Sane : Secure Encryption Technique for Alphnumeric Data Over Web Based Applications

Lalitha Ruby,
GGSIPU University,
Delhi, India

Rahul Johari,
USICT,GGSIP University,
Delhi, India

***Abstract*—In today's scenario of cyber-attacks like phishing, man in the middle attacks and system compromises, it is difficult to ensure the secure data transfer. In order to ensure confidentiality there is a requirement to encrypt the data. Various techniques have been proposed by the researchers over a period of time regarding the encryption of data and it's subsequent transmission over the web. But in our literature survey we didn't across a technique which is able to encrypt and decrypt the Alphabets , Numbers and Alphanumeric data in minimum span of time with minimum lines of code. The designed logic has been tested successfully by writing modules coded using open source JAVA programming language with the file containing plain text in the form of only alphabets, numbers and alphanumeric characters . Since the logic implemented is custom made, there is remote possibility of breaking the encryption by an intruder, since the logic will be a secret known only within the organization.**

***Keywords*—encryption, decryption, internet security, data, cipher, JAVA.**

I. INTRODUCTION

Internet revolution has changed the way the organizations conduct operations. The organizations are now operating as small modules located at physically diverse locations even in multiple countries. These organizations use the Internet as a backbone to carry out their day to day operations including sensitive data transfer. Although the technology has been growing exponentially there is a gap between the technology solutions and security solutions which is exploited by the malicious adversaries. As per the latest legislations of different countries the onus of data protection lies with the organization/data owners especially if data of the customers are involved. Basically Data Security means protecting its confidentiality, integrity, and availability. The consequences of a failure to protect any of the three of these aspects will incur losses in business, loss of customer trust, legal liability, and loss of company's goodwill. It has been observed that most of the organizations transfer sensitive files in clear text without even encrypting thus vulnerable to various cyber attacks. This paper has attempts to suggest a custom encryption/decryption technique which can be used as a template to develop a robust customized encryption algorithm by any organization. In this paper we have attempted to encrypt a sample text file that can containing text,numbers and alphanumeric data .The resultant encrypted data would be transmitted across the web and the decryption logic is implemented at the receiving end decrypting the data to original text.This custom made logic has been compared with the well known Caesar cipher to transform the same text file, however it was observed that the Caesar cipher technique failed to handle/transform all forms of alphanumeric data.

II. RELATED WORK

In [1] author(s) brings out the nuances of encryption and decryption and discusses implementation of ASCII conversion as part of encryption process. In this paper a secret key is generated subsequent to ASCII conversion, by implementing a logic of finding the mod of the ASCII value of the sequence of character, and subsequently generation of key which is converted to binary and back to ASCII. This logic although is logically strong encryption, however is not feasible to implement for conversion of larger files which are required to be taken as input and stored in encrypted format. The format of input files also are restricted in this type of conversion. However the encryption technique discussed is strong and stable. In [2] author(s) have considered multimedia data stream as plain text to be transformed into cipher text and have proposed a new block cipher based on randomized key of size n × n where n is the block size and the block undergoes n2 iterations with the plaintext.Everyiteration generates the pseudo cipher text. The encryption process generate the ciphertext C with the help of the randomized key. The decryption apply the key in reverse order on the cipher text, to get back the plain text. This work deals with the problem of efficient multimedia data encryption.In [3] A block cipher technique for security of data and computer networks is proposed. The technique can be used for text, binary and hexadecimal information. It can be placed in any one of the network layers. It is based on changing the system parameters, starting with the block length, including the number of processing rounds, the used permutation, substitution and arrangement boxes, and ending with a disturbance XOR sequence which is XORed with the final cipher-text block. This makes the system looks like a one-time pad system. These keys are indirectly generated from a text key string either inputted from the keyboard or read from a file. This happens in a delicate way using two input key numbers L1 and L2 which indicate the orders of the generated keys. The generated keys are used to make all the used parameters changeable from one block to another and from one 8-bit combination to the next. This is done using ElGamal discrete logarithm pseudo-random sequence generators in a special way. Compared with existing techniques, the proposed method offers good properties.In [4] author(s) demonstrate the comparative performance analysis of MD5, DES and AES encryption algorithms on the basis of execution time, LOC (Lines of Code) over a web application. In [5] author(s) discuss and analyze the current developments in online authentication procedures including one-time-password systems, biometrics and Public Switched Telephone Network for cardholder authentication. The author(s) propose a complete new framework for both onsite and online (Internet shopping) credit card transactions. In [6,9] author(s) presents a detailed review on various types of vulnerabilities, Structured Query Language Injection attacks, Cross Site Scripting Attack, and prevention techniques. The Author(s), also propose future expectations and possible development of countermeasures against Structured Query Language Injection attacks. In [7]author(s) present an integrated model to prevent reflected cross site scripting attack and SQL Injection attacks in applications which are made in PHP. There model works in two modes which are production and safe mode environment. They create sanitizer model for reflected cross site scripting attack and security query model for SQL Injection attack in safe mode. They validate user input text against sanitizer model and input entries which create SQL queries are validated against security query model in production mode. In [8] author(s) demonstrate the exploitation of web vulnerabilities in a credit card validation web application using brute force and dictionary attack. In[10] authors also propose a similar technique to handle the security of the alphabets and numbers but without any detailed comparison.

