DATA SECURITY USING LIGHTWEIGHT PATTERN

N. Subramanyan[1], K. Hari Priya[2], Y. Suma[3]

[1]Teaching Assistant, Dept. of CSE, YSR Engineering College of YVU, Proddatur, (India)

[2,3]Student IV B.Tech CSE, YSR Engineering College of YVU, Proddatur, (India)

ABSTRACT

The present generation facing so many problems in the data transfer due to lack of security. The establishment of network is not an issue but providing security for the information is a big issue in current environment. There exist various tools and methods to destroy the security. In today's world, being number of data protection algorithms are introducing, on the other hand there is a rapid growth in algorithm's to break the security. The present paper concentrates on light weight pattern representation with respect to directions along with this, to provide more flavor gray code and nibble swapping were introduced for effective protection of data.

***Keywords: Cryptography, Gray Code, Light Weight Pattern, Nibble Swapping, Security*.**

I. INTRODUCTION

Security grew to become a foremost situation in current era. The historical past of safety allows for a greater understanding of the emergence of protection. Network security has come to be an extra primary to users, companies, etc. The monstrous subject of network security is cryptanalysis. There are five major foremost security offerings. Among them the first one is confidentiality, which means that the knowledge in a laptop procedure and expertise that is transmitted are accessible just for reading by licensed ones or events. For example exhibiting, printing and other varieties of disclosure. The second one is authentication, which ensures that the origin of a message or digital record is properly identified, with an assurance that the identification just is not false. The third one is integrity, which ensures that to modify computer procedure assets and transmitted information the most effective licensed parties are ready. Fourth one is non repudiation, which requires that neither the sender nor the receiver of a message be able to deny the transmission. The fifth one is access manipulate, which requires that access to knowledge resources could also be managed by the goal approach.

For a broad sort of purposes, procedure and network technological know-how is a key science. The accessories for network protection are identity threads, security practices, identification vulnerities, identity property, security practices, design for security, security policy, and protection technologies, manage incidents and investigate asset price.

II. REVIEW ON NETWORK SECURITY

The term 'Cryptography' comes from the Greek word which means "secret (crypto) writing (grapy)". The art of remodeling/converting an intelligible message into one that is unintelligible, and that obtained message is retransformed back to its original form is called as cryptography. The cryptography [1,2] is a 5-tuple that contains (E, D, M, K, C), where E-encryption algorithm, D-decryption algorithm, M-the set of plain texts, K-the set of keys, C-the set of cipher texts;

$$E: M*K \rightarrow C \qquad (1)$$

$$D: C*K \rightarrow M \qquad (2)$$

Encryption means the process of converting plain text into cipher text and the process of converting cipher text into plain text is called as decryption [3];

$$E\text{ (key, plain text) =cipher text} \qquad (3)$$

$$D\text{ (key, cipher text) =plain text} \qquad (4)$$

Encryption algorithm is an important tool in cryptography which is used to make content unreadable by all others except the meant receiver. Encryption or decryption methods fall into two types. One is symmetric key algorithm and the one other is public key or asymmetric algorithm. In symmetric key encryption algorithms, the encryption and decryption keys are identified each to sender who sends the message and receiver who receives the message. In almost all circumstances, the encryption and decryption keys are the same. In public/asymmetric key cryptography, there are two keys namely public and private keys. In this algorithms encryption secret's made public, but it is computationally infeasible to find the decryption key without the expertise known to the receiver side.

