A NEW APPROACH TO THE DATA SECURITY USING MODERN ENCRYPTION STANDARD

[1]Rama Krushna Rath, [2]Hema S, [3]Manohar M, [4]Neeraj Ch, [5]Varma IVSN
[1] Assistant Professor, Department of Computer Science and Engineering
[2,3,4,5] UG student, Department of Computer Science and Engineering
[1,2,3,4,5]Godavari Institute of Engineering and Technology, Rajahmundry, Andhra Pradesh, India.

Abstract

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. The present work focus is on how one can achieve data security while transmitting from one place to another place. 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).This paper shows a new symmetric stream cipher cryptography algorithm for secure data transmission.

Key words: encryption, decryption, key generation, binary-gray-excess3 code, prolic series.

I. 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. In this regard security measures should be taken to protect the data, which in turn facilitates the secure data transmission. The security measures developed need to maintain few principles of security like confidentiality, integrity, authentication, non-repudiation.

Considering the data transmission between two entities Sender and Receiver, 'if Sender ensures that none expect Receiver gets the data is termed to be as confidentiality, integrity states that both Sender and Receiver will undergo an agreement such that, none of them would tamper the data further. 'Receiver assures that the data was sent by Sender only' designated as authentication, non-repudiation does not allow the sender of a message to refuse the claim of not sending the message. Therefore the algorithms developed should have principles of security.

Although 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 can access it, on the other side decryption is illustrated as un-encrypting the encoded text so as it can be treated as human readable format of that text. 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.

Cryptography is the science of securing data, while cryptanalysis is the science of analysing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

We proposed the encryption algorithm to encrypt plaintext to cipher text and the decryption algorithm to do the reverse. We applied the basic computing operations to design these algorithms in this study. We used the inserting dummy symbols, rotating, transposition, shifting, complement and inserting control byte to build the data and tables in the encryption algorithm. These operations are simple and easily to implement. Without knowing the data and tables of encryption, it is difficult to do cryptanalysis. In the decryption algorithm, we used these data and tables to decrypt cipher text to plaintext. We can easily apply these algorithms to transmit data in network and the data transmission is secure.

II. EXISTING SYSTEM

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. In this regard security measures should be taken to protect the data, which in turn facilitates the secure data transmission.

In this regard a new symmetric stream cipher cryptography algorithm with a title Ultramodern Encryption Standard (UES) was proposed which primarily focuses 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 cipher rounds are used in this algorithm for security, such that a third person cannot intercepts the message and the results revealed that this algorithm withstand over any type of attack.

In contrast, sharing of keys is the disadvantage; but the binary-gray code analysis can overcome up to an extent. The basic problems in the earlier proposed system are:

1. Intruder can access the plaintext with knowledge about the secret key.
2. If the message is encrypted with a particular key, and is taken compliment of that encryption will be same as that of the encryption of the compliment message and compliment key.

III. PROPOSED SYSTEM

We proposed a new symmetric stream cipher cryptography algorithm with a title Modern Encryption Standard to overcome the problems of UES algorithm which mainly focuses on handling sensitive data and providing secure data transmission. The binary-gray-excess3 code conversions and the multilevel cipher rounds used in this algorithm elaborate the security such that an intruder/third person cannot intercept the message and the results revealed that this algorithm with stand over any type of attack.

The key advantages considered for this cryptosystem are comparatively more secure, and a better key generation process. The binary-gray-excess3 code analysis can overcome attacks on key up to an extent. Key is in the form of encrypted format and combination of binary numbers; Which is formed in the process of permutations.

IV. KEY GENERATION PROCESS

The keys in practice represent the secret information stored in it, which can give access to the authorized users. The key generation of UES algorithm starts by selecting an arbitrary prolic series number following the relation Tn= n*(n+1) such that $0 \leq n \leq 255$, the ASCII character range, it is being represented as 34 bit binary code and 16 bit combinations will be formed. The binary code is converted to 34 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 and combinations are of 16 blocks of 8 bits each, which are being used as set of keys for encryption and decryption process.

