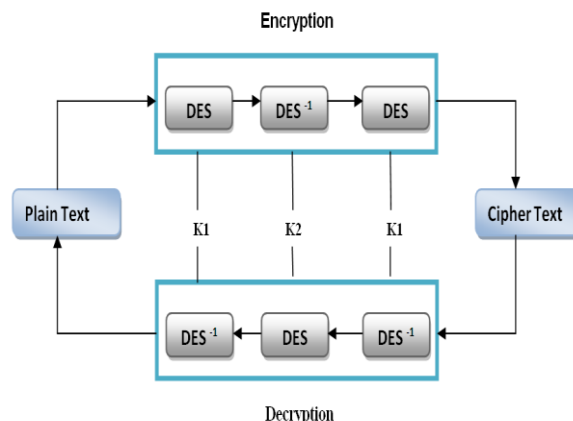


Figure-2 Triple DES Process

3.1 Key preparation

The 144 bit key (static IP address) is used STDES algorithm. Split this one key K1 (48 bit) into left and right halves, **C0** and **D0**, where each half has 24 bits. With **C0** and **D0** defined, we create sixteen blocks **Cn** and **Dn**, $1 \leq n \leq 16$. Each pair of blocks **Cn** and **Dn** is formed from the previous pair **Cn-1** and **Dn-1**, respectively, for $n = 1, 2, \dots, 16$, using the following schedule of "left shifts" of the previous block. To do a left shift, move each bit one place to the left, except for the first bit, which is cycled to the end of the block.

Table-1 Bit Rotation

Sender Address	Static IP Number of Left Shifts	Receiver Address	Static IP Number of Left Shifts
1	1	1	1
2	1	2	2
3	8	3	2
4	8	4	2
5	0	5	1
6	9	6	7
7	1	7	8
8	1	8	8
9	2	9	1
10	3	10	8
11	4	11	0
12	4	12	0
13	0	13	2
14	5	14	4
15	0	15	7
16	0	16	7

Example **C3** and **D3** are obtained from **C2** and **D2**, respectively, by left shifts, and **C16** and **D16** are obtained from **C15** and **D15**, respectively, by zero left shift. In all cases, by a single left shift is meant a rotation of the bits

one place to the left, so that after one left shift the bits in the 24 positions are the bits that were previously in positions 2, 3,..., 24, 1.

3.2 Encryption process

Step1: k_1, K_2, k_3 are the keys in key expander with the selection function.

Step2: Encryption process is activated with key k_1 . And this encryption output is given to input of the decryption with key K_2 .

Step3: Decryption output is given to input of encryption with k_3 .

There is an initial permutation **IP** of the 64 bits of the message data **M**. This rearranges the bits according to the following table, where the entries in the table show the new arrangement of the bits from their initial order. The 58th bit of **M** becomes the first bit of **IP**. The 50th bit of **M** becomes the second bit of **IP**. The 7th bit of **M** is the last bit of **IP**.

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

Figure-3 Initial permutation

Next divide the permuted block **IP** into a left half **L0** of 32 bits, and a right half **R0** of 32 bits, continues proceed through 16 iterations, for $1 \leq n \leq 16$, using a function **f** which operates on two blocks--a data block of 32 bits and a key **Kn** of 48 bits--to produce a block of 32 bits. Let + denote XOR addition, (bit-by-bit addition modulo 2). Then for **n** going from 1 to 16 we calculate

$$L_n = R_{n-1} \quad R_n = L_{n-1} + f(R_{n-1}, K_n)$$

This results in a final block, for $n = 16$, of **L16R16**. That is, in each iteration, we take the right 32 bits of the previous result and make them the left 32 bits of the current step. For the right 32 bits in the current step, we XOR the left 32 bits of the previous step with the calculation **f**.

$$L_1 = R_0 \quad R_1 = L_0 + f(R_0, K_1)$$

It remains to explain how the function **f** works. To calculate **f**, we first expand each block **Rn-1** from 32 bits to 48 bits. This is done by using a selection table that repeats some of the bits in **Rn-1**. Next to use of this selection table the function **E**. Thus **E (Rn-1)** has a 32 bit input block, and a 48 bit output block. Let **E** be such that the 48 bits of its output, split as 8 blocks of 6 bits each, are obtained by selecting the bits in its inputs in order according to the following table:

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

Figure-4 E Bit Selection Table

Thus the first three bits of **E(Rn-1)** are the bits in positions 32, 1 and 2 of **Rn-1** while the last 2 bits of **E(Rn-1)** are the bits in positions 32 and 1. Next in the **f** calculation, we XOR the output **E(Rn-1)** with the key **Kn**:

$$K_n + E(R_{n-1}).$$

We have expanded **Rn-1** from 32 bits to 48 bits, using the selection table, and XORed the result with the key **Kn**. We have 48 bits, or eight groups of six bits. Do something strange with each group of six bits: we use them as addresses in tables called "**S boxes**". Each group of six bits will give us an address in a different **S** box. Located at that address will be a 4 bit number. This 4 bit number will replace the original 6 bits. The net result is that the eight groups of 6 bits are transformed into eight groups of 4 bits for 32 bits total.

$$K_n + E(R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8, S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$

where **Si(Bi)** refers to the output of the **i**-th **S** box. To repeat, each of the functions **S1, S2, ..., S8**, takes a 6-bit block as input and yields a 4-bit block as output.

