DOI: 10.24996/ ijs.2017.58.3C.19

Iraqi Journal of Science

ISSN: 0067-2904

Strong Triple Data Encryption Standard Algorithm using Nth Degree Truncated Polynomial Ring Unit

Mayes M. Hoobi

Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.

Abstract

Cryptography is the process of transforming message to avoid an unauthorized access of data. One of the main problems and an important part in cryptography with secret key algorithms is key. For higher level of secure communication key plays an important role. For increasing the level of security in any communication, both parties must have a copy of the secret key which, unfortunately, is not that easy to achieve. Triple Data Encryption Standard algorithm is weak due to its weak key generation, so that key must be reconfigured to make this algorithm more secure, effective, and strong. Encryption key enhances the Triple Data Encryption Standard algorithm securities. This paper proposed a combination of two efficient encryption algorithms to satisfy the purpose of information security by adding a new level of security to Triple Data Encryption Standard algorithm using Nth Degree Truncated Polynomial Ring Unit algorithm. This aim achieved by adding two new key functions, the first one is Enckey(), and the second one is Deckey() for encryption and decryption key of Triple Data Encryption Standard to make this algorithm more stronger. The obtained results of this paper also have good resistance against brute-force attack which makes the system more effective by applying Nth Degree Truncated Polynomial Ring Unit algorithm to encrypt and decrypt key of Triple Data Encryption Standard. Also, these modifications enhance the degree of complexity, increase key search space, and make the ciphered message difficult to be cracked by the attacker.

Keywords: Block Ciphers, Cryptography, PTR, DES, 3DES, Key.

الخوارزمية القوية للتشفير الثلاثي للبيانات باستخدام حلقة متعددة الحدود

ميس محمد هوبي

قسم الحاسبات، كلية العلوم، جامعة بغداد، العراق.

الخلاصة

التشفير هو عملية تحويل رسالة لتجنب الوصول غير المصرح به من البيانات. واحدة من المشاكل الرئيسية وجزء مهم في التشفير مع خوارزميات السرية هو المفتاح. لمستوى أعلى من الاتصال الآمن المفتاح يلعب دورا هاما. ولزيادة مستوى الأمن في أي اتصال، يجب أن يحصل الطرفان على نسخة من المفتاح السري الذي للأسف ليس من السهل تحقيقه. خوارزمية تشفير البيانات الثلاثي القياسية ضعيفة في لتوليد المفاتيح ، بحيث يجب إعادة تشكيل المفتاح لجعل هذه الخوارزمية أكثر أمنا وفعالية وقوية. مفتاح التشفير يعزز تشفير البيانات القياسية في الأوراق المالية. اقترحت هذه الورقة مجموعة من خوارزميتي تشفير كفوئتين لتحقيق غرض أمن المعلومات عن طريق إضافة مستوى جديد من الأمان إلى خوارزمية تشفير البيانات

Email:mais.shms@yahoo.com

الثلاثي باستخدام خوارزمية حلقة متعددة الحدود . هذا الهدف يتحقق من خلال إضافة اثنين من الوظائف الرئيسية الجديدة، أول واحد هو ,Enckey()والثاني هو Deckey() للتشفير وفك التشفير مفتاح الثلاثي تشفير البيانات القياسية لجعل هذه الخوارزمية أكثر قوة. نتائج هذه الورقة لديها أيضا مقاومة جيدة ضد القوة الغاشمة الهجوم الذي يجعل النظام أكثر فعالية من خلال تطبيق حلقة متعددة الحدود لتشفير وفك تشفير مفتاح التشفير الثلاثي للبيانات القياسية. أيضا هذه التعديلات تعزز درجة التعقيد، وزيادة مساحة البحث الرئيسية، وجعل الرسالة مشفرة الصعب أن يكون متصدع من قبل المهاجم.

1- Introduction

With the wide developments of computer applications and networks, the security of information has high attention in our common fields of life. The most important issues are how to control and prevent unauthorized access to secure information [1]. In this case, especially cryptography techniques are applicable [2]. Cryptography (the science of using secret codes) is the process of secret writing means scrambling the data which is not in readable format [3]. The need of cryptography is arises to protect the private information from unauthorized person. There are different goals of cryptography like confidentiality, authentication, integrity, non-repudiation, access control etc. Data is encrypted by using various cryptographic algorithms. Security of the data or system is depends on both cryptographic algorithm and key used for encryption/decryption [4].

Cryptography mainly includes two parts i.e. encryption and decryption, encryption is the process of converting of plain text (readable) to cipher text (unreadable) and decryption is the process of converting cipher text (unreadable) to plain text(readable) as shown in Figure-1,[5]. There are several ways of classifying cryptographic algorithms ,they were categorized based on the number of keys that are employed for encryption and decryption .Figure -1 depicts this ways [6]. Symmetric (private – key) use the same key for encryption and decryption, for example AES, DES, TDES, RC2, and RC6 while asymmetric (public-key) use the different keys for encryption and decryption for example Diffie-Hellman, RSA, and DSA.