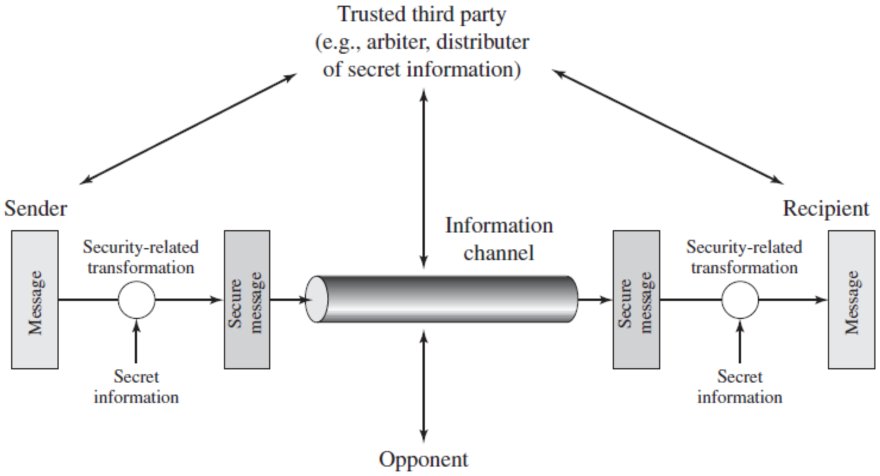

Figure 1. A model for network security system

The science of breaking ciphers is called as cryptanalysis, and the art work of devising them is mutually often called as cryptology.

2.1 History of cryptography

Along with the art of writing, the art of cryptography is considered to be born. As civilizations evolved, human beings got organized in groups, tribes, and kingdoms and this led to the emergence of ideas such as battles, powers politics and supremacy. These ideas lead to the natural use of people to communicate very secretly with only the selective recipient which in turn leads to the continuous evolution of cryptography as well.

2.1.1 The oldest cryptographic technique - Hieroglyph

The use of ‘hieroglyph’ is the first known evidence of cryptography. Some 4000 years ago, the Egyptians used to communicate by using messages written in hieroglyph cryptographic technique. This secret code was known only to the scribes who transmit messages on behalf of the kings in the oldest days. One such hieroglyph cryptographic technique is shown in Fig.2.

Figure 2. Hieroglyph-Cryptography Technique

Caesar shift cipher is the earliest roman method of cryptography, which relies on shifting the letters of a message by an agreed number and the recipient who receives this message would then shift the letters of message back by the same agreed number and finally obtain the original message.

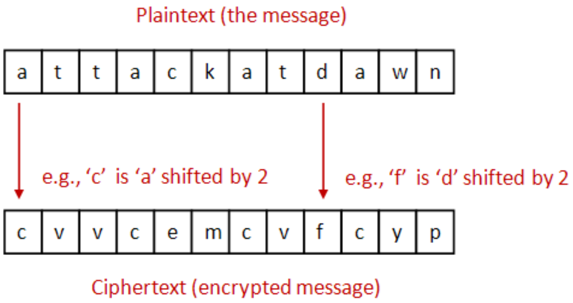
Plaintext (the message)
a t t a c k a t d a w n
e.g., ‘c’ is ‘a’ shifted by 2
e.g., ‘f’ is ‘d’ shifted by 2
c v v c e m c v f c y p
Ciphertext (encrypted message)

Figure 3. Caesar Shift Cipher

2.2 Public Key Cryptography

Asymmetric cryptography which is also known as public-key cryptography is a cryptography in which a pair of keys like public and private keys is used to encrypt and decrypt a message so that the message occurs very securely. Initially, a network user receives a public and private key pair from a specific certificate authority. Any other user who wants to send a message which is encrypted can get the intended recipient's public key from a public directory.

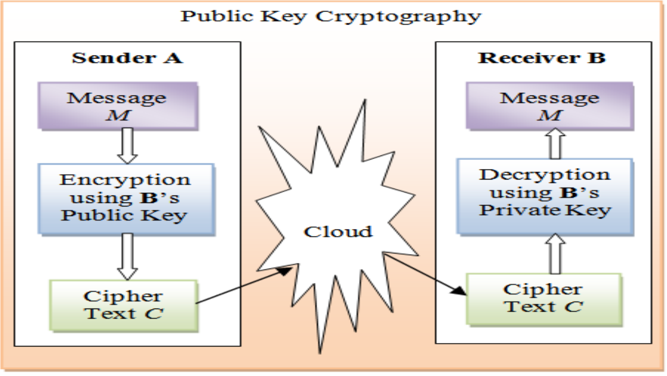

Figure 4. Public Key Cryptography

They use the specific key to encrypt the message, and they send it to the receiver. When the receiver gets the message, they decrypt it with their private key, which no one else should have access to it.

2.3 Types of intrusions

There are some basic classes of attacks which causes for slow network performance, viruses, uncontrolled traffic etc.