III. PROPOSED WORK

Methodology Adopted :For designing the SANE : Secure Encryption technique for alphanumeric data over web based applications, the entire process of encryption and decryption has been accomplished by writing the modules coded in Java platform. To begin with, first the already existing Caesar Cipher is tried to covert plain text to cipher text and a self encryption and decryption technique is developed to convert the same plain text to cipher text and the transformed decrypted file from both the programs has been compared . The plain text used for transformation to cipher text had alphanumeric text.

A. Step I:

In the step 1 it was planned to Script a program to implement Caesar Cipher encryption technique which is a symmetric Algorithm Caesar Cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

The process involved for step are:

- A program is developed to read the contents of the file.
- Stored the contents of the file in an array.
- Read the contents from the array.
- Printed the same.
- Applied the encryption technique: Caesar Cipher
- Printed the original and encrypted contents of the file.
- After applying the decryption technique the original script was reproduced but failed for the special characters.

B. **Step II**

In order to develop the self encryption and decryption technique, it was proposed to encrypt in the following manner:

- The original contents of the file are stored in a String array.
- The contents are read character by character.
- Each and every character is replaced by its ASCII code.
- A random pattern is added to the ASCII code.

(i) Similarly the Decryption is done as per the following steps

- The random pattern is then subtracted from the integer number to get the ASCII code.
- The ASCII code is replaced by the respective character and stored in a String array
- Now the decrypted original contents are read and displayed.

We have the respective functions in Java that helps us to achieve the above proposed algorithm. Since this technique is not available publicly as Caesar Cipher. Definitely this is more secure than the Caesar Cipher technique.

(ii) Decryption Logic:-

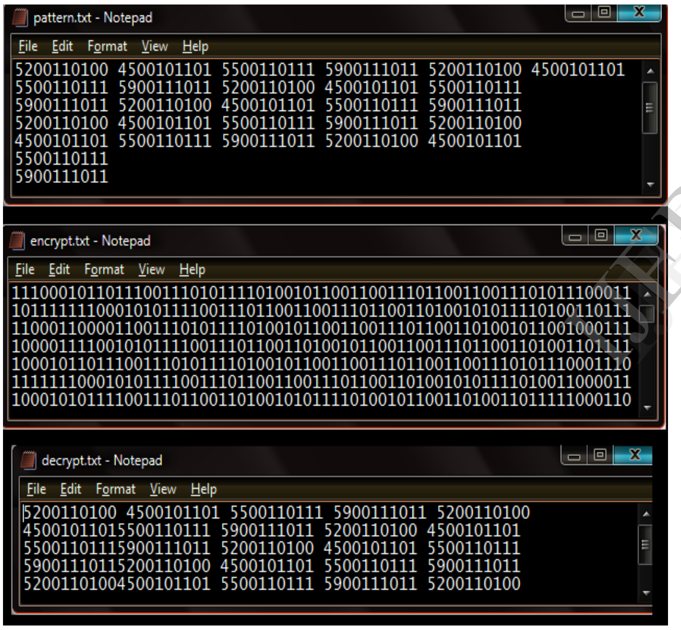
The random pattern is then subtracted from the integer number to get the ASCII code. The ASCII code is replaced by the respective character and stored in a String array.Now the decrypted original contents are read and displayed.