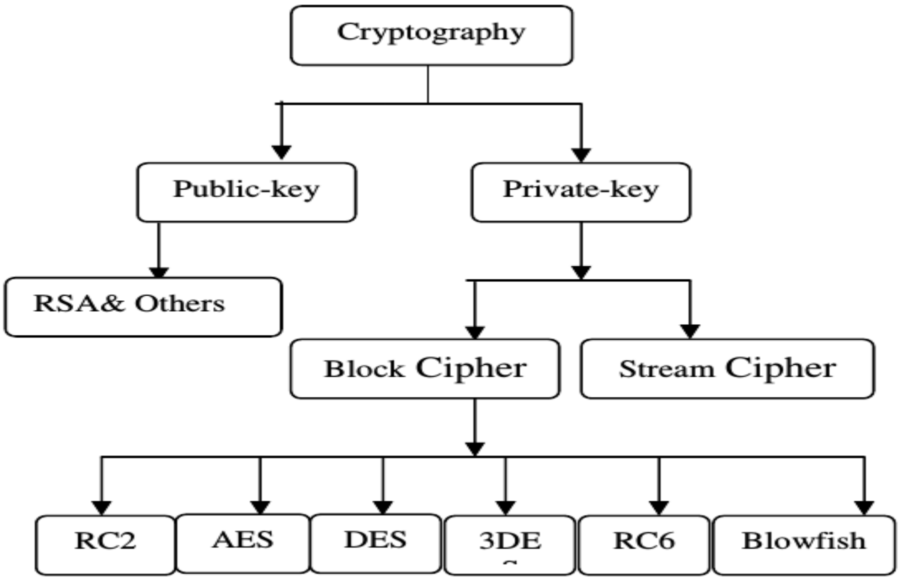


Figure 1- Cryptography Classifying Ways.

The DES (Data Encryption Standard) algorithm is a block cipher operates on the 64-bit plain text which uses the same key for both encrypt and decrypt data blocks, 64-bit key produces the 64-bit encrypted cipher text from 64-bit plain text and for decryption same process is done in reverse. The DES algorithm is weak due to its key generation [7].

The rest of the paper is organized as follows. Section 2 includes related work. Section 3 includes overview of DES and 3DES algorithms. Section 4 explains the TPR algorithm. Section 5 explains proposed system. Section 6 includes results analysis and section 7 includes conclusions.

2- Related Work:

The expansion of key search space of several cryptography algorithms is the aim of several works. [8] proposed an extended DES called Random Data Encryption Algorithm (RDEA). New features added to the DES include pseudo randomized cipher key for encryption and protocols for sending cipher key embedded in the cipher text.

[9] proposed the idea of TKE (Two Key), which is versatile in the sense that it can perform faster and works easily with hardware. Aside from these advantages, it also has high-level security like the DES.

[10] Blowfish encryption encrypts a 64-bit block of data using a key with lengths ranging from 32 to 448 bits. The encryption itself is a sixteen round encryption revolving around utilizing S-Boxes and complex key schedules.

In this paper applying Nth Degree Truncated Polynomial Ring Unit algorithm to encrypt and decrypt key of 3DES algorithm.

3- (DES) Data Encryption Standard Algorithm:

DES it is a symmetric key encryption scheme i.e. the same secret key is used for encrypting and decrypting message. DES is the shortest for Data Encryption Standard, in addition it a block cipher i.e. it operates on the blocks of plaint text input message of fixed length and processes using the key, and transforms the plaintext through a complicated series of operations to produce cipher text (of the same length). All blocks are numbered from left to right which makes the eight bits of each byte.The description of DES algorithm shown in Figure-2 [3].

