Proposing an Encryption/ Decryption Scheme for IoT Communications using Binary-bit Sequence and Multistage Encryption

Iqra Hussain[1], Mukesh Chandra Negi[2], Nitin Pandey[3]

[1]*Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida*
[2]*Tech Mahindra Ltd, A7, Sector 64, Noida*
[3]*Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida*
[1]*iqrahussain4@gmail.com*, [2]*MN00330419@techmahindra.com*, [3]*npandeyg@gmail.com*

Abstract: **Currently for a secured communication to take place it has become important to use cryptography on both the sides i.e. encrypting data at sender's side later followed by decryption processes at the receiver's side. It is difficult to provide security against the attackers, since they can easily get the significant data by uncovering the encryption key. A lot of algorithms are being expounded for providing data security and most of these algorithms use random key generations, and perform arithmetic operations with the key. This paper puts forward a new encryption/decryption algorithm that is based on the ASCII, Binary-Bit sequence and further uses the XOR operation. It insinuates encryption at compound stages and the key is imparted by the user. In the proposed algorithm, the original data will be encrypted at multiple stages and a key will be made use for encryption of plaintext to cipher text; next same key will be put to use for decryption of cipher to plain text. The proposed algorithm comes under the category of Symmetric key algorithms.**

Keywords: **Encryption, Decryption, Plaintext, Cipher text, Key, XOR, RSA, DES, PA, IoT**

I. INTRODUCTION

During any data transmission it becomes an essential to transmit data securely to the receipt without any sort of third party intrusions. Cryptography is the practice by which plaintext (original) data is encrypted by a specified algorithm, and the resulted text called cipher text (encrypted) data, that does not bring out the original data. The cipher text can be rearranged by a specified Algorithm to get back the plaintext (original) data. In cryptographic discipline, the Caesar cipher comes out to be the former most and more extensively recognized encrypting practice provided by the Julius Caesar. It is the substitution method in which each latter/word in the plaintext is replaced by the latter/word by adding or subtracting the fixed position. Caesar cipher encryption method is based on the modular arithmetic operation.

It can be represented as, Let encrypt and decrypt the letter m by the shift of n, further mathematical illustration will be as; Encryption, En (m) = (m+n) mod 26 Decryption, Dn (m) = (m-n) mod 26.

Cryptographic algorithms are classified in to two categories public key algorithms and symmetric key algorithms. Symmetric key algorithms use the same keys for encrypting and decrypting processes, whereas public key algorithms use different keys for encrypting and decrypting processes.

A recently developed technique named "Advance cryptography algorithm for improving data security" is discussed in [4].

In this method the encryption/decryption is defined using symmetric key. The initial key and key block concepts are used in this method.

Before proposing any algorithm of encryption or decryption, factors that must be considered include: security, countenances of algorithms, space complexities and time complexities of algorithm. Fig. 1 represents the conventional model of encryption.

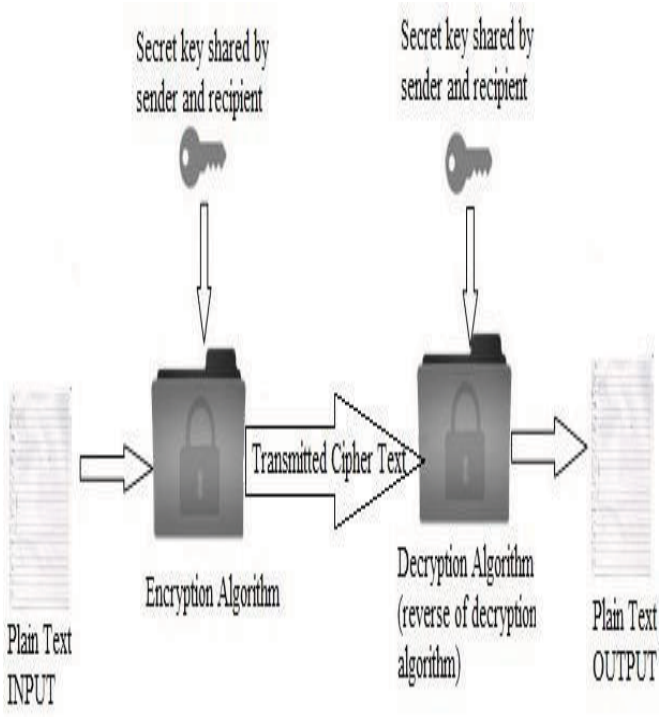

Fig. 1. Conventional Encryption Model

978-1-5386-4692-2/18/$31.00 ©2018 IEEE

If the security of the information is over looked, following services need to be delivered: [4]