C. **Step III:**

The encryption of converting the ASCII text to binary text has been accomplished by taking the examples of a file having only alphabets,numbers and alphanumeric text.This will be the final encrypted message.The binary text is then again decrypted back to ASCII .Then the further reversing of the applied logic is been done to get back the original message.

(i) Plaintext having only numbers:

A file with name 'pattern.txt' is read and stored in a StringBuffer array.Then each character is taken one by one and converted into respective ASCII code.The resultant ASCII code is then added with a random pattern of integer numbers.Now this random pattern is converted into binary code and saved as 'encrypt.txt' file.This is the file that will be sent at the transmitter end through web and by running the same program at the receiver end the encrypt.txt file is read and the entire logic will operate in reverse order and the original text is saved as 'decrypt.txt'.



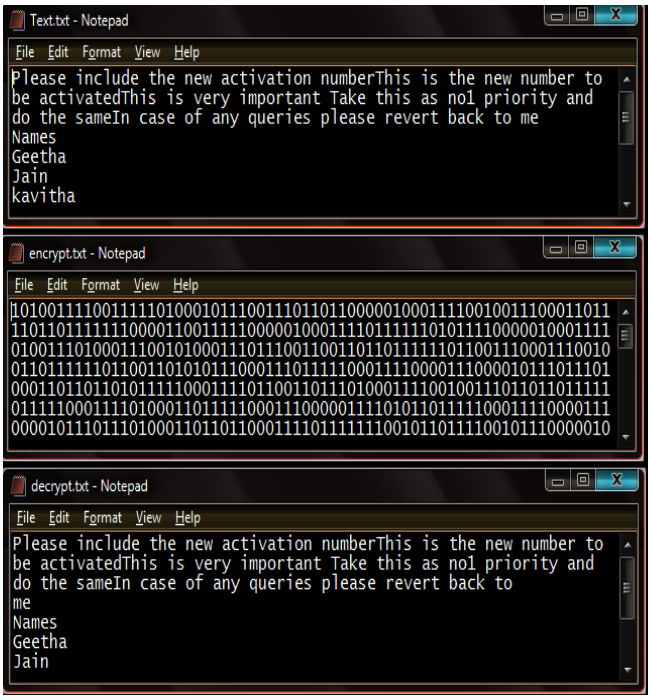
```
5200110100 4500101101 5500110111 5900111011 5200110100 4500101101
5500110111 5900111011 5200110100 4500101101 5500110111
5900111011 5200110100 4500101101 5500110111 5900111011
5200110100 4500101101 5500110111 5900111011 5200110100
4500101101 5500110111 5900111011 5200110100 4500101101
5500110111
5900111011
```

```
111000101101110011101011110100101100110011101100110011101011100011
101111111000101011110011101100110011101100110100101011110100110111
110001100001100111010111101001011001100111011001101001011001000111
100001111001010111100111011001101001011001100111011001101001101111
100010110111001110101111010010110011001110110011001110101110001110
111111100010101111001110110011001110110011010010101111010011000011
100010101111001110110011010010101111010010110011010011011111000110
```

```
5200110100 4500101101 5500110111 5900111011 5200110100
45001011015500110111 5900111011 5200110100 4500101101
55001101115900111011 5200110100 4500101101 5500110111
59001110115200110100 4500101101 5500110111 5900111011
52001101004500101101 5500110111 5900111011 5200110100
```

