Ultramodern Encryption Standard Cryptosystem using Prolic Series for Secure Data Transmission

P.Sri Ram Chandra[1], G.Venkateswara Rao[2], G.V.Swamy[3]

[1](CSE, GIET (A) and Gitam University, Andhra Pradesh,India)
[2, 3](IT, Gitam University, Andhra PradeshIndia)

Abstract: We are in the era of transforming technology, where secure data transmission plays a vital role in protecting the data. The best means of protecting the data are cryptographic techniques, which are classified as symmetric key cryptography(both the encryption and decryption uses same keys) and asymmetric key cryptography(two different keys are used for encryption and decryption). In this paper we have proposed a new symmetric stream cipher cryptography algorithm with a title Ultramodern Encryption Standard (UES) for secure data transmission which uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes. If an intruder intercepts the message, it is difficult to decipher the message because of multilevel cipher rounds used in this algorithm. We have analyzed the strength of this algorithm over differential cryptanalysis. This algorithm unfailingly follows the Strict Plaintext Avalanche Criterion (SPAC) and Strict Key Avalanche Criterion (SKAC) which gives the study of how differences in input or key can affect the respective output and the results are tabulated.

Keywords: Binary code,Cryptanalysis,Cryptography, Decryption,Encryption, Gray code, Intruder, Prolic number.

1. Introduction

Now-a-days computer applications were developed to handle the data related to crucial areas like banking, army and government, in transferring such significant data across the network may sometimes get into the hands of the intruders who may tamper the contents of the data [1]. In this regard security measures should be taken to protect the data, which in turn facilitates the secure data transmission [2].

The security measures developed need to maintain few principles of security like confidentiality, integrity, authentication, non-repudiation [2]. Considering the data transmission between two entities A and B, ‘if A ensures that none expect B gets the data’ is termed to be as confidentiality, integrity states that both A and B will undergo an agreement such that, none of them would tamper the data further. ‘B assures that the data was sent by A only’ designated as authentication, non-repudiation does not allow the sender of a message to refuse the claim of not sending the message [2].

Therefore the algorithms developed should have principles of security, in this paper the authors have proposed a new algorithm for secure data transmission which ensures that an intruder cannot access the plaintext without having knowledge about the secret key.

2. Cryptography

Cryptography is one of the principle means of secure data transmission where the data encryption and decryption processes are involved with or without a secret key. In cryptography, a cryptosystem is a suite of three algorithms: one for key generation, one for encryption, and the other for decryption. Encryption is the process where encoding of messages took place with proper keys in such a way that only authorized users canaccess it, on the other side decryption is illustrated as un-encrypting the encoded text so as it can be treated as humanreadable format ofthat text [2]. Here the encoded message can be called as cipher text whereas the original message is called the plain text. Precisely speaking enciphering and deciphering are most common synonyms of encryption and decryption respectively [1].

2.1 Classificationof Cryptography algorithms

From the point of view of using keys in the cryptographic algorithms, they primarily classified as symmetric and asymmetric key cryptography. The symmetric key cryptography uses two identical keys for the process of enciphering and deciphering. The keys in practice can be represented as a shared secret between sender and receiver in order to maintain the private information link [4]. On the other side asymmetric key cryptography uses two un-identical keys i.e., one for enciphering and the other for deciphering process respectively [1].

2.2 Cryptographic attacks

A cryptographic attack is a method in which the security of a cryptosystem is bypassed by the intruder having knowledge either on encryption or decryption, cryptographic protocol used or key management scheme [3]. The first attack identified was ciphertext attack, which occurs when an attacker is well aware of only the cipher text. The attacker can deduce the plain text on analyzing the frequency of the occurrences of the characters [5]. The known plaintext problem occurs when the attacker is having some paired fragments of plaintext and the corresponding cipher text [2].

The chosen cipher text is the attack in which the cryptanalyst (attacker) captures the part of the information and deduce the decryption process under the unknown key [7]. The chosen plain text is quoted to be one of the most dangerous attacks where attacker chooses a plaintext to be encrypted further analyses the relation between chosen plaintext and obtained cipher text to procure the key used for encryption process [5]. Codebook attack is a kind of attack where the block of given plaintext is always encrypted to same block of cipher text as long as the same key is used [1]. A ‘man-in-the-middle’ attack is a kind of active attack where the attacker furtively relays and perhaps amend the conversation between the two entities who believe they are directly communicating with each other [6].