Authentication (who created and send the data)

- Availability (performance of algorithm)
- Access Control (control use of resources)
- Confidentiality (privacy on algorithm process)

For improvement of Caesar cipher the random numbers generating techniques are used for generating keys [6]. Proposed idea suggests a method to generate the Caesar substitution key using the key matrix trace value restricted to module of 94. This method gives enough secure protection along with peak throughput with minimal memory occupancy. This technique is impervious to brute-force attack.

Quantum cryptography uses the key distribution technology for security and use of quantum cryptography in the future of information security [3]. Symmetric, Asymmetric key cryptography and random key transmission, secure way for key distribution [2]. Symmetric key cryptographic techniques apply random key generators [9]. Security of the network using the cryptography algorithm, network infrastructure, protects the network and network resources [1].

Security of the data communication, channel uses the quantum cryptography [5]. Enhanced approach of the Caesar cipher algorithm and columnar transposition, but key generation should be strong [7]. Cryptographic technique at multilevel, encrypt the key used for encryption or decryption in RSA [8]. Transmit an error free image over the communication channel or the medium with efficient use of channel [10].

II. PROPOSED WORK

The paper is presents a new symmetric cryptography algorithm and uses the symmetric key provided by the user. The same key will used to encrypt the given data making use of the projected algorithm. On a whole in this technique we substitute the plain text with the cipher text by performing some operation on the binary bit sequence of the plain text. The key that will be provided by the user should be from 0 to 255.Basic concept of the symmetric cryptography process is shown in Fig. 2

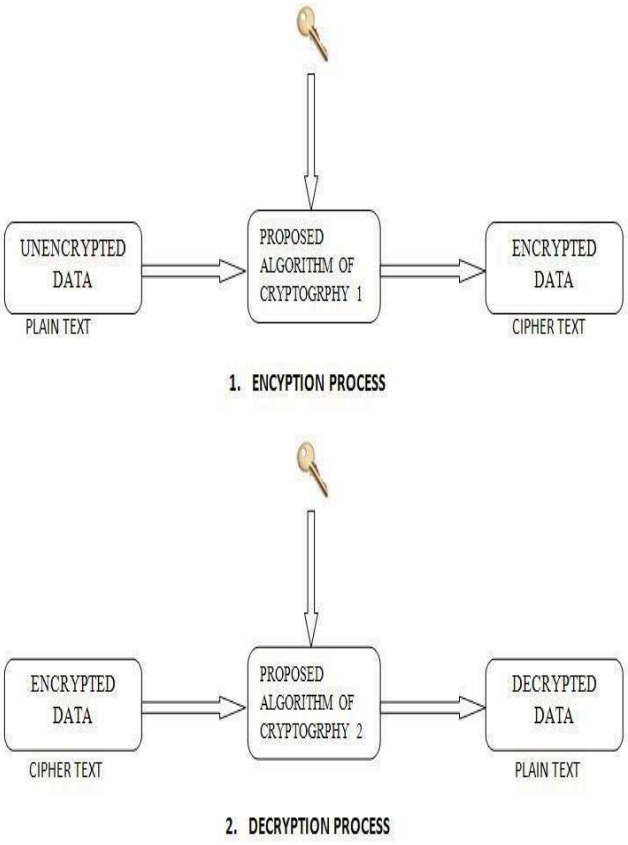

Fig. 2. Basic Concept of Symmetric Cryptography

Main reasons of using the symmetric key for encryption and decryption are:

1. Process is undemanding to use.
2. Security is reliant on the key.
3. Both the dispatcher and the corresponding recipients can use the similar keys and same processes for encryption and decryption techniques.

Proposed Encryption Algorithm:

First we need to define some character values that will used to replace the plain text.

Defined characters = $2n/2$

N is binary bit sequence.

1. Reading the plaintext message from user.
2. Replacing the plaintext by their ASCII values.
3. Read a secret key from the user.
4. Perform the XOR of ASCII values with the key provide by user.

5. Convert numerical values in the binary n-bits sequence.

6. Convert the received n-bit sequence in the n/2-bits binary sequence.

7. Convert the n/2-bits binary sequence in the decimal format.

8. Change all the decimal values with respective character from the character table.

9. Transmit the cipher text.

Proposed Decryption Algorithm:

Use the same character table used in the encryption process.