Fig1 Plaintext having only numbers

(ii) Plaintext having only alphabets:



```
Please include the new activation numberThis is the new number to
be activatedThis is very important Take this as no1 priority and
do the sameIn case of any queries please revert back to me
Names
Geetha
Jain
kavitha
```

```
101001111001111101000101110011101101100000100011110010011100011011
110110111111000011001111100000100011110111111010111100000100011111
010011101000111001010001110111001100110110111111011001110001110010
011011111101100110101011100011101111100011110000111000010111011101
000110110110101111100011110110011011101000111100100111011011011111
011111000111101000110111110001110000011110101101111100011110000111
000010111011101000110110110001111011111111001011011110010111000010
```

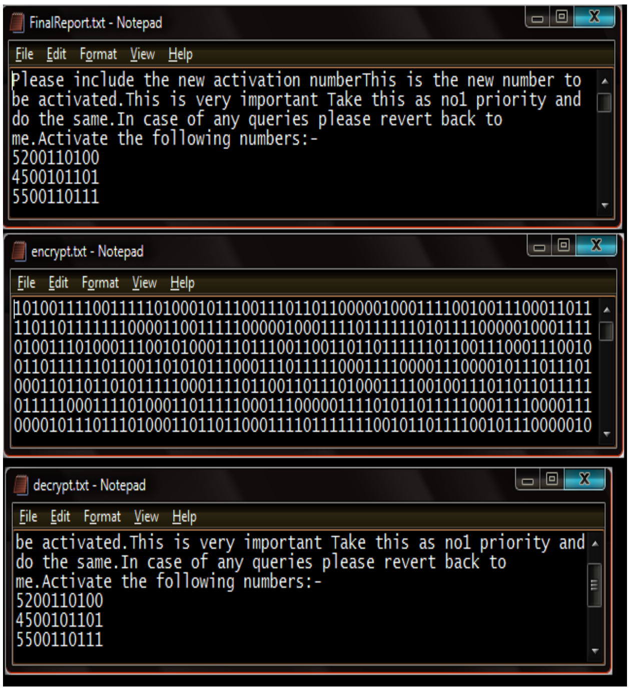
```
Please include the new activation numberThis is the new number to
be activatedThis is very important Take this as no1 priority and
do the sameIn case of any queries please revert back to
me
Names
Geetha
Jain
```

Fig2 Plaintext having only alphabets.

A file named 'Text.txt' is read and stored in a StringBuffer array.Then each character is taken one by one and converted into respective ASCII code.The resultant ASCII code is then added with a random pattern of integer numbers.Now this random pattern is converted into binary code and saved as 'encrypt.txt 'file.This is the file that will be sent at the transmitter end through web and by running the same program at the receiver end the encrypt.txt file is read and the entire logic will operate in reverse order and the original text is saved as 'decrypt.txt.'

(iii) Plaintext having alphanumeric characters

A file named 'FinalReport.txt' is read and stored in a StringBuffer array.Then each character is taken one by one and converted into respective ASCII code.The resultant ASCII code is then added with a random pattern of integer numbers.Now this random pattern is converted into binary code and saved as 'encrypt.txt 'file.This is the file that will be sent at the transmitter end through web and by running the same program at the receiver end the encrypt.txt file is read and the entire logic will operate in reverse order and the original text is saved as 'decrypt.txt.'