A. Protection threats

There are some quantities of safety attacks that can be the rational of a network security assault. Among them most important security attacks/threats are denial of service, dispensed denial of service, trojan horses, viruses, malwares, spywares, unauthorized entry to the network information and assets, uncontrolled internet entry and the accidental deletion of the records.

B. Virus attack

When virus attack occurs, it penetrates the security and third party tries to pinch the information from the system. Viruses planted into the systems through some fake programs.

C. Unauthorized entry

Entry to the some community resources and data should only be allowed handiest to the approved persons.

D. Unauthorized application installations

One other important virus and network security assault prevention method is to install most effective applications of the licensed program to our network server and in all client systems.

III. PROPOSED WORK

The main aim of the proposed work is to enhance the security with lightweight pattern [4,5]. This work consist various stages with respect to encryption and decryption procedures. The first stage of this work deals with pattern oriented intermediate cipher text[6,7] generation. Further to enhance the security different operations are applied such as gray coding and nibble swapping. Fig. 5 illustrates steps involved in encryption process. Fig 6. illustrates the steps involved in decryption process.

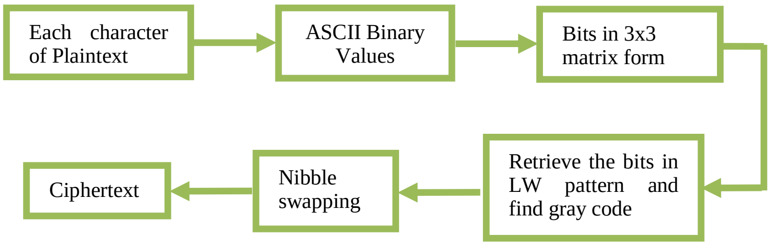
Each character of Plaintext
ASCII Binary Values
Bits in 3x3 matrix form
Retrieve the bits in LW pattern and find gray code
Nibble swapping
Ciphertext

Figure 5. Flowchart Showing Steps In Encryption

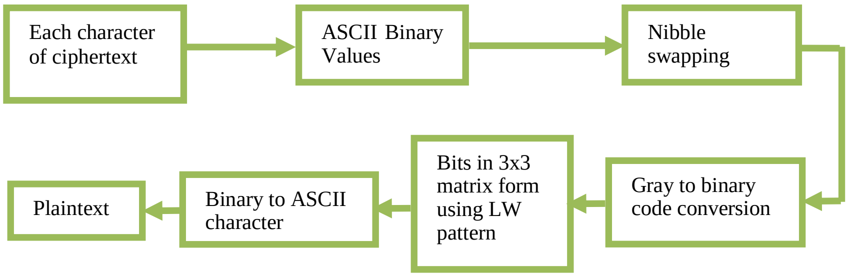
Each character of ciphertext
ASCII Binary Values
Nibble swapping
Gray to binary code conversion
Bits in 3x3 matrix form using LW pattern
Binary to ASCII character
Plaintext

Figure 6. Flowchart showing the steps in decryption

3.1 Encryption algorithm

Encryption is performed in three rounds.

Steps in Round 1 are as follows

Step 1: For each plaintext character, find the corresponding ASCII value.

Step 2: Convert the ASCII value into its equivalent binary bits.

Step 3: Arrange the binary bits in 3x3 matrix.

Step 4: Retrieve the bits in 8-directions pattern like N NE E NW W SW S SE.

Steps in Round 2 are as follows

Step 5: Find gray code for the obtained binary bits.

Step 6: Compute the decimal number for each row.

Steps in Round 3 are as follows

Step 7: Apply nibble swapping for each decimal number.

Step 8: The final cipher is obtained by converting result into its equivalent ASCII.

3.2 Decryption algorithm

Decryption is performed in three rounds.

Steps in Round 1 are as follows

Step 1: For each ciphertext character, find the corresponding ASCII value

Step 2: Apply nibble swapping for the obtained cipher text.

Step 3: Find the appropriate binary equivalent for it.

Steps in Round 2 are as follows

Step 4: Perform gray to binary code for the above resulted binary bits.

Steps in Round 3 are as follows

Step 5: Arrange the bits in 3x3 matrix using 8-directions pattern.

Step 6: Retrieve the bits according to the lightweight pattern .

Step 7: Convert the binary bits into its equivalent decimal values.

