Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.850 – 856

RESEARCH ARTICLE

A DNA Based Scheme to Improve SMS Cryptography

Shivani[1], Mamta Sachdeva[2]

Student, MTech(CSE), South Point Institute of Technology & Management, Sonepat, Haryana
nirun788@gmail.com

Associate Professor, Department of Computer Science
South Point Institute of Technology & Management, Sonepat, Haryana
get_mamta@rediffmail.com

Abstract : Mobile Cryptography provides the secure information transmission of message. In this present work, A DNA enabled approach is defined to improve the cryptography. In this work, a two stage model is presented to improve the DNA Cryptography. In the first age of work, the DNA based key generation is performed and later on information transformation is performed using DNA. The work is applied on Mobile SMS. The analysis of work is done under efficiency parameter to analyze the time taken in cryptography process. The obtained results shows the effective communication of information for mobile SMS.

Keywords : DNA, Cryptography, SMS, Secure Transmission

I. INTRODUCTION

Cryptography enables the data communication between two persons or between a group to provide secure communication over the network. This kind of communication not only prevents the unauthorized access over the network but also maintains the data integrity. The authentication is provided by digital signature or digital certificates. At the basic level cryptography approaches are divided in two main categorized based on number of keys involved in communication. These approaches are called private key cryptography and public key cryptography[1][2].

A) Symmetric Key Cryptography

This kind of cryptography approach is also called private key cryptography. As the name suggested in this cryptography approach only single key is involved to enable the encoding and decoding process. It means same key is used to perform data encryption and to retrieve the data back from cipher text. At the earlier stage, this kind of cryptography not looks

stronger as the complete security depends on single key. But there are number of cryptography algorithms comes under symmetric key cryptography that increases the data integrity by using the larger key size and number of encoding level in the algorithmic approach. This is the most traditional type of cryptography, in which the key information is common for both sender and receiver. In such system, the sharing mechanism of key requires some effective approach. Single key is here defined to perform data encoding and decoding. This single key is able to provide the reliable communication over the network[3][4][5]. The cryptographic mechanism supported by this approach is shown in figure 1

