MSMET: A MODIFIED & SECURE MULTILANGUAGE ENCRYPTION TECHNIQUE

[1]Anoop Kumar Srivastava, [2]Sanjeev Sharma, [3]Santosh Sahu

[1,2,3]School of IT, Rajiv Gandhi Technical University, Bhopal(M.P.), India
[1]anoop.shriwastawa@gmail.com,[2]sanjeev@rgtu.net,[3]santoshsahu@rgtu.net

Abstract

Cryptography plays an integral role in secure communication and is usually the strongest link in the chain of security. Multilanguage cryptography, an advancement of classical cryptography, may evolve as a choice of classical cryptography lovers seeking a better security. We proposed an algorithm in Multilanguage approach, which generates different ciphertexts at different time for the same plaintext over a range of languages supported by Unicode. It has a better frequency distribution of characters in the cipher text than previous work on this approach.

Keywords-Unicode, Encryption, Decryption, Software Localization and Cryptanalysis.

1. Introduction

The electronic age has pushed a heavy incorporation of electronics and communication in human life. It, on one hand, miraculously simplified the human life and on other hand it has also put a lot of security challenges for our communications and transaction. Security of communication systems heavily depends on the security of cryptographic solutions incorporated. A number of eves-droppers, hackers, cryptanalyst, therefore, eye on these solutions only. Their constant efforts over a period of time have given rise to discovery of a number of cryptanalytic attacks [1, 2]. For network based systems encryption techniques two types of techniques viz., asymmetric key encryption including RSA [3] and ECC[7] and symmetric key encryption including AES [4], DES [5] and IDEA etc. Another class that has evolved itself from classical encryption techniques is the multilanguage encryption technique. A very few techniques have been proposed till recently. One of such technique named MULET has been proposed in [6].We have studied the encryption technique in details and observed weakness in the algorithm. In this paper we present our observations and our modification of the technique. We also analysis the advantage of new scheme over the MULET scheme. In the following section we present MULET algorithm in brief and in section 3 we discuss shortcomings and our modifications. In section 4. We present our algorithm and test vectors. In the conclusion section we discuss utility of the modified technique and the possible extension of the work.

2. Related Literature

As discussed above, the multilanguage encryption is the area where only a few schemes have been proposed. Apart from MULET, there is another scheme named MANET proposed by Prasenjit Chaudhary et. al. It is a key based Multilanguage encryption scheme[9]. Security issues of MANET are discussed in [10]. Attacks exploiting these issues are proposed in [11].

3. Our Observations and Modifications

We studied “MULET : A Multilanguage Encryption Technique” proposed by G. Praveen Kumar et.al. We have observed two serious weaknesses in the scheme MULET.

1. Each language has a probable frequency distribution of letters. For a given k and set of characters MULET produces a unique ciphertext for each plaintext. This may make the frequency distribution of letters in ciphertext non-uniform. This is highly non-desirable.

2. The authors state that The trespasser, to initiate a brute force attack, must have the knowledge of different aspects of the algorithm viz, mapping constant, mapping domain and replacement strategy." As none of these parameters is a part of key, the scheme cannot be analyzed in light of Kerchoff’s Principle. The security is analyzed with the assumption of Security by obscurity".

To overcome these weaknesses we suggest the following changes:

1. We fix the parameter k = 20 and we provide a fixed set of hindi characters (tabulated in the next section). For other languages we can provide similar tables but the tables need not be kept secret.

2. A random number f between 0 to 19 (we call it fluctuator) is generated. Fluctuator is a part of the key. This is the first entry in the key file.

3. To ith character read from the file, (-1)i if is added.
In the next section we suggest an algorithm MSMET (A Modified Secure Multilanguage Encryption Technique) comprising of the above security considerations.

4. Proposed Algorithm

The character set is given in the following table

Table III. Character set for MSMET (ch map)

Index	0	1	2	3	4	5	6	7	8	9
Value*	0x0905	0x0906	0x0907	0x0908	0x0909	0x090a	0x090b	0x090c	0x090d	0x090e

Index	10	11	12	13	14	15	16	17	18	19
Value*	0x090f	0x0910	0x0911	0x0912	0x0913	0x0914	0x0915	0x0916	0x0917	0x0918

Table IV. Numeral set for MSMET (chno)

Index	0	1	2	3	4	5	6	7	8	9
Value*	0x0966	0x0967	0x0968	0x0969	0x096a	0x096b	0x096c	0x096d	0x096e	0x096f

*We write the hex value of corresponding character instead of writing the character.