2.3 General metrics of the Cryptographic algorithm

Cryptography is the art and science of keeping the messages secure and it is practiced by cryptographers. On the other side the cryptanalysts are the practitioners of cryptanalysis, the art and science of breaking the ciphertext [9]. In developing cryptographic algorithms, cryptographers need to consider the following general characteristics.

a) Type of the algorithm based on key: The algorithms based on usage of the keys are generally of two kinds i.e., symmetric key and asymmetric key [9].
b) Function: The encryption function used for message secrecy must follow theprinciples of security [9].
c) Key length: The key length is the base function in providing security to the cryptosystem [9].
d) Attack steps: Formally defined as the number of steps required by the attacker to perform the best known attack [9].
e) Attack time: The time taken by the attacker to crack the key or cryptosystem [9].
f) Rounds: The increase in the number of rounds of encryption may lead to more confusion and diffusion, hence more security exists [9].

3. The Ultramodern Encryption Standard (UES) Cryptosystem

In this paper the authors have proposed a new symmetric cryptography algorithm titled Ultramodern Encryption Standard for secure data transmission which uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes. Prolic series number is a number which satisfies the relation $T_n = n*(n+1)$ $n \geq 0$ where T_n is n^{th} term of the prolic series.The 8 bit plaintext acts as an input and two 8 bit keys are used for encryption process in a single round, in fact the process undergoes 16 rounds of encryption and two output transformations of 8 bit keys each i.e., a total of 34 blocks of keys 8 bit each are required. The process of key generation, encryption and decryption are briefly described in the sections 3.1, 3.2 and 3.3 respectively. In the further sections of this paper we use the acronym UES which represents Ultramodern Encryption Standard.

3.1 Key generation process

The key generation of UES algorithm starts by selecting an arbitrary prolic series number following the relation $T_n= n*(n+1)$ such that $0 \leq n \leq 255$, the ASCII character range, it is being represented as 17 bit binary code. The binary code is converted to 17 bit gray code i.e., 34 bits were considered, the process continues till it generates 272 bit key. Now the generated 272 bits are divided into 34 blocks of 8 bits each, which are being used as set of keys for encryption and decryption process. The detailed key generation algorithm and pseudo code were described in the table1.

TABLE 1.UES Key generation algorithm and pseudo code

UES Key generation algorithm	UES key generation pseudo code

Step1:Select an arbitrary prolic number in the Range 0 through 255 and represent it in 17 bit binary code.
Step2: Now convert the 17 bit binary code to 17 bit Gray code. Here we count 34 bits.
Step3: Rerun the step2 until we count 272 bit key.
Step4: Partition the above generated 272 bit key as 34blocks of 8 bit each and name them as $K_{n,}$ 1 ≤n≤34.
	SET n = arbitrary prolic number.
	SET i = 1
	SET array [ ]
	SET count = 0
	b = binary code (n)….17 bits
	ADD b to array [ ]
	WHILE i ≤ 15
	b = gray code (b)
	$g_n = b_n$ /*n is most significant bit*/
	$g_i = b_i \oplus b_{i+1}$, 0 ≤i≤ n-1
	ADD b to array [ ]
	Set i = i+1
	FOR j=0 to array length – 1
	IF j+1 mod 8 = 0
	PRINT the array [0] through array [j] as K_n
	END IF
	END FOR

After the keys generated, the sender has to send the sequence of decryption keys saved in a file to the concerned receiver via a secured means of communication channels like Short Message Service (SMS) or e-mail or Flash message (more secured, even older) [1].

3.1.1 Binary-Gray Code analysis

The section 3.1 briefly described about the conversion of binary to gray code as part of the key generation which aims at security such that even part of the key was hacked by intruder, it should be a tough task to find the origin of the key. Since gray code is the reflected binary code, it looks like as same as binary with change in the bits. Soif an intruder tries in converting it to any other form, even its corresponding ASCII character the original key would not have been generated.

In this regard we made an analysis that, in conversion of 2bit binary code to 2bit gray code, the original 2 bit binary code can be achieved in two steps of conversion. Similarly 3 and 4 bit binary code can be achieved in four steps of binary-gray code conversions.In this key generation we are converting 17 bit binary code to gray code for 15 times, absolutely less than 32 times (No of Binary-Gray code conversions required to achieve original Binary) so it's a tough task for the intruder to crack the original key when he/she come to know even part of the key. The table2 briefly describes the number of binary to gray code conversions required to achieve the original binary.