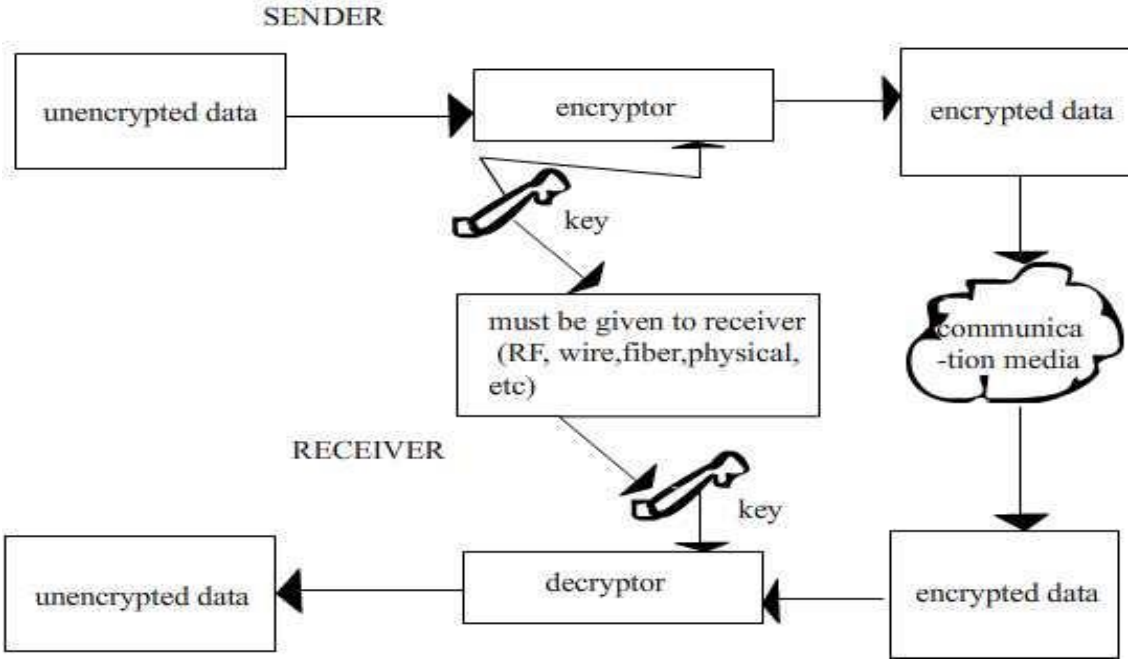

Figure 1 : Symmetric Key Cryptography

As figure shows, the sender is having the raw information to transfer over the network. This raw information can be available in different media types. These media types can be textual information, image, videos etc. To perform the cryptography, the approach requires some algorithm called encryptor and the key. This key is symmetric key shared between the sender as the receiver. As the cryptography algorithm is applied, the information is encoded to the cipher data form or called encoded information. Now this encoded information is transferred over the network. As the receiver receives the information it is in encoded form. Now the decryptor is applied here to get the actual information back. The decryptor uses the decoding algorithm and the same symmetric key to get the information data back. The security of these kind of algorithm depends on three main vectors called cryptography algorithm, key size and way to share the key. There are number of symmetric key cryptography algorithms such as DES (Digital Encryption Standard), Triple DES, AES (Advanced Encryption Standard) etc[6][7][8]. This algorithm provides the high level information security.

B) DNA Sequencing

DNA itself defines the instruction code for genetic and by using it the protein structure of any living thing can be constructed or recomposed. Each DNA sequence ia based on four different bases called Adenine (A), cytosine (C), guanine (G) and Thymine (T). DNA sequence study is helpful to do the structural change or property change or behavior change for a particular living thing. To identify the characteristic match or to identify the similarity between two living things in terms of characteristics or the functionality or behavior, it is required to analyze them respective to their DNA sequence. Each DNA sequence is defined as the large information group that contains all kind of information about the living things. Such as if we take the example of wheat, it contains the information about the wheat color, smell, quality etc. If we have to find a particular quality of wheat among the wheat samples, the DNA sequence match for the particular pattern can be performed. Each pattern in DNA sequence represents the existing or non-existence of some characteristics

or the behavior. But the identification of these patterns over the DNA sequence is a challenging task. In this present work, the main focus is to perform the identification of some of such patterns over the DNA Dataset Group.

In this paper, DNA based Symmetric Key cryptography approach is defined. Here, the symmetric Key is generated using DNA sequencing and DNA component based substitution is applied to perform the cryptography. In this section, the description of cryptographic algorithm is given along with exploration of public and private key cryptography. The section also defined the concept of DNA sequencing. In section II, the work defined by earlier researchers is presented. In section III, the proposed two stage model is defined to perform DNA cryptography using DNA sequence Key. In section IV, the results obtained from the work are presented and discussed. In section V, the conclusion obtained from the work is presented.

II. EXISTING WORK

Lot of work is already done by different researchers to improve the information security under different media types and under different communication system. Some of the efforts of earlier researchers are discussed in this section.

In year 2012, Ohood S. Althobaiti, discuss the relationship between cryptography and mathematics in the context of Elliptic Curve (EC). Author presents the idea of biometric signature - a new method to combine biometrics with public key infrastructure (PKI), the security can be increased using the ECC in biometric signature creation, because the private and public keys are produced without saving and sending any secret information anywhere[1]. In Year 2012, Seny Kamara defined a work on Symmetric encryption using dynamic searchable technique. The presented approach allow a client to encrypt the data in such way the search can over the data can be performed over it. Author has defined SSE based scheme to satisfy the search condition. The work presented by the author actually extend the inverted index approach in different non-trivial ways and also introduce new technique to design the SSE. Author implemented the presented scheme and conducts the performance evaluation. The presented approach is highly efficient and ready for the deployment[2]. In year 2011, Parisa Kaghazgaran presented a work on the to provide the information security in case of involvement of more than one party in encryption process. Author defined the variant of comparision problem under different input. Author presented the work in real time sitautions where the cryptography is required. Author presented the cryptography at protocol level and provide the comparative analysis on existing and modified secure protocol approach for data encoding. Author enabled the secure transmission over the network [3].
Trisha Chatterjee presented a work on the cryptographic algorithms for symmetric key cryptography. Author provided more secure approaches by modifying the existing symmetric key cryptography appraoches. The modifification is here done at cipher text generation. Author provided the new algorithm to provide the text based encoding at the frequency level analysis. Author enabled the ASCII character encoding to perform the cryptography and to convert the information one form to other. This cryptography approach is based on random key generation[4]. Another work on visual information cryptography using the DH scheme was proposed by Chao-Wen in year 2008. Author presented an improved mechanism based deffie helman approach for visual crypgraphy approach. Author used a shared key mechanism using visual cryptography. Author used the half tone shadow images to show the work implementaiton. Author implemented the work using shared key and symmeteric key approches to achieve high level security[5]. Another work on block cipher cryptography and white box cryptography to secure the data was performed byJaesung Yoo in year 2012. In this paper, Author implemented an improved AES for image encryption by using the dynamic key updation approach. Author adopted composite mode using White-Box AES and Standard AES. Presented scheme shows almost same performance with Standard AES and provides dynamic key approach effect. Moreover, it has a CPA-secure property and can be constructed for CCA-secure scheme with Message Authentication Code[6]. Wasim A Al-Hamdani defined a work on Elliptic Curve Cryptography to protect the data. Authro defined a public key based approach under the algebraic structure. The was performed on a smaller group can be used to obtain the same level of security as RSAbased. In this article a simple presentation on cryptography with focus on elliptic curve algorithm, examine its security, benefits and its functions with privacy issues[7].
A work on identity based cryptography was performed on symmetric cipher cryptography by Joonsang Baek. In this paper, as contributions to this line of research, Author construct hybrid identity-based encryption schemes which produce compact ciphertexts while providing both efficiency and strong security without resorting to the strong lengthpreserving symmetric cipher. In this paper, author defined a comparative analysis under different communication attacks to reveal the communication information and to extract the user data under different assumptions. Author provided the symmetric