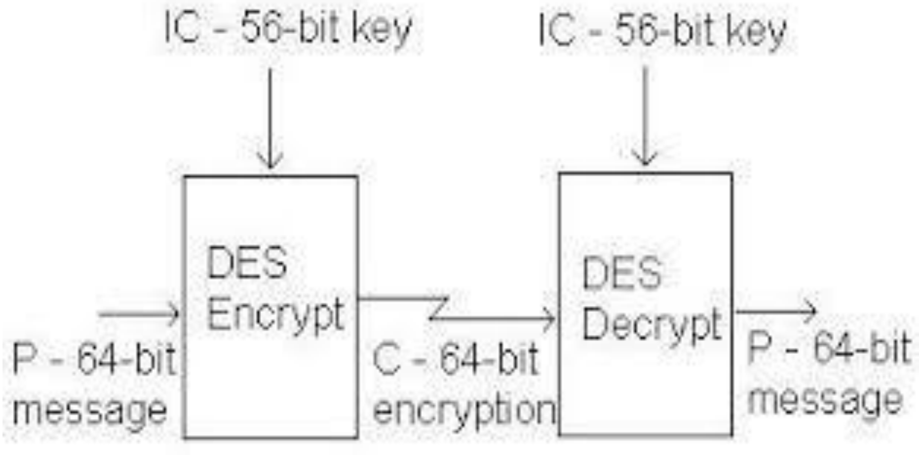


Figure 2- DES Algorithm Description

It works on 64-bit plain text to produce 64-bit cipher text, therefore 64-bit plain text data is given as input to perform the initial permutation (IP) first, then key dependent permutation and at last final permutation which is inverse initial permutation i.e.IP-1 DES algorithm performs 16-rounds of operation to produce 64-bit output data. The implementation of DES requires four basic operations mainly XOR, shift, LUT (Look up table) and permutation. As shown in Figure -3 [5], 64-bit data input is initially getting permuted by IP and then get splits into two equal parts right half (R0) and left half (L0), each is 32-bit in length. Right half in first round will be the left half of the next round and right half of next round is obtained by firstly expanding 32-bits to 48-bits by using expansion function in that we expand it by repeating some bits then this expanded 48-bit are XOR with 48-bit key and then results fed into eight 6-bit substitution boxes (S-boxes) which converts 48-bit input to 32-bit output i.e. 6-bit sbox gives 4-bit output to form 8 4-bit boxes and finally permutation is done on these 32-bits. In next stage this 32-bit permuted output is get XORed with first right half 32-bits to get next right half 32-bits [11].

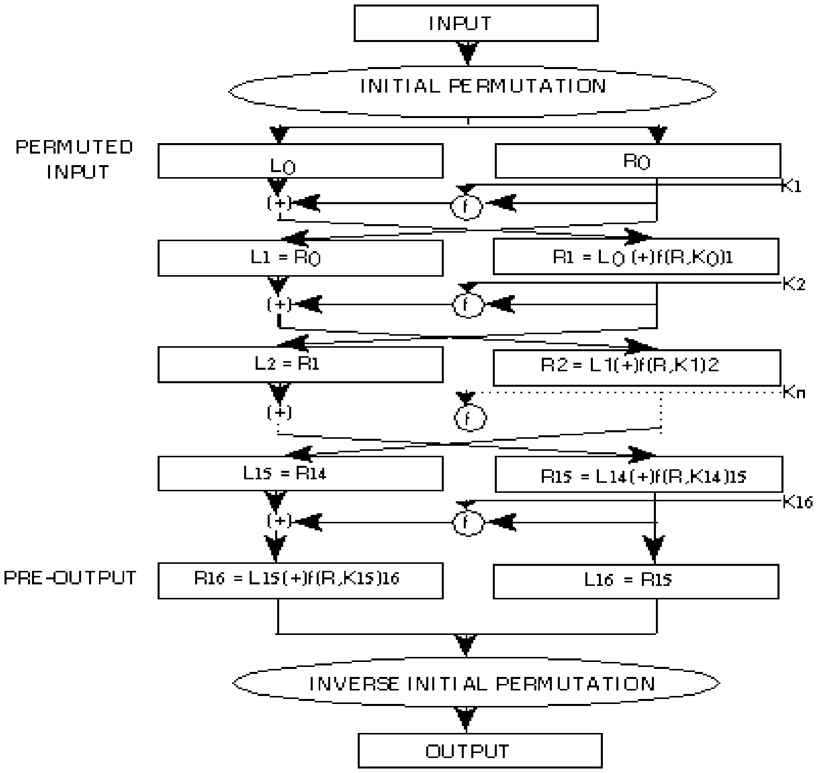


Figure 3-64-bit plain text DES Encryption.

The parity bit DES uses a key of bit length 56 bit, which is considered short. And hence DES algorithm is considered weak. In actual, the key length for DES key is 64 bits, but only 56 bits are considered and the rest of 8 bits are used as parity bits (for calculating checksum). Function F in the key dependent permutation is the most important function of the DES algorithm and its operation is as shown in Figure -4 [12].

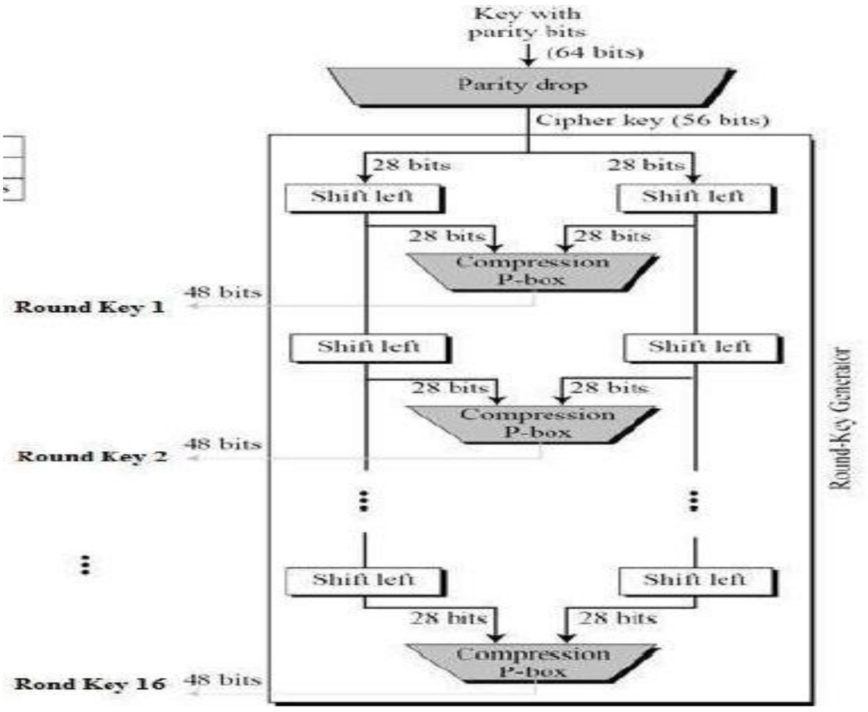


Figure 4- 64-bit DES Key Encryption.