1. Read the cipher text from user.
2. Replace cipher text by their numerical values.
3. Read the secret key form the user.
4. Manage the binary bits sequence.
5. Perform the XOR operation of binary bits sequence and secret key.
6. Perform reverse character substitution.
7. Process the plaintext.

III. RESULTS COMPARISONS

Here we have compared the proposed algorithm with RSA (Rivest-Shamir-Adleman), AES algorithm. We are comparing two parameters for execution time that includes the encryption time and the decryption time of both algorithms. We compared the execution time for encrypting the plain text by both the algorithms. RSA is an asymmetric key algorithm, AES and Proposed Algorithms come under symmetric key algorithm.

The "RSA Algorithm", "AES Algorithm" and "Proposed Algorithm" are implemented on java, compiler version jdk1.6.0_26 was used to find the execution time (in milliseconds) of RSA, AES and Proposed Algorithm. In each cycle, the same plaintexts are encrypted by copying the same plaintexts for each algorithm. Comparison of the text files was done alone.

As a final point, the outputs of execution time in the form of milliseconds in numeric form are shown in the tabular form. This is shown in table 1 and table 2.

TABLE I: ENCRYPTION TIME COMPARISONS

Plain Text Size	RSA Algorithm	AES Algorithm	Proposed Algorithm
100 bytes.txt	45	63	2
1 kb.txt	62	64	8
2 kb.txt	78	65	24
5 kb.txt	192	112	110

TABLE II: DECRYPTION TIME COMPARISONS

Plain Text Size	RSA Algorithm	AES Algorithm	Proposed Algorithm
100 bytes.txt	141	2	2
1 kb.txt	156	2	4
2 kb.txt	169	3	7
5 kb.txt	172	8	69

Graphical representations of the table 1 and table 2 are shown in Fig. 3 and Fig. 4 with the blue line and green line respectively for RSA algorithm and Proposed Algorithm. These observations are made using personal computer machine with the specification of Intel® Core™ 2 Duo CPU, GHz, 4GB of RAM, Micro Soft Windows 8 (32-bit) as the testing platform.

