Data Protection by Multi-Level Encryption Algorithm (TTJSA Algorithm)

Meenu Verma
Department of Electronics and telecommunication
Chouksey Engineering College
Bilaspur, India
meenuniist@gmail.com

Rahul Gedam
Department of Electronics and tele communication
Chouksey Engineering College
Bilaspur, India
engg.rahul2801@gmail.com

***Abstract*--In the present paper the authors have proposed a new combined cryptographic method for data encryption using TTJSA algorithm. TTJSA algorithm uses three methods MSA, NJJSAA and Vernam Cipher Method. The above three methods are applied in random order on any given plain text for a number of times to get the ultimate cipher text file. The encrypted data is send to receiver and can be decrypted using TTJSA decryption algorithm. In the present work, authorsmodified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad. Proposed method can provide security against passive attack suchas password based attack.**

This technique can be applied to encrypt data in Defense system, Banking sector, mobile network etc. or to verify the data in other applications like Aadhar card, Voter ID, Driving License, Passport & Visa etc.

Index Terms—Cryptography, Encryption, TTJSA, Passive attack.

I.NTRODUCTION

In the information age, cryptography has become one of the major methods for protection in all applications. Cryptography allows people to carry over the confidence found in the physical world to the electronic world. In today’s scenario hundreds of thousands of people interact electronically every day,whether it is through e-mail,e-commerce, ATM machines, or cellular phones. The constant increase of information transmitted electronically has led to an increased reliance on cryptography and authentication. Now there is no guarantee that between sender and receiver no one is intercepting confidential data providedthat the data is not encrypted or properly protected? The security originality of data has now become a very important issue in data communication network. One cannot send any confidential or important message in raw form from one computer to another computer as any hacker can intercept that confidential message or important message. Imagine that the hacker has been able to break the ‘security key’ of a person’s bank account during an ‘e-banking’ session and has intercepted all data. In that case, if the data is not properly encrypted, the victim may incur a huge loss. It must be ensured that, when a client is sending some confidential data from the client machine to another client machine or from the client machine to the server, then that data should not be intercepted by someone. The data should be protected from any unwanted intruder otherwise a massive disaster may happen all of a sudden.

Cryptography is an emerging research area where the people are trying to develop some good encryption algorithm so thatno intruder can intercept the encrypted message. Cryptographic algorithm can be broadly classified into two categories: (i) ‘symmetric key cryptography’, and (ii) ‘public key cryptography’. The merit of ‘symmetric key cryptography’ is that the key management is very simple as one key is used for encryption as well as for decryption. In case of symmetric key cryptography the key is secret.In the present work we are proposing a symmetric key method called TTJSA which is a combination of 3 distinct cryptographic methods, namely, (i)Vernam Cipher Method, (ii) MSA method [1] and (iii)NJJSAA method.

TTJSA	Trisha Chatterjee, TamodeepDas, Shayan dey, Joyshree Nath, Asoke Nath symmetric key cryptographic method
NJJSAA	Neeraj Khanna, Joel James, Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath symmetric key cryptographic method
MSA	Meheboob, Saima & Asoke(msa) symmetric key cryptographic method

Table: 1 Acronyms used in this paper

II. METHOD USED

TTJSA [1] encryption algorithm is used which is an amalgamation of three different cryptographic modules: Vernam cipher [1], MSA [2] and NJJSAA [3], for the encryption purpose of data. We discuss the procedure elaborately in the following sections.Brief study of the methods used in TTJSA algorithm is as follows:

A. Algorithm for Encryption

1. Vernam Cipher:

In this method the cipher text is generated by applying the logical XOR operation (Exclusive-OR or Modulo-2 addition) to the plain text and the key. The advantage of using the XOR operation is that it can be undone with the same operation. In other words: XOR-ing the cipher text with the key, would reveal the plain text again.

Cipher text= Plain Text XOR key.

Step 1: The whole file is broken into different small blocks, where each block size should be less than or equal to 256 byes.