In DES algorithm there are 16 round, probably to guarantee the elimination of any correlation between the cipher text and either the plaintext or key. At the end of the 16th round, create what is known as the pre-output. The sequence of events that occur of key DES algorithm, initially the key is passed through a permutation function then for each of the 16 iterations, a subkey is produced by a combination of a left circular shift and a permutation which is the same for each iteration. However, the resulting sub key is different for each iteration because of repeated shifts. The decryption process with DES is essentially the same as the encryption process but use the cipher text as the input to the DES algorithm but use the keys Ki in reverse order. That is, use K16 on the first iteration, K15 on the second until K1 which is used on the 16th and last iteration[13]. Some critical analysis have theoretically proved the weakness of DES algorithm, although it is practically too tough to crack it. DES is no exception, intruders have exploited its weaknesses to bypass secure encryption to steal sensitive information since it has been publicly known as a standard of encryptions. One major concern surrounding DES security is the key length (56 bits). Intruders have devised attacks that can work against it. Attacks known to have successfully broken DES security are Brute Force (exhaustion attack), Differential Cryptanalysis, and Linear Cryptanalysis [14].

3-1 Triple DES (3DES): A stronger form of DES

Triple DES algorithm has another form which is comparatively considered secure because of long key length. Triple DES algorithm involves key of length 3 X 64 = 192 bits, which is three times the key length of single DES key. A triple DES consists of three DES keys as shown in Figure-5 [14], say k1, k2 and k3 each of 64 bits. In Triple DES encryption, data is encrypted with first key (k1), then the output is decrypted with second key (k2) and then the resultant is again encrypted with third key (k3). It is important to remember that only 56 bits of each key i.e. k1, K2 and k3 are considered not 64 bits. That means, 8 bits of every key is ignored as key bits and used as parity bits based on the values of these three keys [15].

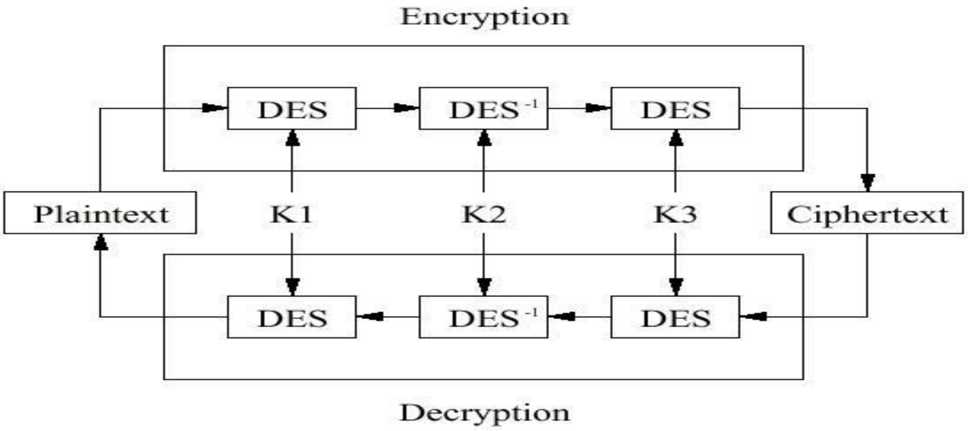


Figure 5- 3DES Keys.

Triple DES can be categorized into 3 types, also known as keying options as listed below [11]:-

1. **Single key 3DES**: if all the three keys are identical. For example – if your single DES key is abcdef0123456789, then your equivalent 3DES key would be abcdef0123456789-abcdef0123456789 -abcdef0123456789.
2. **Double key 3DES**: If the first and the third keys (i.e k1 and k3) are identical. For example – If k1 = abcdef0123456789 and k2 = 9abcdef012345678 , then the equivalent 3DES key would be – abcdef0123456789- 9abcdef012345678- abcdef0123456789 .
3. **Three Keys3DES**: If all the keys are different. For example – k1 = abcdef0123456789- k2 = 9abcdef012345678- k3 = 89abcdef01234567 Equivalent 3DES key would be - abcdef0123456789- 9abcdef012345678- abcdef0123456789
4. **(TPR)Nth Degree Truncated Polynomial Ring Unit Algorithm:**

According to Kirchhoff's principle, the resistance of the cipher to attack is based on the secrecy of the key. According to this the guessing the key should be so difficult that there is no need to hide the encryption and decryption algorithms, but in 3DES algorithm, 56 bit key is the main weakness because there are now 2^{56} possible keys are available which are easily get crack by “brute force attacks”. It involves trying all 2^{56} keys. So to improve the performance of the 3DES algorithm and enhance security we have to increase number of possible probability of key. TPR is relatively new cryptosystem. The strength of cryptographic TPR performs valuable private key operations much faster in comparison to other algorithms [16]. The algorithm is based on embedding messages in a polynomial ring, R. The ring R consists of truncated polynomials of degree N-1 having integer coefficients that are reduced modulo certain parameters. The notation for the Ring is given as: [17, 18]

$R= Z[X] / (X^{N-1})$ ………………………………………………………………………………… (1)

Where Z represents the set of integers and N is 1 more than the degree of the polynomial. TPR PKCS is specified by a number of parameters (par) and keys as shown in Table-1 [17, 18].