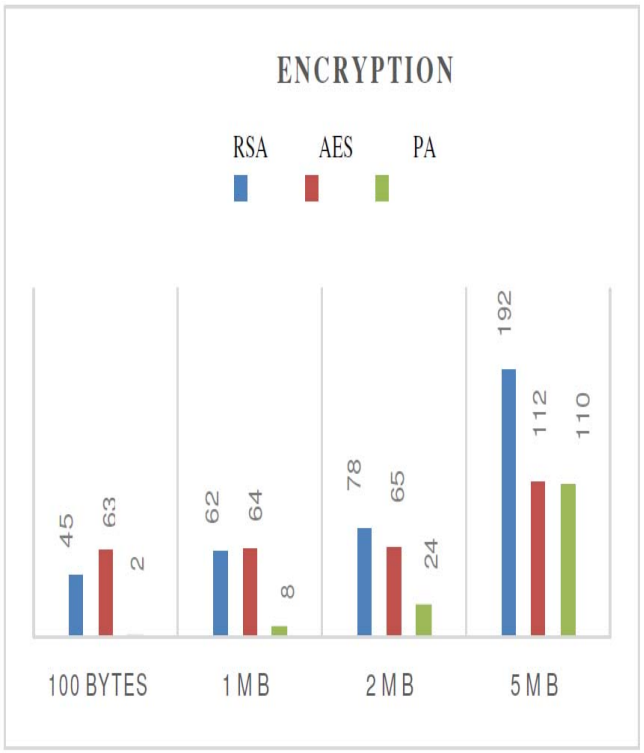

Fig. 3. Encryption Time Comparisons

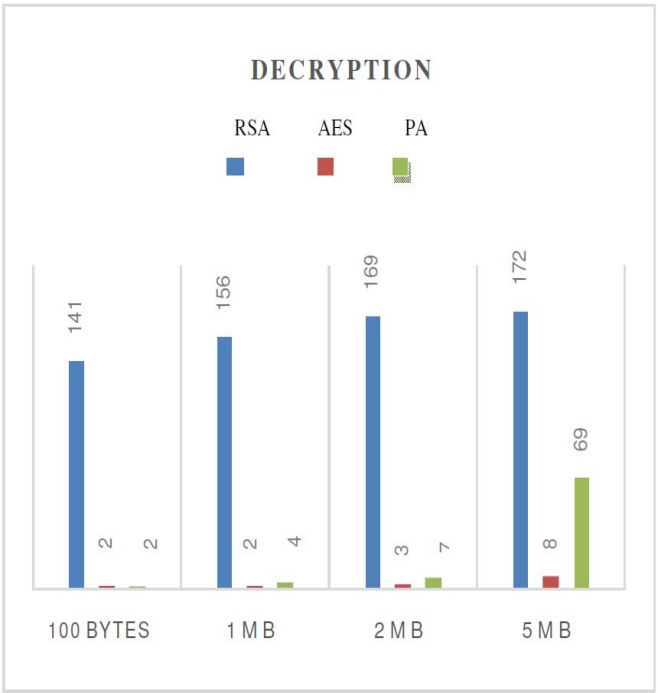

Fig. 4. Decryption Time Comparisons

IV. FEATURES OF PROPOSED ALGORITHM

Some features of this proposed algorithm are:

- Algorithm occupies minimum memory.
- Provided key for the algorithm depends on the binary Bits sequence.
- Brute Force attack requires n! Attempts, so algorithm is more robust
- Algorithm works very fast, time efficient algorithm.
- Multistage encryption is using by the algorithm
- Algorithm is simple and more secure.
-

V. CONCLUSION

The security for data becomes an aspect of importance for any encrypting or decrypting processes. The space and time are also other important aspects while designing any cipher algorithm. Our method provides high throughput by occupying less memory.

The affirmative fraction of the projected algorithm compromises the fact it's not quite viable cracking the encrypting/decrypting processes with no knowledge about the accurate secret key and thus the projected algorithm can be put to use on different types of public applications in Iot communications to transmit confidential data from one machine to another machine.

ACKNOWLEDGEMENT

Authors of this study are sincerely grateful to the Founder President of Amity University, Dr. Ashok K Chauhan, who has overwhelmingly shown his keen Interest in fostering research in Amity University and has always been a motivation for achieving greater heights.

REFERENCES

[1] Ankur Singhal, Sumedha Kaushik, "Network Security Using Cryptographic Techniques", IJARCSSE - 2012, ISSN: 2277 128X, V2, Issue 12, PP 105 – 107.

[2] Vidiksha, Shekher Saini, "Data Encryption and Decryption using Deterministic Random Key for Transmission: A Review", IJARCSSE – 2013, ISSN: 2277 128X, V3, Issue 8, PP 817 – 818.

[3] Payal P. Kilor, Pravin.D.Soni, "Quantum Cryptography: Realizing next generation information security", IJAIEM - 2014, ISSN 2319– 4847, V3, Issue 2, PP 286 – 289

[4] Vishwa gupta, Gajendra Singh, Ravindra Gupta Ravindra Gupta, "Advance cryptography algorithm for improving data security", IJARCSSE – 2012, ISSN: 2277 128X, V2, Issue 1, PP 164 – 67

[5] Navleen Kaur, Amardeep Singh, Sarabpreet Singh, "Enhancement of Network Security Techniques using Quantum Cryptography", IJCSE – 2011, ISSN : 0975-3397, V3, No. 5, PP 1960 – 1964

[6] S. G. Srikantaswamy, H. D. Phaneendra, "Improved Caesar Cipher With Random Number Generation Technique And Multistage Encryption", IJCIS-2012, V2, No.4, PP 39-49

[7] Dharmendra K Gupta, Sumit K Srivastava, Vedpal Singh, " New Concept of encryption algorithm A hybrid approach of Caesar

Cipher and Columnar transposition in multi stages", JGRCS-2012, V3, No. 1, PP 60-66

[8] K.Govinda, E. sathiyamoorth, "Multilevel Cryptography Technique Using Graceful Codes", JGRCS - 2011, V2, No.7, PP 1-5

[9] A.Nath, S.Ghosh, M.A.Mallik, "Symmetric key cryptography using random key generator", PICSAM-2010, V2, PP 239-244

[10] Ajay Sharma, Abhishek Dwivedi, Nitin Pandey, Amit Kumar, Deo Brat Ojha, "An Approach for Two-Tier Security on Transmission of Medical Image using Post Quantum Cryptosystem over Teeming Channel", IJAEST-2010, V1, No. 1, PP 10 – 15.