IJCAT - International Journal of Computing and Technology, Volume 1, Issue 8, September 2014
ISSN: 2348 - 6090
www.IJCAT.org

A Novel Concept to Enhance Security

[1] Fahim Multani, [2] Gajendra Singh

[1] M.Tech. Scholar CSE Dept., SSSIST, Sehore (M.P.), India

[2] HOD CS/IT Dept., SSSIST, Sehore (M.P.), India

Abstract - In cryptographic application, the data sent to a remote node are encrypted first at the sender node use a key then it encrypt to data and send to the other node called receiver node. This is the method where the attacker or hacker will not have the original key which is necessary to get the original information and thus the hacker or attacker will be incapable to do something with the session. In this paper, A new concept for encryption is proposed and proposed concept is based on the transformation of a text file into word file on both client and server node. We analyze proposed method by calculating the number of all possible key permutations. And the expected results are showing the effectiveness of the proposed method.

Keywords **- Information security, Encryption, Decryption, Cryptography, Symmetric, Asymmetric, Key, Algorithm.**

1. Introduction

In the present scenario where information and communication is the indispensable composition of human activities, where men and technology must communicate or share information in order to make decisions; it therefore behooves that this composite essence of humans should be protected and managed to ensure its sustainability, integrity, accuracy.

Security services [4]

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Encryption techniques have become the immediate solution to protect information against third parties. These techniques required that data and information should be encrypted with some sort of mathematical algorithm where only the party that shares the information could possible decrypt to use the information.

How Encryption Works: Encryption (see Figure 1) uses a systematic or step-by-step procedure called an algorithm to convert data or the text of an original message, known as plaintext, into cipher text, its encrypted form [9]. Cryptographic algorithms normally require a string of characters called a key to encrypt or decrypt data. Those who possess the key and the algorithm can encrypt the plaintext into cipher text and then decrypt the cipher text back into plaintext [12].

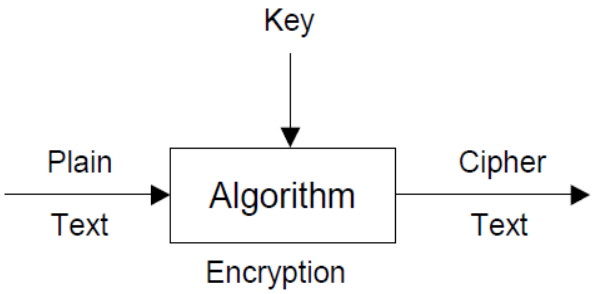


Figure 1 Basic Encryption concepts

What is Cryptography: Cryptographic systems are characterized along three independent dimensions:

- The type o operations used for transformation plaintext to cipher text. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged [2] The fundamental requirement is that no information should be lost.

- The number of key used. If both the sender and receiver are using the same key then it is refereed as symmetric, single-key, secret-key or conventional encryption. If sender and receiver

each use a different key, the system is refereed as asymmetric, two-key or public-key encryption.

The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block [5]. A stream cipher processes the input elements continuously, producing output one element at a time.

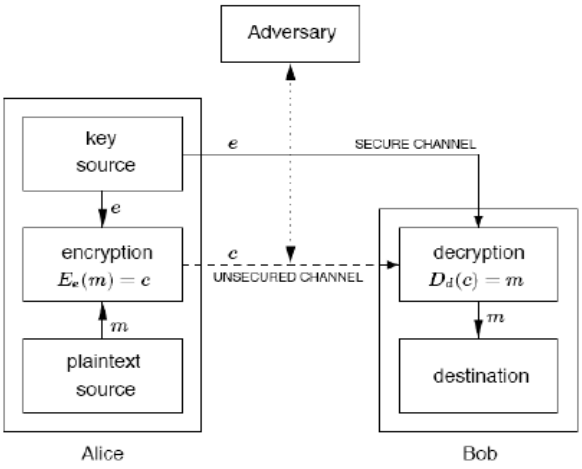
Cryptanalysis: Cryptanalysis is the art of analyzing cipher text to extract the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers. Understanding the process of code breaking is very important when designing any Encryption system.