Table 1- TPR Parameter and Keys

Par	Explanation
N	The polynomials in the truncated polynomial ring have degree N-1
Q	Large modulus: The coefficients of the truncated polynomials will be reduced mod q
P	Small modulus: The coefficients of the message are reduced to mod p
F	A polynomial that is the private key
G	A polynomial that is used to generate the public key h from f
H	A polynomial that is the public key
R	The random “blinding polynomial.
K	A security parameter which controls resistance to certain types of attacks, including plaintext awareness.
d_f	The polynomial f has df coefficients equal to 1, (d_f-1) coefficients equal to -1, and the rest equal to 0.
d_g	The polynomial g has d_g coefficients equal to 1, d_g coefficients equal to -1, and the rest equal to 0.
d_r	The polynomial r has d_r coefficients equal to 1, d_r coefficients equal to -1, and the rest equal to 0.

Key Generation:

Bob wants to create a public/private key pair for the TPR public key cryptosystem [17, 19].

- Bob chooses 2 random polynomials f and g in the defined ring R. A polynomial is relative to a random polynomial mod q.
- Bob then computes the inverse of f mod q and the inverse of f mod p.

The inverses are denoted as f_q and f_p respectively.

$f * f_q = 1 \pmod q$ ……………………………………………………………….(2)

$f * f_p = 1 (\mathrm{mod}\ p)$……………………………………………………………... (3)

- Bob should select f such that its inverses f_q and f_p exists.
- Bob computes the product,

$h=p.f_q*g(\mathrm{mod} q)$………………………………………………………………………(4)

- Bob's private key is the pair of polynomials f and f_p. Bob's public key is the polynomial h.

TPR Encryption:

Alice wants to send a message to Bob using Bob's public key h [17, 18]

- Alice converts her message in the form of a polynomial m whose coefficients are chosen modulo p, between –p/2 and p/2 (m is a small polynomial mod q)
- Alice randomly chooses a random polynomial r, which is used to obscure the message.
- Alice computes the polynomial

e=pr*h+m(modq)……………………………………………………………………….(5)

- The polynomial e is the encrypted message which Alice sends to Bob.

TPR Decryption:

Bob on receiving Alice's encrypted message e, wants to decrypt it [19, 20].

- Bob uses his private polynomial f to compute

a=f*e(modq)……………………………………………………………………………..(6)

Since Bob is computing a mod q, he chooses the coefficients of a to lie between –q/2 and q/2.

- Bob next computes the polynomial

b=a(m mod p)……………………………………………………………………………(7)

- reducing each of the coefficients of a mod p.
- Bob uses his other private polynomial f_p to compute

c=f_p*b(modp)…………………………………………………………………………. (8)

- Polynomial c will be Alice's original message m.

5. Proposed improved 3DES -TPR algorithm (3DES -TPR)

The 3DES algorithm is now must be replaced by the proposed improved algorithm , since its adoption have been concerns about the level of security provided by 3DES in two areas, Key and nature of the algorithm. 3DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. 3DES uses a key bundle that comprises 3DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is: ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$.

i.e., DES encrypt with K_1, DES decrypt with K_2, then DES encrypt with K_3. Decryption is the reverse: plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$.

i.e., decrypt with K_3, encrypt with K_2, and then decrypt with K_1. Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last, this improves the strength of the algorithm. This section illustrates the steps involved in constructing the proposed hybrid cryptography algorithm called (3DES -TPR) as shortest for Triple Data Encryption Standard and Nth Degree Truncated Polynomial Ring Unit algorithms. Addition level of security and increasing the probability of brute force attack are the purposes of this proposed algorithm. The 3DES algorithm is a symmetric block cipher that operates on 64-bit block as input and output data. 3DES encrypts/decrypts a plaintext /ciphertext by repeatedly applying the specific round functions a number of times, (16 rounds). Until now the DES has been as standard, at this time need for more secure information to prevent the attacker from discover the original plain text message. Because of using key in more than one phases (encryption and decryption), now want to focus and highlight on importance in 3DES algorithm and to improve this key encrypted it using TPR algorithm to satisfy the purpose of cryptography system in 3DES algorithm. If the attack was able to recognize the keys used in encryption, he can discover the plain text by deciphering the cipher text. Now in this position the proposed algorithm 3DES -TPR strong the encryption system by entered TPR algorithm to encrypt/decrypt 3DES key as addition level of security and increase the hide secure information to prevent attack from code breaking. In the proposed algorithm 3DES -TPR was differ, this different was implemented by adding encryption function (Enckey()) of 3DES keys by using TPR algorithm. In this case the sender must send (encrypted message and keys). Now the inverse cipher phase must be apply, initially in this phase of proposed algorithm the decryption function (Deckey()) of 3DES keys must be applied also by using TPR algorithm , then the cipher transformations can be implemented in order to produce a straight forward . Shortly, in the proposed 3DES -TPR algorithm there are two functions were added to improve the 3DES algorithm. The first function Enckey() was added at encryption (encrypt key using TPR algorithm), the second one Deckey() was added before the first round at decryption (decrypt DES key using TPR algorithm). The structure of 3DES is the same except the encryption and decryption key functions are added. The main improvement of the proposed functions is to increase the probability of brute force attack that was used to cryptanalytic the cipher. This operation leads to increase the degree of complexity and key search space during the encryption and decryption processes. This proposed improvement functions using with hybrid algorithm 3DES -TPR to encrypt and decrypt 3DES keys in three cases. :-