TABLE 2. Binary – Gray code Analysis

No of bits in Binary code (key)	No of Binary-Gray code conversions required to achieve original Binary.	No of bits in Binary code (key)	No of Binary-Gray code conversions required to achieve original Binary.
2	2	17 through 32	32
3 or 4	4	33 through 64	64
5 through 8	8	65 through 128	128
9 through 16	16	129 through 255	256

3.2 Encryption process

The process of encoding a message m with proper key(s)k and encryption algorithm E in such a way that only authorized users can access it is termed to be as encryption, which generally represented as cipher text $c= \boldsymbol{E}(k,m)$[4]. The encryption process starts with giving 8 bit plaintext as an input, there after it undergoes 16 rounds of encryption where 32 blocks of key 8 bits each are being used. Finally the process would halt by operating two output transformations using 2 blocks of key 8 bits each. Detailed execution of encryption and one round of encryption are illustrated in the Fig1 and Fig2 respectively.

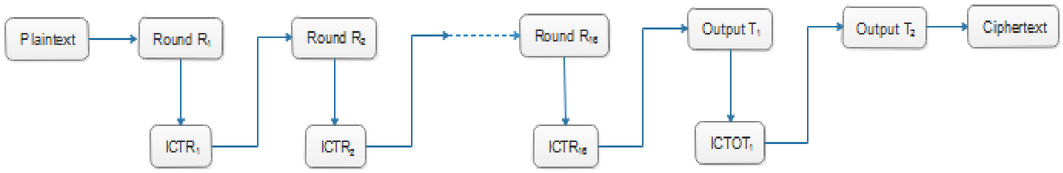

Fig 1. Encryption process of UES.

Where ICTR$_{\#}$ indicates Intermediate Cipher text of the corresponding Round.
Output T$_{\#}$ indicates Output Transformation,
ICTOT$_{\#}$ indicates IntermediateCipher text of the Output Transformation.

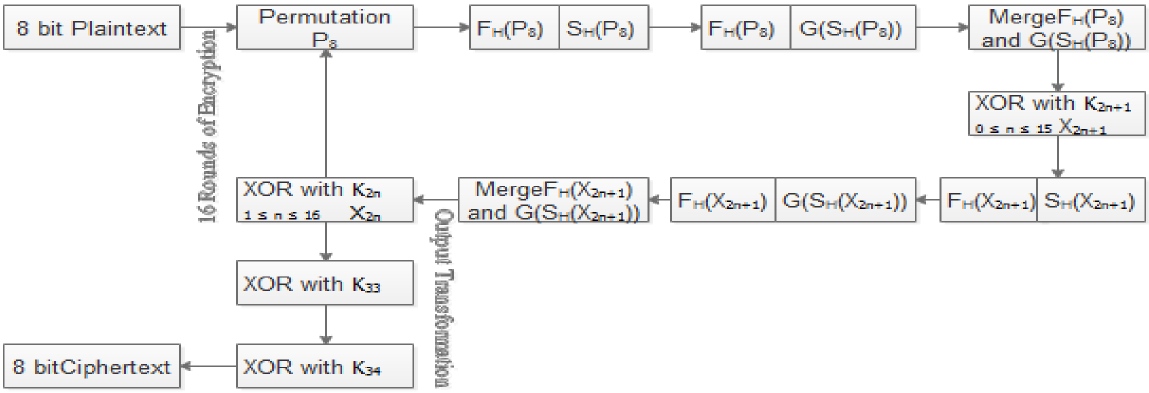

Fig 2. Detailed execution of one round of encryption in UES

Where F$_{H}$: First Half
S$_{H}$: Second Half
G: Gray code

3.3 Decryption process

The process of un-encrypting the message mwith proper key(s) k and decryption algorithm D in such a way that the human or computer can understood the message termed as decryption, which generally represented as message$m = \boldsymbol{D}(k, c)$[4].Here the process starts by considering the 8 bit cipher text as an input and applying the reverse output transformations, there after it undergoes 16 rounds of decryption using 32 blocks of key of 8 bits each.Detailed execution of decryption and one round of decryption are illustrated in the Fig3 and Fig4 respectively.

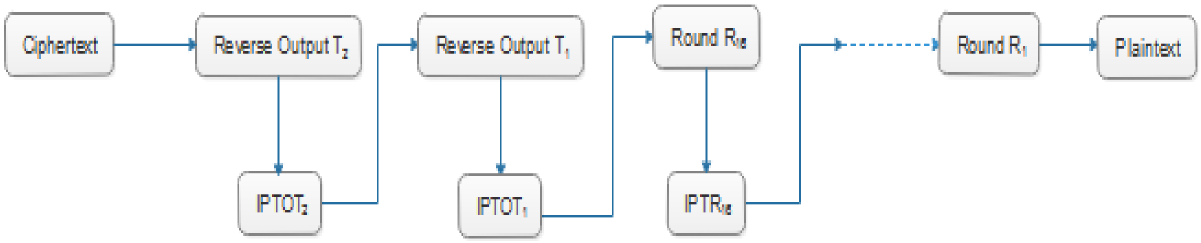

Fig 3. Decryption process of UES

Where Reverse Output T$_{\#}$:Reverse Output Transformation.
IPTOT$_{\#}$:Intermediate Plaintext corresponding to Output Transformation.
IPTR$_{\#}$:Intermediate Plaintext corresponding to Round number.