If **S1** is the function defined in this table and **B** is a block of 6 bits, then **S1(B)** is determined as follows: The first and last bits of **B** represent in base 2 a number in the decimal range 0 to 3 (or binary 00 to 11). Let that number be **i**. The middle 4 bits of **B** represent in base 2 a number in the decimal range 0 to 15 (binary 0000 to 1111). Let that number be **j**. Look up in the table the number in the **i**-th row and **j**-th column. It is a number in the range 0 to 15 and is uniquely represented by a 4 bit block. The final stage in the calculation of **f** is to do a permutation **P** of the **S**-box output to obtain the final value of **f**:

$$f = P(S_1(B_1)S_2(B_2)...S_8(B_8))$$

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

Figure-5 P Table

The permutation **P** is defined in the following table. **P** yields a 32-bit output from a 32-bit input by permuting the bits of the input block.

In the next round, we will have $L2 = R1$, $R2 = L1 + f(R1, K2)$, and so on for 16 rounds. At the end of the sixteenth round we have the blocks **L16** and **R16** [12]. We then **reverse** the order of the two blocks into the 64-bit block **R16L16** and apply a final permutation **IP-1** as defined by the following table:

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

Figure-6 IP⁻¹

Output of the algorithm has bit 40 of the pre-output block as its first bit, bit 8 as its second bit, and so on, until bit 25 of the pre-output block is the last bit of the output. Result in hexadecimal format is

- 1st Output: 47BC956CF71C5A0A
- 2nd Output: B71A8D7D6E78CFA1
- 3rd output: 7D8EDC151BA8F30A

For the plain text “123456ABCD132536”, secure Static IP key1 “118.091.234.050” and Key2 “122.178.180.247”, the STDES algorithm generate the following output value 7D8EDC151BA8F30A

4. PROTECTION OF STRONG KEY BASED STDES

A main challenge of data security in open network (Internet) is unauthorized access of data, duplicates, hacking of password, hacking of messages, data loss. Static IP address based Triple Data encryption standard algorithm solved these problems. Any doubt for Senders and recipients Static IP address is hackers address then easy to check geo location, it's through identified address originality.

I. WAN IP address

Only authorized WAN IP address(receiver) holder access the text, this algorithm protect automatically checked allowed IP address list. Suppose unauthorized access is attempt in decryption process than the decryption process will be stopped or the text also be erased.

II. Geo location

Since dispatcher, recipients WAN IP address are included in this algorithm, it is easily identified dispatcher and recipient in geo location [13]. For example WAN IP address and geo location is given below


IP Address	: 118.91.234.50
Location	:  INDIA, TAMILNADU, POLLACHI
Latitude / Longitude	: 10.6638 LATITUDE, 77.0066 LONGITUDE
Connecting through	: ABTINFO SYSTEMS PVT LIMITED
Time Zone	: UTC+05:30
Net Speed	: DSL
IDD Code	: 91
Weather Station	: INXX0177 - COIMBATORE/PEELAMEDU

Figure-7 Receiver's Static IP address Geo-location


IP Address	: 122.178.180.247
Location	:  INDIA, TAMILNADU, COIMBATORE
Latitude / Longitude	: 10,9925 LATITUDE, 76,1694 LOGITUDE
Connecting through	: Bharati Airtel Ltd, Telemedia
Time Zone	: UTC + 05:30
Net Speed	: DSL
IDD Code	: 91
Weather Station	: INXX0177-COIMBATORE

Figure-8 Sender's Static IP address Geo-location

III. STDES Algorithm

Secure key based Triple Data Encryption Standard algorithm is included the part of IP address key (Static IP address).STDES Encryption process is based on recipient WAN IP Address, using IP address key automatically checked and capture the decryption process. So hackers, unauthorized access is not possible.

5. CPU TIME COMPARISON

Time taken for encryption and decryption process is significantly less in STDES algorithm than TDES algorithm. The Table-2 shows time taken for encryption and decryption process of TDES algorithm and STDES algorithm

Table-2 Time comparison encryption-decryption

Method / Process	Encryption	Decryption
TDES	4.21	4.22
STDES	3.21	3.21

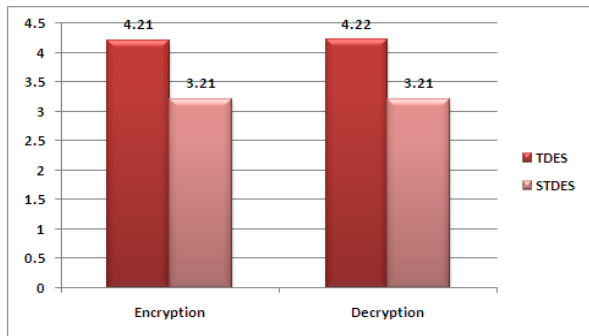


Figure-9 Time management of TDES vs. STDES

7. CONCLUSION

This approach also provides more security, confidentiality, and authentication as STDES algorithm is strong enough to Encryption and decryption process. This procedure explores efficiency of time/space, hardware and software and flexibility of IP address key (Static IP address).

