GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DATA SECURITY BY USING EXCRYPTION ALGORITHM (TTJSA ALGORITHM) AND QR CODES

Meenu Verma[1], Rahul Gedam[2]

Department of Electronics and Tele-Communication Chouksey Engineering College,Bilaspur, India[1,2]

ABSTRACT

Security is a fundamental component of every network design. Authenticity and Security of data is a big challenge when planning, building, and operating a network. A security policy defines what people can and can't do with network components and resources. In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security.

To solve this problem, we propose an innovative method to authenticate the digital documents. Our proposal is a new method, where the Details listed in a sample passport (or other applications, Aadhar card, Voter ID, License, Mark sheet) will be encoded in QR Code in encrypted form, so that if an intruder tries to change the text details in Passport still he cannot do that in the QR Code, because the encryption key is unknown to him. In this method, we encrypt the passport data using the TTJSA encryption algorithm. The encrypted passport details are entered inside QR code and that QR code is also printed with the original data of the passport. The passport details can then be retrieved from the QR code and can be decrypted using TTJSA decryption algorithm and then it can be verified with text details already there in the passport. 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.

Keywords—Cryptography, Encryption, TTJSA, Passive attack.

I. INTRODUCTION

In today's cutting edge technology scenario, security and authenticity of data is a big challenge. The massive development in internet technology in the last few years now it is a real challenge for the sender to send confidential data from one computer to another computer. There is no guarantee that between sender and receiver there is no one is intercepting those confidential data provided 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. There is no guarantee that the message will not be intercepted by anyone. 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 that no 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 XOR each 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 n^{th} bit of data array.

Step5: Obtained the corresponding key value.

Step 6: Interchange the n^{th} bit of data with n^{th} 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 upshift()

Step-3: call Function downshift()

Step-4: call Function leftshift()

Step-5: call Function rightshift()

B. B. Algorithm for Decryption

1. Vernam Cipher

In this method The plain text is generated back by applying the logical XOR operation (Exclusive-OR, or Modulo-2 addition) to the cipher text 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 rightshift()

Step-2: call Function leftshift()

Step-3: call Function upshift()

Step-4: call Function downshift()

Step-5: call Function cycling()

III. Flowchart of proposed method

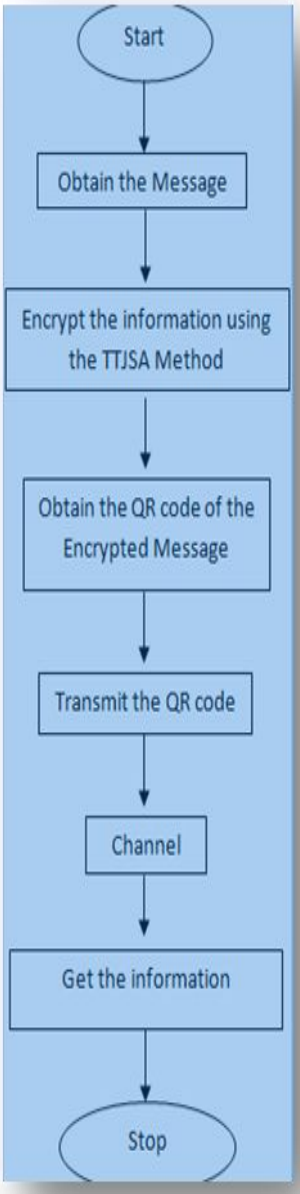

Fig1: Flow chart of Method

IV. RESULT & DISCUSSION

This encryption and decryption algorithm is applied and checked On Passport and Result is found.

1. At Transmitter End

Step1. Enter passport details.

Step 2.Enter key.

Step 3. Press encrypt button.

Step 4. Generate QR code.

Step 5. Embedd QR code.

Step 6. Save Image.