The science of cryptography has kept up with the technological explosion of the last half of the 20th century [12]. Current systems require very powerful computer systems to encrypt and decrypt data. While cryptanalysis has improved as well, some systems may exist that are unbreakable by today's standards.

Problem of Encryption Techniques: Although, encryption mechanisms make information unreadable. Therefore, no third parties, including server administrators and others, have access to plain text version of transmitted information through public networks such as internet, but the following are the problems encountered or associated with encryption techniques [11, 12].

Symmetric Encryption: In symmetric encryption (see Figure 2) also known as the Private Key Method or encryption, a single key is used for encrypting and decrypting the data. This type of encryption is quite fast, but has a severe problem. The inherent weakness of this method is mostly the requirement of a key exchange between communications partners [3].

In other words, in order to share a secret with someone, they have to know your key. This implies a very high level of trust between people sharing secrets, if an unscrupulous person has your key or if your key is intercepted by a spy they can decrypt all the messages you send using that key[8, 9]. However, Asymmetric encryption solves the trust problem inherent in symmetric encryption by using two different keys: a public key for encrypting messages, and a private key for decrypting messages. This makes it possible to communicate in secrecy with people you don't fully trust. If an unscrupulous person has your public key, who cares? The public key is only good for encryption; it's useless for decryption. They can't decrypt any of your messages! However, asymmetric encryption is very slow. It's not recommended for use on more than roughly 1 kilobyte of data [12]



. Figure 2: A two party symmetric encrypted communication scheme

Asymmetric Methods: In Asymmetric encryption (see Figure 3) also known as the Public Key Method, it uses two different keys: the private key and public key. The public key is distributed freely and the private key is known only to the owner of a key. The two keys have a (mathematical) relationship. However, for obvious reasons, calculation of a private key on the basis of the public key must be impossible or at least not feasible. Both keys have different functions depending on the application at hand. In the case of data encryption, data is encoded using the public key. The private key is required in order to decrypt the message. The private key can also be used to generate digital signatures, which can later be verified using the public key [12].

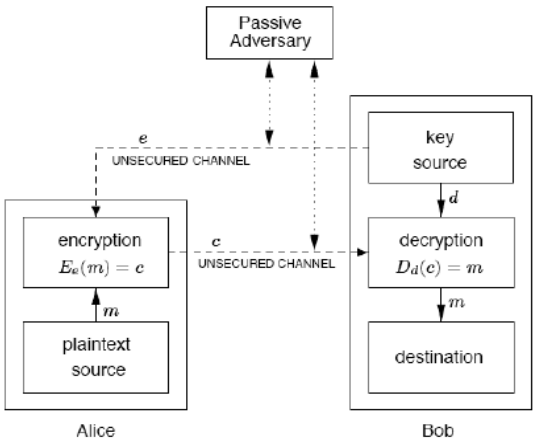


Figure 3: Public-key cryptography Courtesy of the Handbook of Applied Cryptography

Rest of the paper are as follow: part-II Present study of earlier presented technique in terms of literature survey with analysis of earlier presented techniques, part-III, this part presents the concept on new approach in terms of proposed concept, part-IV this part presents the expected

out come on various parameter of proposed concept followed by conclusion.

2. Literature Survey

In [6] a method presented for hiding any encrypted secret message inside a text/ASCII or Microsoft word document file, by manipulating the blank/white space characters of a cover file. Initially the secret message is encrypted using Modified Generalized Vernam Cipher Method. For hiding secret message inside any ASCII file they presented method in which the bits of each character of secret message file is inserted in place of eight randomly selected blank space characters of the cover file. For inserting bit-0 they choose one blank space inside the cover file and to embed bit-1 they convert the blank space to ASCII code 160 and this is will show as blank in the screen. To embed bit-0 and bit-1 in cover file they select the blank spaces from cover file in random manner. The randomly selected blank characters are read from cover file correspond to positions of a shuffled offset matrix starting from a certain base address in cover file. The offset matrix is randomized using the randomization method of the previously published MSA encryption algorithm.