1. First Case (Single key 3DES)

In this case two proposed key functions Enckey() and Deckey() are added to encrypt and decrypt single key of 3DES algorithm, i.e key length=56-bit.

2-Second Case (Double key 3DES)

In this case the two proposed functions Enckey() and Deckey() are used to encrypt and decrypt double keys of 3DES algorithm, i.e key length=112-bit .

3- Third case (Three key 3DES)

In this case the two proposed functions Enckey() and Deckey() are used to encrypt and decrypt three keys of 3DES algorithm i.e key length=168-bit.

The goal of the proposed approach is to use proposed two additional functions that applied on 3DES keys, these additional proposed functions lead to generate more secure block cipher instead of using one or more keys in direct manner. The proposed algorithm 3DES -TPR encrypts/decrypts different keys by using TPR algorithm. Figures- (6, 7) illustrates the original and proposed algorithms 3DES -TPR

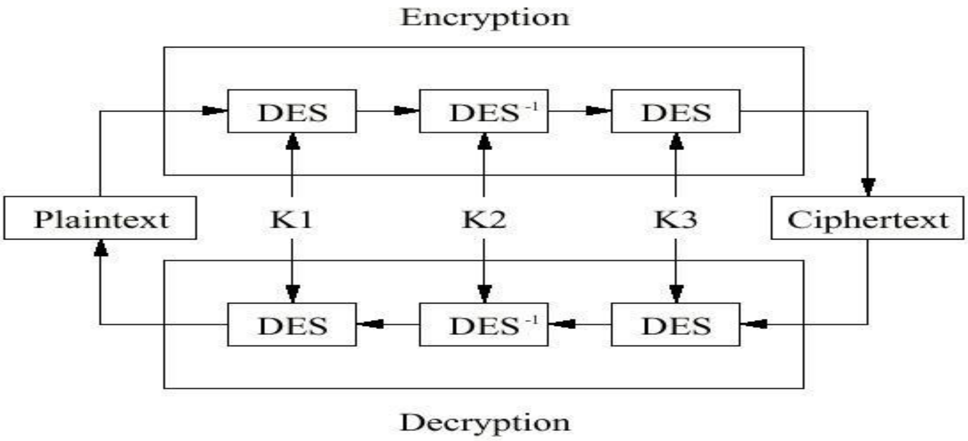


Figure 6-Standard 3DES Algorithm.

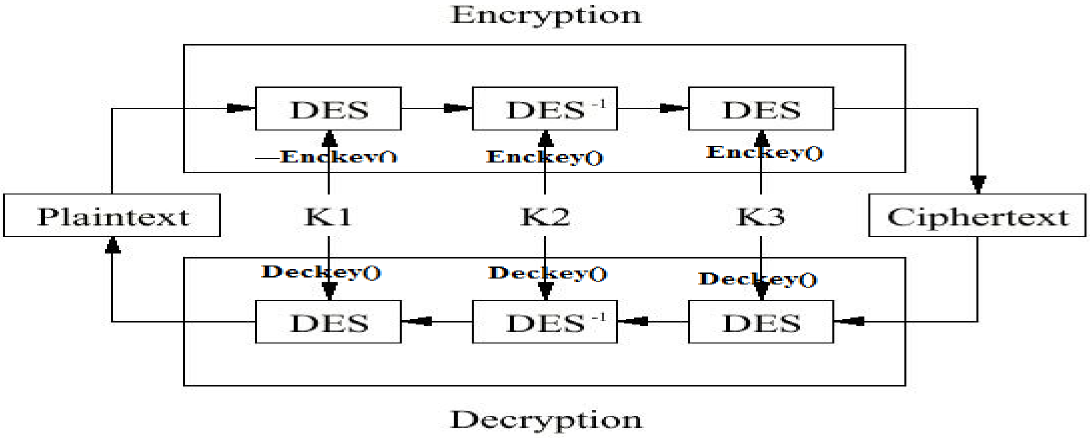
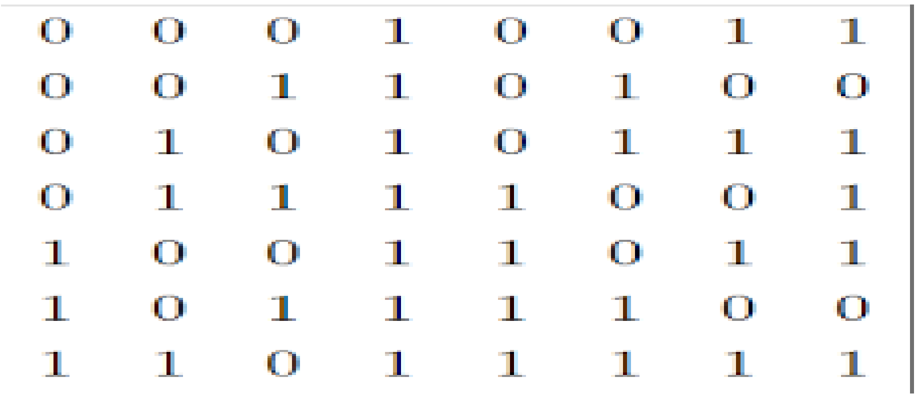