Step 8: The original plain text is obtained by finding ASCII value.

3.3 Example for encryption algorithm

Given plain text is: CRYPTOGRAPHY

Table 1. Encryption Example

Plaintext Character	ASCII Value	Binary equivalents	After Applying LW Pattern	Gray code	After Nibble swapping	Ciphertext Character
C	67	01000011	11000010	10100011	58	:
R	82	01010010	10001010	11001111	252	ü
Y	89	01011001	01101010	01011111	245	õ
P	80	01010000	00001010	00001111	240	ð
T	84	01010100	00011010	00010111	113	q
O	79	01001111	11110010	10001011	184	¸
G	71	01000111	11010010	10111011	187	»
R	82	01010010	10001010	11001111	252	ü
A	65	01000001	01000010	01100011	54	6
P	80	01010000	00001010	00001111	240	ð
H	72	01001000	00100010	00110011	51	3
Y	89	01011001	01101010	01011111	245	õ

Final ciphertext is ": ü õ ð q ¸ » ü 6 ð 3 õ"

3.4 Example for decryption algorithm

Given ciphertext is: : ü õ ð q ¸ » ü 6 ð 3 õ

Table 2. Decryption Example

Ciphertext Character	ASCII Value	After nibble swapping	After gray to binary code	After Applying LW Pattern	Decimal values	Plaintext Character
:	58	163	11000010	01000011	67	C
ü	252	207	10001010	01010010	82	R
õ	245	95	01101010	01011001	89	Y
ð	240	15	00001010	01010000	80	P
q	113	23	00011010	01010100	84	T
¸	184	139	11110010	01001111	79	O
»	187	187	11010010	01000111	71	G
ü	252	207	10001010	01010010	82	R
6	54	99	01000010	01000001	65	A
ð	240	15	00001010	01010000	80	P
3	51	51	00100010	01001000	72	H
õ	245	95	01101010	01011001	89	Y

Final plaintext is "CRYPTOGRAPHY"

IV. ADVANTAGES

- The number of ways to represent the intermediate cipher text at round1 is 8!.
- To enhance the security, gray code is applied for the result of round1.
- Nibble swapping is added as one of the flavor to enhance the security.

V. CONCLUSION

Security is a complicated topic in current tendencies. In this paper, direction oriented encryption is proposed. The proposed algorithm having a lightweight secret key which produces an intermediate cipher text. Two extra operations are carried out to enhance the protection. Apart from this, unauthorized user can not be ready to decrypt the message within the feasible amount of time despite of figuring out the key pattern. This algorithm avoids man in the middle of intrusions. Moreover, the proposed system will also be applied with cloud computing, uni-code system, smartcard protection and steganography.

REFERENCES

[1] Darga, Paul T., Liffiton, Mark H., Sakallah, Karem A. and Markov. Igor L., Exploiting structure in symmetry detection for cnf. DAC, pages 530–534. ACM, 2004.

[2] Ammar, A., El Sherbini, A. , Ashour, I. , Shiple, M., Random data encryption algorithm (RDEA), Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National, 15-17 March 2005.

[3] Junttila., Tommi and Kaski. Petteri, Conflict propagation and component recursion for canon-ical labeling. Theory and Practice of Algorithms in (Computer) Systems, Lecture Notes in Computer Science, 6595:151–162. Springer Berlin / Heidelberg, 2011.

[4] "Analysis and Review of Encryption and Decryption for Secure Communication", International Journal of Scientific Engineering and Research (IJSER) Vol.2 Issue.2, Feb-2014.ISSN (online) 2347-3878.

[5] "Recommendation for Cryptographic Key Generation", National Institute of Standards and Technology Special Publication 800-133 Natl. Inst. Stand. Technol. Spec. Publ. 800-133, 26 pages (December 2012)

[6] Agrawal., Monika, Mishra., Pradeep, A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science & Engineering; May2012, Vol. 4 Issue 5, p877.

[7] Govind Prasad Arya, Aayushi Nautiyal, ashish pant,Shiv Singh & Tishi Handa, "A cipher design with automatic key generation using the combination of substitution and transposition techniques and basic arithmetic and logic operations," the SIJ Tansactions on computer science engineering & its applications(CSEA), Vol. 1,No. 1,March-April 2013.