4.1 MSMET Encryption

```
Generate a random number f in the interval [0,20)
i:=0
Quo[i]=f
while(!End of plaintext)
        Read a unicode character from file and store into n
        R:=(n+((-1)^i)*f)\%k
        Quo[i+1]:=n/k
        Enc[i]:= ch map[R]
        Increment i ;
End while
L:=i
i:=0
while(!end of Enc)
        while(Enc[i]==Enc[i+1])
                Increment count;
                Increment i ;
        End while
        if(count>=2)
        Replace the repetitions with chno[count] in enc
        Reset count to zero
End while
```

The array Quo[i], i=0,1,...,L is the key and Enc[i], i=0,1,2,...,L-1 is the ciphertext.

4.2 MSMET Decryption

```
While(!end of enc )
        If(character is chno[i])
        Remove the character from enc and the character preceding chno[i] in the cipher text is    repeated 'i' number of times and store in Dec
End while

While(!end of Dec)
        Compare the character Dec[i] with  the mapping array ch_ map;
        Position of the character in ch_map is the required remainder R;
End while

i:=0
f:=Quo[0]
While(!End of plain text)
        U:=Quo[i+1]*M+(R-((-1)^i)*f)%k;
        Convert U to the corresponding Unicode character and write as decrypted text.
        Increment i
End while
```

4.3 MSMET Test Vectors

For generation of test vectors we have chosen two plaintexts of size 10 bytes and we provide a set of two keys and two ciphertexts for each of them.

Set1:
Plaintext: Prasanna

Key1: 0x12 0x4 0x5 0x4 0x5 0x4 0x5 0x5 0x4
*ciphertext1: 0x0911 0x0907 0x090e 0x0908 0x090e 0x0917 0x0907 0x090a

Key2: 0x14 0x4 0x5 0x4 0x5 0x4 0x5 0x5 0x4
*ciphertext2: 0x0913 0x0905 0x0910 0x0906 0x0910 0x0915 0x0909 0x0908

*We have written the hex values of ciphertext character so that the actual mathematical relations may be easily understood.

Set2:
Plaintext: God is great.

Key1: 0x8 0x3 0x5 0x5 0x1 0x5 0x5 0x1 0x5 0x50x5 0x4 0x5
ciphertext1: 0x0918 0x0908 0x090d 0x0909 0x0912 0x090c 0x0905 0x0914 0x0907 0x0912 0x090a 0x090d

Key2: 0x7 0x3 0x5 0x5 0x1 0x5 0x5 0x1 0x5 0x50x5 0x4 0x5
ciphertext2: 0x0917 0x0909 0x090c 0x090a 0x0911 0x090d 0x0918 0x0915 0x0906 0x0913 0x0909 0x090e

5. Analysis of MSMET

As the parameters k, ch map[] and chno[] are now the part of algorithm and are no longer secret, the security entirely lies in the key not on the obscurity of the algorithm. Secondly, the fluctuator arbitrarily changes the value of character, the ciphertext of a character is not unique. Hence it further destroys the frequency pattern of the language in the ciphertext. The ciphertext now also dependent on the fluctuator, there may be different ciphertext of a same plaintext at different times. This further makes difficult for a cryptanalyst to map ciphertext to correct plaintext, thereby making the known plaintext attack more difficult. The changes made in the scheme are put negligible computational overhead. We have therefore ensured an enhanced security without a significant increase in computational complexity.

6. Conclusion

MSMET is the modified MULET with added security. It encompasses all features of MULET with the improved security. As the changes do not alter the structure of the algorithm significantly and computational overhead is also negligible, existing MULET systems can easily be upgraded to MSMET. We are working on more such alteration which can further enhance the security without making it computationally intensive. Apart from it we have also developed a Graphical interface for MSMET which can be obtained from us on request. We are planning to develop an API for MSMET so that it can be easily embedded into other S/w easily.

References

[1] Ross J. Anderson, “Why Cryptosystems Fail", Communications of the ACM,New York, USA, 1994, pp. 32-40.
[2] Brickell, E.F.; Odlyzko, A.M.,Cryptanalysis: a survey of recent results, proc.of IEEE, issue 5 1998, pp. 578-593.
[3] R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,ACM communications 1978.
[4] AES Algorithm ,http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html
[5] Walter Tuchman (1997). A brief history of the data encryption standar,ACM Press/Addison-Wesley Publishing Co. New York, NY, USA. 1997 pp.275{280
[6] G. Praveen Kumar et.al. “MULET :A Multilanguage Encryption Technique”, Seventh International Conference on Information Technology, 2010.
[7] Elliptic Curve Cryptography, Certicom Research, 2000
[8] Unicode Character form http://www.unicode.org
[9] Prasenjit Chaudhary et. al.”A New Multi-language Encryption Technique for MANET”,
[10] Nishu Garg, R.P.Mahapatra. “MANET Security Issues”. IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.
[11] K. Rai et.al.”Different Types of Attacks on Integrated MANET-Internet Communication”,