Step2: Perform Vernam Cipher method with the block of randomized key i.e. each byte of blocks of the file XOReach byte of the blocks of randomized key.

Step 3: Perform Step 1 and Step 2 until the whole file is encrypted and repeat this step for random number of times. After performing the aforementioned steps, we again merge the blocks of the encrypted file and thus we get the final encrypted result of this modified Vernam Cipher method.

2. NJJSAA Method:

Step 1: Read the encryption number and randomization number is calculated in the input file.

Step 2: Convert 32 bytes of data into 256 bits and store in some 1- dimensional array.

Step 3: Store 32 bytes key in another 1-dimensional array.

Step 4: Obtained the nth bit of data array.

Step5: Obtained the corresponding key value.

Step 6: Interchange the nth bit of data with nth bit of key.

Step 7: Repeat step 4, 5 & 6 for 256 times.

Step 8: Perform right shift by one bit.

Step 9: Perform bit(1) XOR bit(2), bit(2) XOR bit(3)…..bit(255)XOR(256)

Step 10: Repeat Step 8 with 2 bit right, 3 bit right,..., n bit right shift followed by Step 9 after each completion of Right bit shift .

3. MSA

Nath et al. (1) proposed a symmetric key method where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. MSA method is basically a substitution method where we take 2 characters from any input file and then search the corresponding characters from the random key matrix and store the encrypted data in another file. MSA method provides us multiple encryptions and multiple decryptions. The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order. The randomization of key matrix is done using the following function calls:

Step-1: call Function cycling ()

Step-2: call Function up shift ()

Step-3: call Function down shift ()

Step-4: call Function left shift ()

Step-5: call Function right shift ()

B. Algorithm for Decryption

1. Vernam Cipher

In this method The plain text is generatedback by applying the logical XOR operation (Exclusive-OR, or Modulo-2 addition) to the ciphertext and the key.

Plain text= cipher text XOR key.

2. NJJSAA Method

Step1:Perform left shift by one bit.

Step2: perform inverse bit XOR of receive encrypted data.

Step3: Repeat Step 1with 2 bit left, 3 bit left,...,n bit left shift followed by Step 2 after each completion of left bit shift .

Step4: Obtained the nth bit of data array.

Step5: Obtained the corresponding key values.

Step6: Interchange the nth bit of key with nth bit of data.

3. MSA

The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order. The randomization of key matrix is done using the following function calls:

Step-1: call Function right shift ()

Step-2: call Function left shift ()

Step-3: call Function up shift ()

Step-4: call Function down shift ()

Step-5: call Function cycling ()

III. FLOWCHART OF PROPOSED METHOD

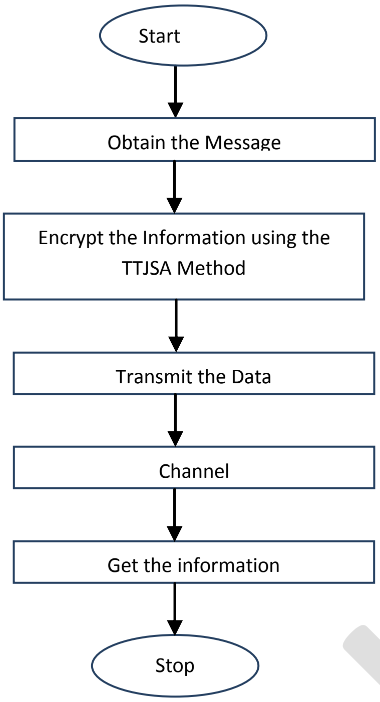
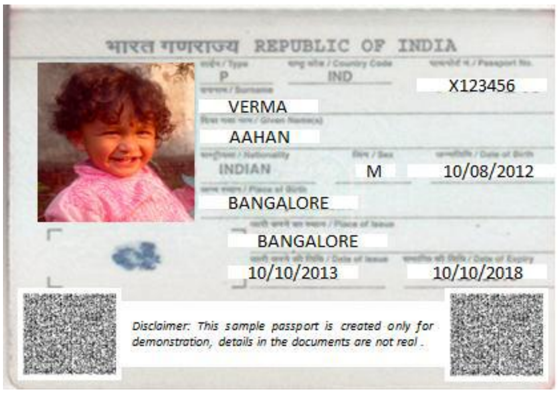


Fig1: Flow chart of Method

IV. RESULT AND DISCUSSION

This encryption and decryption algorithm is applied and checked on various types of files. Few of the examples are listed in below table.