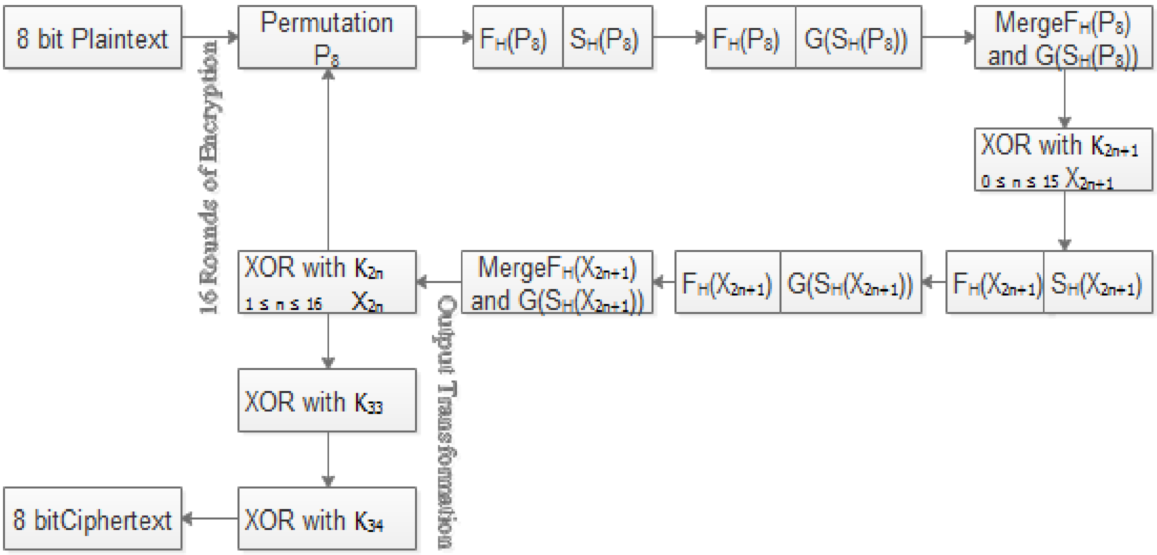
V. ENCRYPTION PROCESS

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=E(k, m).

Algorithm:

Step-1: Input: Plain Text.
Step-2: Random number generation from prolic series.
Step-3: Key Generation
Step-4: Encryption
Step-5: Output: Cipher Text

The following diagram represents the encryption process for proposed system.



Where

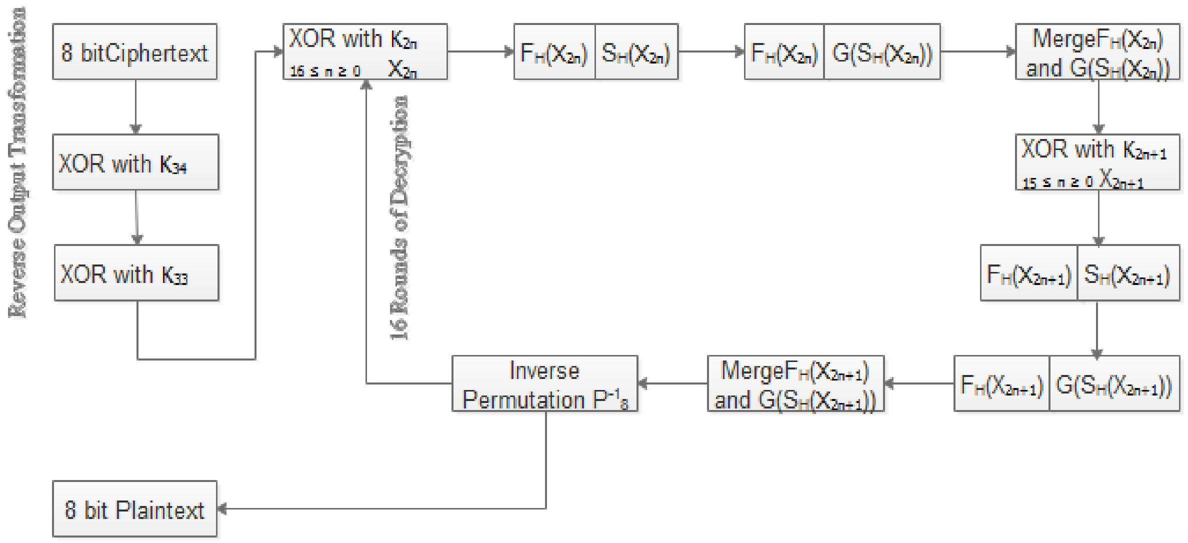
F_H: First half and
S_H: Second Half
G: Gray code

VI. DECRYPTION PROCESS

The process of un-encrypting the message '**m**' with 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=(K, c).

Algorithm:

Step-1: Input: Cipher Text.
Step-2: Input: Generated key
Step-4: Decryption
Step-5: Output: Plain Text



Where

F_H: First half and
S_H: Second Half
G: Gray code

The above decryption process is followed to get plaintext again.

VII. CONCLUSIONS AND FUTURE SCOPE

As we conclude that society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique.

DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable with high security. In this regard our proposed cryptography algorithm focuses on strong key generation process, where it will not be easy for the intruders to break. The only concern is the complexity of algorithm. Further this work can be extended by modifying the key size and using tangled operations in the encryption and decryption.

VIII. REFERENCES

1. Wikipedia, https://en.wikipedia.org/wiki/Category:Cryptographic_attacks.
2. Mohd Zaid WaqiyuddinMohdZulkifli, Attack on Cryptography, April 2008.
3. Norman D. Jorstad: Cryptographic Algorithm Metrics, January 1997.

ACKNOWLEDGEMENT

We have great pleasure in expressing our gratitude to Sri K.V.V.Satyanarayana Raju, Founder & Chairman, Chaitanya Group of Institutions, Sri K. Sasi Kiran Varma, Vice Chairman, GIET Group of Institutions, Smt. Lakshmi Raju Executive Director, GIET, for their kind support in providing us an opportunity to do research in this college.