The randomized embedding of message in a cover file gives an additional layer of security over the encryption. In [1] authors have introduced an integrated symmetric key cryptographic method DJMNA which combine two independent methods (i) Modified Generalized Vernam Cipher (MGVC) method and (ii) DJSA method which is an extension of MSA method. The Generalized Vernam Cipher algorithm extends text encryption to any type of data encryption.

This is done by using ASCII code of all characters (0-255). This modified version of Generalized Vernam Cipher uses “feedback” effect and also reverses the file while encryption. This makes the encryption process very hard to decrypt by using any brute force method. It was found that the encrypted text has huge difference for similar plaintexts having minor difference even for the same text-key. From this text key two randomized matrices are generated. The elements of this matrix decides the order of application of DJSA and MGVC methods.

In [7] the present work authors have proposed a symmetric key method where authors have used a random key generator for generating the initial key and that key is used for encrypting the given source file. In that method basically a substitution method where they take 4 characters from any input file and then search the corresponding characters in the random key matrix file after getting the encrypted message they store the encrypted data in another file. For searching characters from the random key matrix they have used a method which was proposed by author in MSA algorithm. In the presented method authors have the provision for encrypting message multiple times. The key matrix contains all possible worlds comprising of 2 characters each generated from all characters whose ASCII code is from 0 to 255 in a random order.

The pattern of the key matrix will depend on text key entered by the user. Authors have proposed an algorithm to obtain randomization number and encryption number from the initial text key. Authors have given a long trial run on text key and found that it is very difficult to match the above two parameters from 2 different Text key which means if someone wants to break encryption method then he/she has to know the exact pattern of the text key.

To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to apply 65536! trial run and which is intractable. Authors have applied that method on possible files such as executable file, Microsoft word file, excel file, access database, fox-profile, text file, image file, pdf-file, video file, audio file, oracle database.

In [2] this paper the authors have introduced a new advanced symmetric key cryptographic method called NJJSAA. The authors introduced new bit manipulation method for data encryption and decryption of any file. Authors have already developed some technique where authors have used some randomized key matrix for encryption and decryption methods. In the present work the authors have used a bit manipulation method which include bit exchange, right shift and XOR operation on the incoming bits.

To exchange bits the authors used a randomized key matrix of size (16x16). The present method allows the multiple encryptions and multiple decryptions. To initiate the encryption process a user has to enter a text-key which may be maximum of 16 characters long. From the text-key the authors have calculated randomization number and the encryption number. A slight change in the text-key will change the randomization number and the encryption number quite a lot.

Multiple encryption using bit exchange, bit right shift and XOR operations makes the system very secured. The present method is a block cipher method and it can be applied to encrypt data in sensor network or in mobile network. The advantage of the present method is that one can apply this method on top of any other standard algorithm such as DES, AES or RSA [11]. The method is suitable to encrypt any large or small file

3. Analysis

Each of the above specified techniques is having their own strong and weak points. In order to apply an appropriate technique in a particular application it is required to know these strong and weak points. Therefore the comparison of these techniques based on several features is necessary. Some of these points under which the cryptosystems can be compared are described below:

- Avalanche effect: A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. But in the earlier presented techniques this property are not fully satisfied.

- Memory required for implementation: Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible. This is important attribute for any techniques because it's related to the efficiency of the techniques and it is observed that earlier presented techniques suffer from this problem that means they required large memory during processing.

- Simulation time: The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired. It's already know that execution time is the prime attribute of any encryption and decryption technique which is direct relate with the efficiency of the technique. But from the analysis of earlier presented techniques it is observed that too much execution time are taking by these technique.

- Key: According to earlier presented techniques has some improvement in the field of key value which used during encryption process and decryption process. These techniques are using a database of large size in the form of traditional file. Due to this reason these techniques produced low results in terms of efficiency. Some other points are also there where improvements are required like understandability of the techniques and easy implementation which is not in earlier presented techniques because of the structure of the techniques.