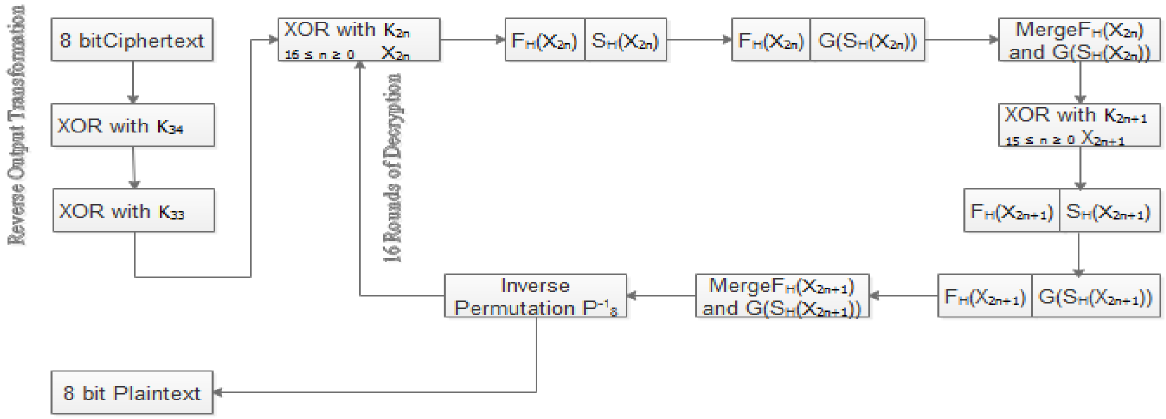

Fig 4. Detailed execution of one round of decryption in UES

Where F_H: First Half
S_H: Second Half
G: Gray code

4. Strength and Cryptanalysis of the UES Cryptosystem

The increase in the security strength of the cryptosystem is based on the notion that deciphering must be a tough task to the intruder without having knowledge about the secret key and its design where the key size plays a fundamental role[1].Here we have used 272 bit key which makes the algorithm free from the at most vulnerabilities. Cryptanalysis is the study of how differences in plaintext or key can affect the respective cipher, the results are tabulated in the table3. Here is the basic criteria to judge the strength of the algorithm. The criterion and its respective justification regarding our algorithm are mentioned in the points 'a' through 'g'.

a) The plaintext cannot be derived from the cipher text without knowing the key [9]. As the minor change in the plaintext or key results significant difference in the cipher text, deriving the plaintext without having knowledge about the key is impractical.
b) No other attack over the cryptosystem should better than the brute-force attack [9]. As the UES algorithm uses 272 bit key, there could be 2^{272} possibilities to crack the key, it seems that the brute-force attack is impractical and no other attack can pushover it.
c) The algorithm should satisfy the Strict Plaintext Avalanche Criterion with an acronym SPAC i.e., with a fixed key and a minor change in the plaintext should result the significant changes in the cipher text [9]. We have analyzed this criterion and the results are tabulated in the table3.
d) The algorithm should satisfy the Strict Key Avalanche Criterion with an acronym SKAC i.e., with a fixed plaintext and a minor change in the key should result the significant changes in the cipher text [9]. We have analyzed this criterion and the results are tabulated in the table3.
e) The algorithm should contain set of permutations as part of the encryption and decryption [9]. As we have used permutation of the 8 bit message and inverse permutation of the same in encryption and decryption, the algorithm is justified over this criteria.
f) The generated cipher text and the considered plaintext or vice versa should be of same length [9]. The detailed description of one round encryption and decryption described in figures 2 and 4 states the length of the plaintext and cipher text are same.
g) Any possible key in the algorithm should produce the strong cipher [9]. As the developed algorithm is following the Strict Key Avalanche Criterion and the encryption has undergone multilevel cipher rounds, we can say that all the possible keys can generate the strong ciphers.