Figure 7-Proposed 3DES -TPR Algorithm.

5-1 DES key Encryption/Decryption Example Using TPR Algorithm

This section represents an example of using TPR algorithm to encrypt /decrypt the values of 3DES keys to satisfy the purpose of the proposed improvement. Because of TPR algorithm encrypts message that can be represent as odd degree polynomial only [20, 21], each value of 3DES keys was treated as message consists of 7 bits with leaving the last bit within each byte for calculating checksum without encryption. Key must be designed to be more resistance to known cryptanalytic attacks. Because of using key in several phases in 3DES algorithm, the improvement of the proposed algorithm was especially applied on 3DES keys. For executing successful cryptography operation converting these values to equivalent binary representation as show in example in Figure-8.



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

Figure 8-Binary Representation of Suggested Key

In other words how to generate cipher key after divided 56bit key in to seven 8-bit blocks, as illustrated in Table-2.

Table 2-Key Representation

Bit no.	Block no.
0-7	1
8-15	2
16-23	3
24-31	4
32-39	5
40-47	6
48-55	7

Now start with TPR key generation stage, choose the parameters to satisfy the condition $q > (6.d + 1)$ p.

So choose, $N = 7$, $p = 3$, $q = 64$, $d = 2$.

Which satisfy $128 = q > (6.d + 1)\ p = 39$.

Then choose

$f = X + X^2 - X^4 - X^5 + X^6 \in L(3, 2)$.

$g = 1 + X^3 - X^4 - X^6 \in L(2, 2)$.

Next computes the inverses as mentioned previously in section that explained PTR Algorithm:

$f_p = 1 + 2X + X2 + 2X3 + 2X4 + 2X6$

$fq = 60 + X + 9X^2 + 17X^3 + 16X^4 + 62X^5 + 28X^6$

store f and f_p as private key then computes the public key according the equation (3):

$h = 46 + 50X + 2X^2 + 35X^3 + 5X^4 + 62X^5 + 56X^6 \pmod{64}$

Now choose the small random polynomial that represent r value,
Let
$r = -X + X^3 + X^4 - X^6 \in L(2, 2)$.
let 8- bit key value can represent by the following polynomial
$m = -1 - X + X^5 + X^6$

Now, apply PTR encryption algorithm to obtain the encrypted message polynomial e according the equation (6):
$e = 61 + 18X + 33X^2 + 31X^3 + 63X^4 + 56X^5 + 58X^6$
In the same manner, each 8 bit key value can be represented as message to be encrypted with NTRU algorithm. Now after receiving the encrypted message (8-bit key) value:
$e = 61 + 18X + 33X^2 + 31X^3 + 63X^4 + 56X^5 + 58X^6$
From sender ,the receiver uses the private key f to compute (a) according to equation (7):
$a = 4 - 6X - 9X^2 + X^4 + 9X^5 + X^6 \pmod{64}$
Next reduce the coefficients of (a) modulo (3) to get (b) according to equation (8):
$b = 1 + X^4 + X^6 \pmod{3}$
Finally the receiver uses his other part of private key f_p to compute (c):
$c = -1 - X + X^5 + X^6 \pmod{3}$
Since the polynomial (d) is the same as the original plain text m (8-bit key), then the decryption of encrypted message successfully. This improvement that was implemented by encrypt /decrypt for each value of 8-bit key in case1 (single key 3DES), case2 (double key 3DES), and case3 (triple key 3DES) as mentioned previously.

6- Results Analysis

This section demonstrates the results obtained by implementing the proposed improved algorithm 3DES -TPR described previously with three cases. The results obtained after applying two proposed functions(Enckey() and Deckey()) in three cases (single key 3DES, double key 3DES, and triple key 3DES encryption and decryption achieve higher complexity compared to standard DES algorithm as illustrated. In the following Tables- (3-5), it could be noticed that the complexity is improved many times and increased key search space compared to the standard 3DES algorithm.