Fig.2. Encryption Output

Vernam cipher encryption output

Answer:
“:²ø€ÉiÐ´œAœŒ¹ˆz–ÇS¹ØsÄøQ©r□åä:óÊ²<W•S“ªùÏšHÊ#Qž°CÕt-L'«J=Ã¬ay¨Ô\Ÿ$[ë6Ý”

NJJSAA encryption output

Answer :

*"eVgáÛZi**®üÓÄÇ [uDÇÄÂô^**,*
*bJ#6;5& KnZÌ/00==k|kÖâåGàRŸ**¶.*¾„—?=^†Ž'äëQ}ð§¶(4_où,°œ¢œ–µ'"*

MSA encryption output

Answer =
*NlQi¾ßò(a9D8-kseVgáÛZi**®üÓÄÇ [udçÄÂÔ^°,*
bj#2#3;6;5&
*KnZÌ/0099oxkÖâåCäR›™².*¾„—?=^†Ž'äëQ}ð

2. At Receiver End

Step1. Take saved passport image
Step2. Enter the key(key should be same for encryption and decryption).

Step3. Extract Information.

.

V. CONCLUSION

In the present work Multilevel Encryption Algorithm and QR code are illustrated on Passport to verify the details listed in passport. In future same algorithm can also be used for other applications also such as Aadhar (UID)

The security of method can be further enhanced by defending the system or network from security attacks such as passive attack (password attack, compromised key attack, Man in the middle attack etc. To check the efficiency of proposed method an analysis can be performed based on the time taken to encrypt and decrypt vs. bytes in a message. This Analysis can be iterated for different inputs such as 64 bytes, 128 bytes, 512 bytes, 1024 bytes, 2048 bytes etc.

VI. REFERENCES

[1] T.chatterjee, T.Das, J.Nath, A.Nath, "Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm " ,Proceedings of IEEE WICT, 2011 held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180

[2] A.Nath, S.Ghosh, M.A. Mallik , "Symmetric Key Cryptography using Random Key generator": Proceedings ofInternational conference on security and management(SAM'10" heldat Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).

[3] N.Khanna, J.James,J.Nath, S.Chakraborty, A.Chakrabarti and A.Nath," New Symmetric key Cryptographic algorithm using combined bitmanipulation and MSA encryption algorithm: NJJSAA symmetrickey algorithm": Proceedings ofIEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Pag125-130(2011).

[4] S.Dey, J.Nath, A.Nath, "An Integrated SymmetricKey Cryptographic Method – Amalgamation of TTJSA Algorithm,Advanced Caesar Cipher Algorithm, Bit Rotation and ReversalMethod: SJA Algorithm", IJMECS, vol.4, no.5, pp.1-9, 2012.

[5] S.Dey, J.Nath and A.Nath, " An AdvancedCombined Symmetric Key Cryptographic Method using BitManipulation, Bit Reversal, Modified Caesar Cipher (SD-REE),DJSA method, TTJSA method: SJA-I Algorithm", InternationalJournal of Computer Applications46(20): 46-53, May 2012.Published by Foundation of Computer Science, New York, USA.

[6] S.Dey, "SD-EQR: A New Technique To Use QR CodesTM inCryptography", Proceedings of "1st International Conference onEmerging 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.

[13] S.Dey, K.Mondal, J.Nath, A.Nath,"Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm", IJMECS, vol.4, no.6, pp. 59-67, 2012

[14] C. Skawattananon and S. Vongpradhip, "An Improved Method to Embed Larger Image in QR Code", 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE).

[15] K. Kaur and Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", 2013 3rd IEEE International Advance Computing Conference (IACC).

[16] Y. Huang and J.Chang , "Non-expanded Visual Cryptography Scheme with Authentication", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE)- February 25-26 2013.

[17] Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima and Koji kobayashi, " A fingerpring recognition algorithm using Phase-based image matching for low quality fingerprints", Image Processing, 2005. ICIP 2005. IEEE International Conference on (Volume:3) Page(s): III - 237-40 Print ISBN: 0-7803-9134-9