key encryption under improved form[8]. Another work on Symmetric encryption with key exchange scheme to achieve the computational soundness. In this paper, Author presnted an improved mechanism for key sharing oer the network. Author defined a new improved protocol to enable the public key cryptography and to provide the secure key sharing over the network [9]. A work on Homomorphic encryption scheme was proposed by Craig Gentry. Author propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Presented solution comes in three steps. Author improved the existing public key cryptgraphy approach by included the ideal lattices. Author defined time bound mechanism to improve the integrity under time frame based key sharing. Author also used a hierarchical approach to enable the secure information encryption and sharing without specifying the conditional data transmission over the network. Author secure the private information communication under secure means. The presented key assignment scheme also improve the security in terms of cryptography approach [10]. Ueli Maurer performed a work on authentication based scheme using symmetric encryption. Author highlight two reasons for investigating nevertheless AtE as a general paradigm: First, this calls for a definition of confidentiality; what separates a confidential from a secure channel is its (potential) malleability. Author propose the first systematic analysis of malleability for symmetric encryption, which, in particular, allows us to state a generic condition on encryption schemes to be sufficient for AtE[11].

III. PROPOSED MODEL

In this presented work a two stage, DNA cryptography approach is presented to text encryption. In this work, the DNA concept will be used for the key generation as well to encode the text. At the earlier stage, the dynamic DNA pattern will be identified over the sequence to generate the key to perform the encoding. Later on, the DNA code dictionary will be defined to perform the cryptography. The model of the presented work is given here under

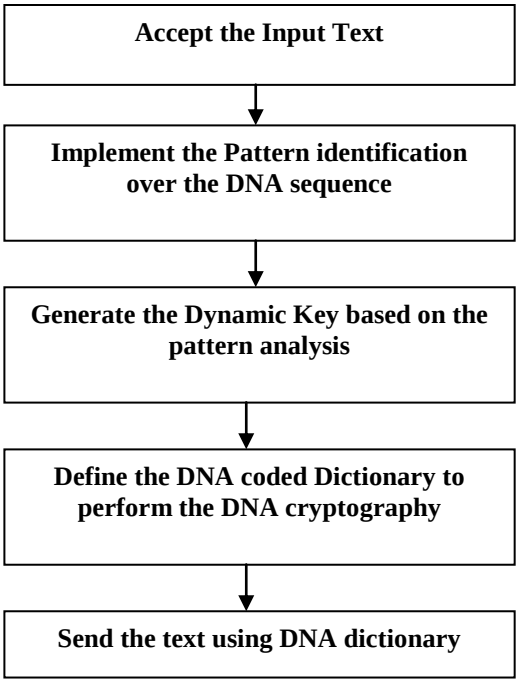

Figure 2: Flow of Work

A) DNA Sequencing

The frequent pattern mining of the DNA sequence is an important mean to study the structure and function of the DNA sequence. In this paper, base on the characteristics of the DNA sequence, to propose the algorithm of JMPS(joined maximal pattern segment), which use of the maximal frequent pattern segments base on adjacent to the maximal

frequent pattern mining, to improve the efficiency and availability of the DNA sequence data mining. DNA sequences use an alphabet {A, C, G, T} representing the four nitrogenous bases Adenine, Cytosine, Guanine and Thymine .
The Homo Sapiens (human) DNA sequence AX829174 starts with TTCCTCCGCGA and contains 10,011 characters.The subsequence mining problem is of particular importance in computational biology, where the challenge is to detect short sequences, usually of length 6- 15, that occur frequently in a given set of DNA or protein sequences.