FinalReport.txt - Notepad
File Edit Format View Help

```
Please include the new activation numberThis is the new number to
be activated.This is very important Take this as no1 priority and
do the same.In case of any queries please revert back to
me.Activate the following numbers:-
5200110100
4500101101
5500110111
```

encrypt.txt - Notepad
File Edit Format View Help

```
101001111001111101000101110011101101100000100011110010011100011011
110110111111100001100111110000010001111011111101011100000100011111
010011101000111001010001110111001100110110111111011001110001110010
011011111101100110101011100011101111100011110000111000010111011101
000110110110101111100011110110011011101000111100100111011011011111
011111000111101000110111110001110000011110101101111100011110000111
000010111011101000110110110001111011111110010110111100101110000010
```

```
be activated.This is very important Take this as no1 priority and
do the same.In case of any queries please revert back to
me.Activate the following numbers:-
5200110100
4500101101
5500110111
```

Fig3 Plaintext having alphanumeric characters

III.ANALYSIS OF VARIOUS ENCRYTION/DECRYPTION ALGORITHMS ON THE BASIS OF EXECUTION TIME

The bar graph has been plotted to show the total execution time needed by different encryption algorithms [Fig 4] . Total Execution Time for different encryption algorithms has been calculatedusing **java.lang.System.currentTimeMillis() m**ethod whichreturnsthe current time in milliseconds.

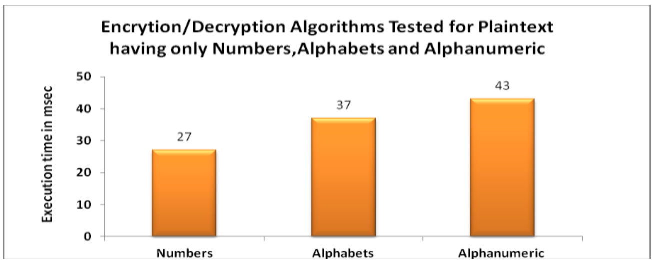


Fig4 Encryption/Decryption Algorithms on the basis of Execution time

4.CONCLUSION

In the current work we were able to write a code to implement custom made SANE technique to encrypt and decrypt all types and kinds of data. Although it is a symmetric encryption algorithm it is a more secure algorithm since the logic is not available in public domain. Moreover since the coding is done in Java it is platform independent and lightweight and special characters cannot be addressed in Caesar cipher whereas it is taken care in custom made encryption.These type of encryption programs have their applicability in day to day operations of various organizations which operate from multiple locations.

REFERENCES

[1] An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms , International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 4 No. 09 Sep 2012 1650-1657.

[2] Aruljothi, S. ; Venkatesulu, M.Symmetric Key Cryptosystem Based on Randomized Block Cipher, Future Information Technology (FutureTech), 5th International Conference,2010.

[3] Rahouma, K.H.A block cipher technique for security of data and computer networks ,1999

[4] R. Johari,I. Jainand R.L.Ujjwal"Performance Analysis of MD5, DES and AES Encryption Algorithms for Credit Card Application" In : International Conference on Modeling and computing (ICMC – 2014) , 2014.

[5] S. Gupta and R. Johari. A New Framework for Credit Card Transactions involving Mutual Authentication between Cardholder and Merchant. In: Communication Systems and Network Technologies (CSNT), 2011 International Conference on, pp. 22-26. IEEE, 2011.

[6] R. Johari and P. Sharma. A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection. In: Communication Systems and Network Technologies (CSNT), 2012 International Conference on, pp. 453-458. IEEE, 2012.

[7] P. Sharma, R. Johari, and S. S. Sarma. Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. In: International Journal of System Assurance Engineering and Management3.4 , 2012, pp. 343-351. Springer 2012.

[8] I. Jain,R. Johari and R.L.Ujjwal. Web Vulnerability Exploitation using Brute Force Attack and Dictionary Attack. In: proceedings of 9th National Conference on Smarter Approaches in Computing Technologies and Applications (SACTA-2014), 2014.

[9] R. Johari and N. Gupta. Secure query processing in delay tolerant network using java cryptography architecture. In: Computational Intelligence and Communication Networks (CICN), 2011 International Conference on, pp. 653-657. IEEE, 2011.

[10] L. Ruby and Rahul Johari, "Designing a Secure Encryption Technique for Web Based Application", International Journal of Advance Research In Science And Engineering(IJARSE) [ISSN-2319-8354],Vol. No.3, Issue No.7, July 2014 ,pp 159 -163,2014.