We proposed a revised Triple Data Encryption Standard algorithm Key mix using Static IP address instead of conventional key addition which increases the security of TDES. Secure key based Triple Data Encryption Standard algorithm is stronger.

6. ADVANTAGES OF SECURE KEY BASED TDES

The proposed STDES algorithm is effectively stops their known attack resistance than the TDES algorithm. As shown in Table1 STDES algorithm takes 3.21sec to encrypt the plain text which is reduce of time while comparing with TDES algorithm. This algorithm designed using simplified Key scheduling and at the same time high data security of encryption and decryption process is maintained. STDES algorithm Protection of three level processes in WAN IP address, geo location, and inbuilt IP address key based algorithm to execute the process is high level security in cryptography.

- Information in computer is transmitted and has to be accessed only by the authorized address holder and not by anyone else.
- The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized address or a false identity
- Only the authorized party is allowed to decryption process, otherwise text or file will be erased.
- Sender, receiver geo-location is identified easily

Table-3 Comparison of DES & STDES

Tribble Encryption Standard	Data	Secure key using Tribble Data Encryption Standard
Key size =168bit		Key Size = 144 Bit
Key distributed		Key Collected (Automatically WAN IP checked)
Key scheduling process number of Left Shifts is constant		Key scheduling process based on WAN IP address
Any place can access		Particular Wan IP Address Holder Only Accessed
Possible for Keys faked and Misused		Not possible for Misused key
Possible Meet-in-the-Middle Attack		Not possible
Geo-locations identification is not possible		Geo-locations identified easily

Only particular WAN IP Address holder to access restriction rule is highly secure in the cryptography world. Static IP address is easy identification of sender's, receiver's IP address gets and put their IP address ip2location .com or check the IP address database and get senders geographical location, i.e. country, region, city, latitude, longitude, ZIP code, time zone, connection speed, ISP and domain name, IDD country code, area code, weather station code and name.

Security analysis and experimental results the proposed encryption and decryption scheme is fast and on the other hand it provides good security on the data.

REFERENCES

- [1]. Bruce Schneier, "Applied Cryptography - Protocol, Algorithm and Source Code in C", Second Edition, John Wiley & Sons, 2008.
- [2]. William Stallings, "Network Security Essentials (Applications and Standards)" Pearson Education, 2004,pp.2-80.
- [3]. Charles P. Pfleeger, Shari Lawrence Pfleeger. "Security in Computing", Pearson Education 2004 pp. 642-666.
- [4]. Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."IBM Journal of Research and Development, May 1994,pp. 243 -250
- [5]. W.Stallings, "Cryptography and Network Security4th Ed," Prentice Hall, 2005, PP. 58-309.
- [6]. NIST Special Publications 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm", National Institute of Standard and Technology, 2000
- [7]. Federal Information Processing Standards Publication 140-1, "Security Requirements forCryptographic Modules", U.S. Department of Commerce/NIST, Springfield, VA: NIST, 1994
- [8]. Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.
- [9]. Diaa Salama, Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, PP.78-87,Sept. 2010.
- [10]. Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, New York,1996.
- [11]. Miles E. Smid and Dennis K. Branstad, "The Data Encryption Standard: Past and Future," in Gustavus J. Simmons, ed., Contemporary Cryptography: The Science of Information Integrity, IEEE Press, 1992
- [12]. O.P Verma, Ritu Agarwal, Dhiraj Dafouti , Shobha Tyagi, "Performance Analysis Of Data Encryption algorithms",IEEE Delhi Technological University India, 2011.
- [13]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures,"AdHoc Networks Journal, vol. 1, no. 2-3,pp. 293-315 (2003) September.



BIOGRAPHIES



Dr. M. Jaya Kumar MCA, M. Phil, Ph.D is presently working as assistant professor, Department of Information Technology, SNMV College of Arts and Science, Coimbatore. He worked as a programmer in Bannari Amman Spinning mills for Seven years. He has published many papers in international

Journals; his area of interest include Software Engineering, Network security. He has to credit 2 Years of Teaching and research experience



Mr. R. Nandha Kumar, M. Sc M. Phil is presently working as a assistant professor, Department of Information Technology, SNMV College of Arts and Science, Coimbatore. He has more than 7 years of teaching experience. His area of interest is Network Security.