Complete work of DNA tandom repeat sequence pattern identification work is divided in number of sub stages. These stages are presented in the form of seprate algorithm. These algorithms includes the

(i) Generation of Frequency Matrix of DNA sequence alphabet
(ii) Search of a DNA pattern over the sequence (Single Alphabet, 2 Alphabet, Multiple Alphabet Sequence)
(iii) Generation of Tandom Repeat Sequence
(iv) Sequence mining of Tandom Repeat Pattern over the DNA Sequence.

IV. RESULTS

The presented work is implemented in java environment. The work is applied on real time SMS system. The DNA sequence is extracted from different keys obtained generated randomly. The analysis of work is defined under different efficiency parameter. The analysis parameters are shown in Table 1

Table 1 : Analysis Parameter

Parameter	Values
Input DNA Sequence	CTATAATCCCAGCTTGTTGGG AGGCCAAGGCAGGAGGATCA CTTGAAGCCCAGGAGTTTGAG ACGAGCCTAAGCAACATAGCA AGACCCTATCTCTACAATTAT AAATATAGTATTTGTTAATATT TGGCCAGGCGTGGTAGTACAT GCCTGTAGGCCCAGCTACTTG GGGAGAGGAGGCAGGAGGAT CACTTGAGGGCCGAAGTTCTG G
DNA Sequence Length	211
Input Text	Hello! How Are You
Input Text Length	19

The analysis of work is here defined in terms of time taken by the work for different cryptography operations on different input text of different length.

Table 2 : Analysis Results

DNA Sequence Length	Input Length	Key Generation Time	Encryption Time	Decryption Time
100	20	2063 ms	.1 ms	.1 ms
200	20	5369 ms	.2 ms	.2 ms
300	20	7256 ms	.2 ms	.2 ms
400	20	10234 ms	.3 ms	.3 ms
500	20	15536 ms	.4 ms	.4 ms

The results are here analyzed respective to different length DNA keys. The results are shown in the form of graph

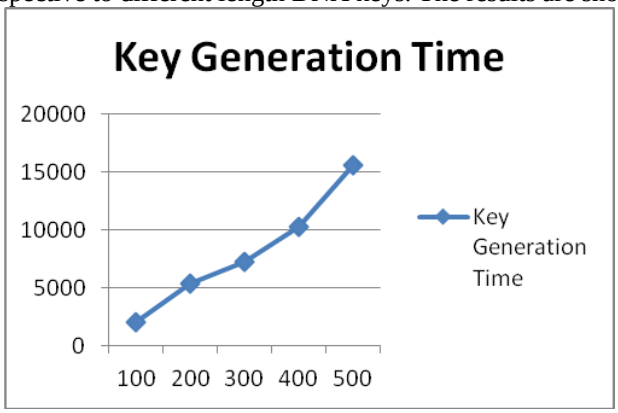

Figure 3 : Analysis Result

V. CONCLUSION

In this paper, a DNA based symmetric key cryptography approach is presented. For SMS encryption The work is applied on SMS encryption and analysis is performed under efficiency parameter. The results shows the effective message transmission over the network.

References

[1] Ohood S. Althobaiti, An Enhanced Elliptic Curve Cryptography for Biometric, 7th International Conference on Computing and Convergence Technology (ICCCT), pp 1048–1055, 2012

[2] Seny Kamara, Dynamic Searchable Symmetric Encryption, CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 965-976)

[3] Parisa Kaghazgaran, Secure Two Party Comparison over Encrypted Data, World Congress on Information and Communication Technologies, pp 1127-1130, 2011

[4] Trisha Chatterjee, Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm, Information and Communication Technologies (WICT), pp 1179, 2011

[5] Chao-Wen Chan, A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme, IJCSNS International Journal of Computer Science and Network Security, Vol.8 Issue.4, pp 128-132, April 2008

[6] Jaesung Yoo, A Method for Secure and Efficient Block Cipher using White-Box Cryptography, Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, 2012

[7] Wasim A Al-Hamdani, Elliptic Curve for Data protection, Proceedings of the 2011 Information Security Curriculum Development Conference, pp 1-14, 2011

[8] Joonsang Baek, Compact Identity-Based Encryption without Strong Symmetric Cipher, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp 61-70, 2011

[9] Ralf Kusters, Computational Soundness for Key Exchange Protocols with Symmetric Encryption, Proceedings of the 16th ACM conference on Computer and communications security, pp 91-100, 2009

[10] Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices,, Proceedings of the 41st annual ACM symposium on Theory of computing, pp 169-178, 2009

[11] Giuseppe Ateniese, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, International Association for Cryptologic Research, pp 288-297, 2006