3. Proposed Concept

Symmetric key techniques are using only single key during encryption and decryption at both end. [10], these types of techniques are theoretically and practically simple. This leads to a numeral of advantages. Performance is comparatively far batter. Also, the study and analyzing of symmetric techniques is relatively systematic. The only one disadvantage of symmetric key technique are key exchanging problem but there are many techniques which are working for key exchange between parties. There are two main aspects of a symmetric key technique system. The first is the encryption process and the second is the uses of private key with encryption process.

The techniques itself is some kind of revolution that takes information, also known as plaintext, and a private key and outputs encrypted text also known as cipher text. This encrypted text and the same private key should also be capable to be revolution again to recuperate the plaintext. The protection of such techniques is evaluated on how much the revolution depends on the private key to recover the plaintext. A strong technique should depend completely on the private key for revival in any sensible situation. It should be renowned that any symmetric key technique, in fact any keyed techniques, is susceptible to brute force attacks while some more than others.

The Proposed Technique is a symmetric key based encryption process which enhancing to the version of earlier encryption process. The proposed technique overcomes the security limitations of previous algorithm by accumulation innovative confusion thus ensuing in strong cryptographic techniques. The proposed technique also ensures that encryption and decryption time. The architecture in the figure 4 and 5 shows the process of encryption and decryption:

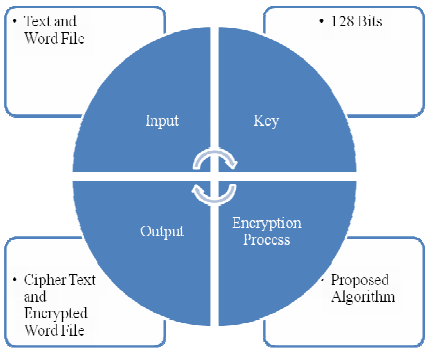


Figure 4: Architecture diagram for encryption

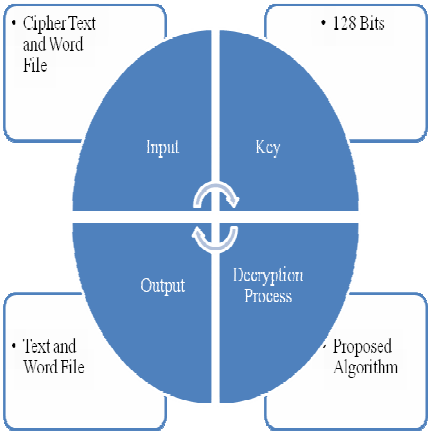


Figure 5: Architecture diagram for decryption

3.1 Description of Proposed Architecture:

Proposed Technique Attributes: Following is the attribute of the proposed technique

- **Reliability and Fault Tolerance:** The Proposed technique should be reliable and of enterprise quality.
- **Security:** The Proposed technique should be contain strong cryptographic algorithm,
- **Accessibility:** The accessibility of proposed technique should not dependent to any extra license. Propose technique is a research objective. Thus, every person is able to use the proposed technique with any operating systems.
- **Consistency and Correctness:** The requirement of proposed concept should be consistent and correct.
- **Performance:** The requirements of the computers do not important for proposed technique. It can be significant for large files or else, its performance is predictable quick sufficient

4. Expected Outcome

Hear proposed concept will implement on high level language. In this proposed concept evolution factors will be execution time [10] in, throughput, CPU uses; RAM uses [4, 8 & 10]. Basically proposed algorithm will perform encryption and decryption on text data of different size with the help of private key. In the experiments, the system will encrypts/decrypt a various size of text file.