Table 3- Case-1(Sinle key 3DES)

Algorithm	Key Length	Key Search Space
3DES	56-bit	2^{56}
3DES-PTR	56-bit	$2^{56} * 2^{56} * 2^m * 2^n = 2^{3136} * 2^n * 2^m$

Table 4-Case-2(Double key 3DES)

Algorithm	Key Length	Key Search Space
3DES	112-bit	2^{112}
3DES-PTR	112-bit	$2^{112} * 2^{112} * 2^m * 2^n = 212533 * 2^n * 2^m$

Table 5- Case-3(Three key 3DES)

Algorithm	Key Length	Key Search Space
3DES	168-bit	2^{168}
3DES-PTR	168-bit	$2^{168} * 2^{168} * 2^m * 2^n = 2^{28224} * 2^n * 2^m$

In this research the value of increasing in probability can be computed as follows:-

- The probability for each 8 bit key is 2^8 =256, and then the probability of 56 bit key is equal to $2^{(56*56)}$. Therefor the complexity of proposed 3DES-PTR as compared with the complexity of standard 3DES was largely increased.

-The probability of finding the two private key polynomials(f and r) of PTR as mentioned previously, let the probability of finding polynomial (f) of degree (n) through GF(2) is 2^n , let the probability of finding polynomial (r) of degree (m) through GF(2) is 2^m. Then the key search space can be increased and computed according the key length used with proposed 3DES-TPR algorithm :- (2^{256} $*2^{256}*2^m*2^n$). The results of the present proposed algorithm have good cryptographic strength. This algorithm is resistant to differential cryptanalysis which requires that the key of encryption to be by using PTR algorithm.

7- Conclusions

The security of any type of algorithm is dependent on the secrecy of the key. Based on the results in this research, the main conclusions can be summarized as improved key functions increase the complexity in a block cipher increase the key search space that increase the probability of brute force attack that used to cryptanalytic the cipher. This can be summarized as: use n-DES because a simple DES is too weak (a 56-bit key can be brute-forced by a determined attacker), but in order to really improve security, must go to n ≥ 3.

References

1. Vilas, V.D. and Dinesh, V.P. and Ashok, S. W. **2014**. Performance Evaluation of AES using Hardware and Software Codesign. *IJRITCC International Journal on Recent and Innovation Trends in Computing and Communication,* **2** (6): 1638 – 1643.
2. Ashwini, R. T. and Akshay, P. D. **2014**. Review paper on FPGA based implementation of Advanced Encryption Standard (AES) algorithm. *IJARCCE International Journal of Advanced Research in Computer and Communication Engineering,* **3** (1).
3. Rahul, L. and Gaurav, P. **2015.** Implementation of AES-256 Bit. *Inventi Journals, Information Security* Volume. (issue3).
4. Ling, D. and Kefei, Ch. S. **2012**. *Cryptographic Protocol*. Springer.
5. Priyan, K. and Vishal, P. **2016.** Design and Implement Dynamic Key Generation to Enhance DES Algorithm. *International Journal for Research in Applied Science & Engineering Technology,* **4**(7).
6. Magesh, B. V. T. Shankar Ganesh, K. **2014**. A Comparative Analysis on Encryption and Decryption Algorithms. *International Journal of Scientific and Research Publications*. **4**(12).
7. William, S**. 2006**. *Cryptography and Network Security Principles and Practice,* 5th edition. Prentice Hall
8. Manfred, L. and Johannes, M. **1986**. *American National Standard for Financial Institution Message Authentication*, American Bankers Association.
9. Washington, D.C. **1982**. *America National Standard for Personal Identification Number (PIN) Management and Security*. American Bankers Association.
10. Schneier, B. **1994.** *Description of a new variable-length key, 64-bit block cipher (blowfish)* Springer pp. 191-204.
11. Grabbe, O. **2011**. *The DES algorithm illustrated*, Laissez Faire City, Vol. 2.
12. Rabah, K. **2005.** Theory and implementation of data encryption standard . *Information Technology Journal*, **4**: 307-325.
13. Washington, DC. **1977** .*Data Encryption Standard, Federal Information Processing Standards Publication* (FIPS Pub) **4**, National Bureau of Standards,
14. Gong-bin Q. and Qing-feng J., and Shui-sheng Q. **2009** A new image encryption scheme based on DES algorithm and Chua's circuit, *IEEE International Workshop on Imaging Systems and Techniques*, pp. 168- 172.
15. Julia, J. and Ramlan, M., Salasiah, S. and Jazrin, R. **2012**. Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key. *International Journal of Cyber-Security and Digital Forensics*,**1** (3).
16. Rhee, M.Y. **2003**. *Internet Security: Cryptographic Principles, Algorithms and Protocols*. Wiley. England.

17. Premnath, A.P. **2010**. Application of NTRU Cryptographic Algorithm for securing SCADA communication. M.Sc. Thesis. Department of Computer Science .University of Nevada.

18. D'Souza, R. **2001**. The NTRU Cryptosystem: Implementation and Comparative Analysis. Semester Project. George Mason University.

19. Blomgren, P. and Kotronx, S.M. **2006** *Cryptographic Protection of SCADA Communications* .American Gas Association (AGA).

20. Brar, R. S. and Singh, S. **2013**. Efficient Cryptography with Compression / Decompression Mechanism of Text Files against IP Spoofing., *International Journal of Application or Innovation in Engineering and Management, (IJAIEM),* **2** (7) .

21. Jeffrey, H. and Pipher, J. and Silverman, J. H. **2008** *.An Introduction to Mathematical Cryptography*, Springer, New York.