भारत गणराज्य REPUBLIC OF INDIA

Type: P
Country Code: IND
Passport No.: X123456
Surname: VERMA
Given Name(s): AAHAN
Nationality: INDIAN
Sex: M
Date of Birth: 10/08/2012
Place of Birth: BANGALORE
Place of Issue: BANGALORE
Date of Issue: 10/10/2013
Date of Expiry: 10/10/2018

Disclaimer: This sample passport is created only for demonstration, details in the documents are not real .

Fig2: Sample passport

Example from sample Passport	**Encrypted text**
AahanVerma 10 august 2012 indian X123456 Bangalore Male 10 August 2013	*????d??o"?2"-qL51k(v6/'i.)u1oibGIUo?)z +r?67.!"-??u*
Other Examples	
HE IS GOOD	*(A) c=¤{ZKÃˆÞ_*
AAAAAAAAAAAAAAAA	*(A) ¼Ü>¶,£~Ä_B_wqá7¯*
AAAAAAAAAAAAAAA	*(B) 81š—‰cŸ¼€˜sÍÇ7 _*

Table: 2 Encrypted text examples

CONCLUSION

In the present work three different algorithms are combined to make the encryption process infrangible. The same is evident from the results. We have applied this method on some known text where the same character repeats for a number of times and found that after encryption there is no repetition of pattern in the output file.The merit of this method is that it is almost impossible to break the encryption algorithm without knowing the exact key matrix. We propose that thisencryption method can be applied for data encryption and decryption in banks, defense, mobile networks, ATM networks, government sectors, Passport etc. for sending confidential data. The present algorithm may be used for databaseencryption also.

REFERENCES

[1] Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm " Proceedings of Information and Communication Technologies (WICT), 2011 " held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.

[2] Symmetric Key Cryptography using Random Key generator: AsokeNath, SaimaGhosh, MeheboobAlamMallik: "Proceedings of International conference on security and management(SAM'10" held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).

[3] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: NeerajKhanna,JoelJames,JoyshreeNath, SayantanChakraborty, AmlanChakrabartiand AsokeNath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).

[4] SomdipDey, JoyshreeNath, AsokeNath, "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", IJMECS, vol.4, no.5, pp.1-9, 2012.

[5] SomdipDey, JoyshreeNath and AsokeNath. Article: An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm. International Journal of Computer Applications46(20): 46-53, May 2012. Published by Foundation of Computer Science, New York, USA.

[6] SomdipDey, "SD-EQR: A New Technique To Use QR CodesTM in Cryptography", Proceedings of "1st International Conference on Emerging Trends in Computer and Information Technology (ICETCIT 2012)", Coimbatore, India, pp. 11-21.

[7] Cryptography and Network Security, William Stallings, Prentice Hall of India.

[8] Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.

[9] "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Online] [Retrieved 2012-02-09]

[10] Reed and G. Solomon, "Polynomial codes over certain finite fields", Journal of the Society for Industrial and Applied Mathematics, 8(2):300–304, 1960.

[11] "ZXING- QR Code Library ", http://code.google.com/p/zxing/[Online] [Retrieved 2012-02-09] [12] N. Johnson and S. Jajodia, "Steganaly- sis: The investigation of hidden information", Proc. Of the 1998 IEEE Information Technology Conference, 1998.

[12] SomdipDey, KalyanMondal, JoyshreeNath, AsokeNath,"Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QRAlgorithm", IJMECS, vol.4, no.6, pp. 59-67, 2012.