Encryption/Decryption Time, Throughput, CUP and RAM Uses for Text File: - Here, "The Proposed Algorithm (PA)" will be implement on a numeral of data records. Expected analysis on Encryption/Decryption time, RAM Utilization, CPU Utilization and throughput of different size of Text files shown in table 1 to 4 respectively

Table 1: Expected Text Encryption/Decryption Analysis of Proposed Algorithm

S.NO	FILE SIZE	Proposed Algorithm
	in KB	Execution Encryption Time in Second(Approx)
1	1	Low
2	2	Low
3	3	Low
4	4	Low

Table 2: Expected Throughput Analysis of Proposed Algorithm

S.NO	FILE SIZE	Proposed Algorithm
	in KB	Throughput(Approx)
1	1	High
2	2	High
3	3	High
4	4	High

Table 3: Expected CPU Uses of Proposed Algorithm

S.NO	FILE SIZE	Proposed Algorithm
	in KB	CPU Consumption (Approx)
1	1	High
2	2	High
3	3	High
4	4	High

Table 4: Expected RAM Uses of Proposed Algorithm

S.NO	FILE SIZE	Proposed Algorithm
	in KB	RAM Uses in Second (Approx)
1	1	Low
2	2	Low
3	3	Low
4	4	Low

5. Conclusion

This part presents the expected performance of proposed concept. The proposed concept is based on symmetric key techniques. Where at both end same key will used. There is some performance parameters used during expected results analysis.

First; there is no important dissimilarity when the results displayed either in base 64 encoding or hexadecimal base encoding. Secondly; in the case of varying size of data, it concluded that proposed concept can be better than earlier presented techniques. Finally in the case of varying size of key which is related with security of the techniques that means larger key produced good security but too large can be a causes of poor efficiency in terms of execution time. In this paper it is surveyed and designed security concept used for securing information which is transferring over public network in open way. The concept is the calculation of selected parameters in cryptography.

We surveyed different schemes that were proposed for selected parameters in cryptography, for its optimism. We have also analyzed the time complexity and expecting that proposed concept will be batter then the other encryption algorithm.

References

[1] D Das, Je Nath, M Mukherjee, N, A Nath and D Das "An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm" Published in IEEE World Congress on Information and Communication Technologies (WICT), 11-14 Dec. 2011 Page(s):1199 – 1204.

[2] A Nadeem., "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, 2006on Communication Systems and Network Technologies (CSNT), 3-5 June 2011 Page(s):125 - 130

[3] J Nath, S Das, S Agarwal and A Nath "Advanced Steganographic Approach for Hiding Encrypted Secret Message in LSB, LSB+1, LSB+2 and LSB+3 Bits in Non standard Cover Files" International Journal of Computer Applications (0975 – 8887) Volume 14– No.7, February 2011

[4] D Salama, Al Minaam, M. Hatem, A Kader, and M M Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010

[5] R. Venkateswaran Dr. V. Sundaram "Information Security: Text Encryption and Decryption with poly substitution method and combining the features of Cryptography" International Journal of Computer Applications (0975 – 8887)Volume 3 – No.7, June 2010

[6] J Sanyal, R Ray, A Nath, D Das, "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm" Published in IEEE International Conference on Communication Systems and Network Technologies (CSNT), 11-13 May 2012 Page(s):889 – 893

[7] J Nath, N Khanna, J James, A Nath , S Chakraborty and A Chakrabarti" New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm" Published in IEEE International Conference

[8] D Chatterjee, J Nath, S Dasgupta, A Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" Published in IEEE International Conference on Communication Systems and Network Technologies (CSNT), 3-5 June 2011 Page(s): 89 - 94

[9] A Kaushik, M Bamela and A Kumar "Block Encryption Standard for Transfer of Data" Published in International Conference on Networking and Information Technology (ICNIT), 2010 11-12 June 2010 Page(s):381 - 385

[10] Y Wang and M Hu "Timing evaluation of the known cryptographic algorithms "2009 Published in International Conference on Computational Intelligence and Security, 2009. CIS '09. 11-14 Dec. 2009 Page(s):233 - 237

[11] Md. N Islam, Md. M H Mia, M F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Published in Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 6-8 Aug. 2008 Page(s): 291 - 294

[12] G C. Kessler, 1998, An overview of cryptography, [online]:http://www.garykessler.net/library/crypto.html ,date accessed: 23/07/06