TABLE3. Results of cryptanalysis under SPAC and SKAC

SPAC				SKAC			
Fixed key and change in plaintext				Fixed plaintext and change in key			
Round Number	No. of bits changed in the Cipher text	Round Number	No. of bits changed in the Cipher text	Round Number	No. of bits changed in the Cipher text	Round Number	No. of bits changed in the Cipher text
1	6	9	5	1	3	9	5

2	5	10	4	2	4	10	4
3	5	11	6	3	3	11	5
4	2	12	3	4	3	12	3
5	5	13	5	5	5	13	5
6	4	14	4	6	4	14	4
7	6	15	7	7	5	15	6
8	7	16	6	8	6	16	6

5. Complexity Analysis of the UES Cryptosystem

The time complexity of an algorithm signifies the total amount of time taken by it to run as a function considering the length of the input as n. Big Oh is the most commonly used asymptotic notation to represent the time complexity of an algorithm, which excludes the coefficients and lower order terms. For example if the time taken by the algorithm to all inputs of size n is at most $2n^3+3n^2+n+1$, the asymptotic time complexity is given as $O(n^3)$[10].In another instance if the time complexity of the consecutive steps in an algorithm are $O(n^3)$,$O(n^2)$,O(n), then the asymptotic time complexity is given as $O(n^3)$ which could be upper bound among all the three. The complexity analysis of UES algorithm is measured in three different categories called key generation, encryption and decryption. The theory of complexity analysis is briefly described in sections 5.1, 5.2, 5.3 respectively.

5.1 Complexity analysis of the key generation process

The key generation process of the UES algorithm holds the series of operations like selection of prolic number and representing it in binary, generating gray code sequence to make it as 272 bit key and dividing that key in to 34 blocks is being done with the complexities of O(n), O(n), $O(n^2)$ respectively. Finally the time complexity of this section is given as $O(n^2)$, which is the upper bound among three.

5.2 Complexity analysis of the Encryption process

The encryption process of the UES holds the common complexity of O(n) for the operations like representing the ASCII value of the plaintext in binary, permutation, binary to gray code conversion and$O(n^2)$ for dividing 8 bit in to two 4 bits, XOR operations and O(2n) for merging the two 4 bits to 8 bits. Finally the time complexity of this section is given as $O(n^2)$, which is the upper bound among three.

5.3 Complexity analysis of the Decryption process

The decryption process of the UES holds the common complexity $O(n^2)$ for dividing 8 bit in to two 4 bits, XOR operations, O(n) for the operations like representing the ASCII value of the plaintext in binary, permutation, binary to gray code conversion and O(2n) for merging the two 4 bit binary codes to 8 bits .The time complexity of UES decryption is given as $O(n^2)$.

6. Conclusion and future scope

The concept of cryptography is playing a vital role in the present era where the secure data transmission is highly needed in the areas like banking, army and government. In this regard we proposed a new symmetric stream cipher cryptography algorithm with a title Ultramodern Encryption Standard which primarily focus on handling sensitive data and providing secure data transmission. The strength of this algorithm is analyzed over differential cryptanalysis ensuring that SPAC and SKAC are satisfied. The binary-gray code conversions and the multilevel cipher rounds used in this algorithm enhances the security such that an intruder cannot intercepts the message and the results revealed that this algorithm withstand over any type of attack.

The key advantages characteristics considered for this cryptosystem are extreme secure, energy efficient, more power and relatively fast. In contrast sharing of keys is the disadvantage, but the binary-gray code analysis described in the section 3.1.1 can overcome up to an extent. Further the cryptosystem can be enhanced by modifying the key size and using tangled operations in the encryption and decryption.

References

[1]. Zirra Peter Buba& Gregory MakshaWajiga.: Cryptographic Algorithms for Secure Data Communication. In: *International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (2): 2011.*

[2]. A. Kahate, *Cryptography and Network Security (2nd Ed.). New Delhi: Tata McGraw Hill, 2008.*

[3]. Wikipedia, https://en.wikipedia.org/wiki/Category:Cryptographic_attacks.

[4]. Delfs, Hans &Knebl, Helmut (2007). *"Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.*

[5]. Mohd Zaid WaqiyuddinMohdZulkifli, Attack on Cryptography, April 2008.

[6]. Benjamin Aziz, Geoff Hamilton: *Detecting Man-in-the-Middle Attacks by Precise Timing*. *2009 Third International Conference on Emerging Security Information, Systems and Technologies, 978-0-7695-3668-2/09 © 2009 IEEE.*

[7]. https://simple.wikipedia.org/wiki/Chosen-ciphertext_attack.

[8]. Eli BihamAdi Shamir*: Differential Cryptanalysis of the Data Encryption Standard, December 7, 2009.*

[9]. Norman D. Jorstad.: *Cryptographic Algorithm Metrics, January 1997.*

[10]. Michael sipser, *Introduction to the theory of Computation (Second Edition).*