ISSN 2320 -2610
Volume 5, No.5, September – October 2016
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis01552016.pdf

Optimizing Cipher Text Size for ASCII Based Cryptography Using Matrices

D.R. Sanyasi[1], Dr. A.K. Desai[2]
[1]Gujarat Arts And Science College, Ahmedabad, India, Email: devendrachemical@gmail.com
[2]Gujarat University, Ahmedabad, India, Email: desai_ak@yahoo.com

ABSTRACT

A secret encoding matrix generation scheme based on recursion is presented in this paper which makes the already existing ASCII Based Cryptography more generalized in the sense of security aspect and it also allows the string length of alphanumeric receiver identity to be at most 40. Our generates an encoding matrix whose entries are relatively smaller than its earlier variant and it is further able to put a cap on the size of cipher text generated for sending to the receiver without compromising the security aspect.

Keywords: ASCII Based Cryptography, Ceiling Prime Number, Cryptography with Matrices, Floor Prime Number.

1. INTRODUCTION

Ways and means of secret messaging of information has been of interest for ages now. Some very basic techniques of early cryptography can be even dated to the ancient civilizations [1]. But its basic rise and development can be traced from the world war time onwards [1]-[3]. The security of information has become even more important since the advent of Internet [2]. Sensitive information and transactions like credit card details, social security numbers etc. need to be protected.

In fact, now a day, every bit of data exchange is demanded in a secured manner. To achieve this target, the data is converted into cipher text. There are many schemes already available for such safe and secured exchange of data. The objective of this paper is to generalize the already existing ASCII based cryptographic algorithms for encryption and propose some changes in the already published papers of Gitanjali et al. [4] and Ubhad et al. [5] on the ASCII Based Cryptography. A technique similar to this is suggested and used by Deepa et al. [6] and Kulkarni et al. [7] which uses the concept of colors for encryption. Miller et al. [8] in their paper on Armstrong Numbers have described the density of such numbers on number line. Devi et al. [9] have used Armstrong numbers along with colors for a similar purpose but they pass on their private key between sender and receiver by Diffie Hellman key exchange algorithm. As per the technique proposed by Gitanjali et al. [4] & Ubhad et al. [5], at the start, each receiver is given a unique alphanumeric receiver identity and all these receiver identities are listed in the sender database. The information is changed into its ASCII number equivalent values and it is further converted to cipher text using an encoding matrix given in the papers of Gitanjali et al. [4] & Ubhad et al. [5]. The existing strategy uses some simple matrix operations to hide original information from its unauthentic users and intruders by the use of a key which is generated with the help of alphanumeric receiver identity and a random number sequence. But the method has a restriction on the string length of receiver identity to exactly 4. Also the existing ASCII based cryptography technique requires that the encrypted data along with the random number sequence and alphanumeric receiver identity be together sent for decryption and receiver authentication. But this actually makes the algorithm vulnerable to straight attacks as the secret key can be obtained with the help of random number sequence and receiver identity.

In this paper, we propose an algorithm which allows the string length of receiver identity to be greater or equal to 4 to upto 39. Also with the help of a new modified encoding matrix proposed in this paper, we are able to put a cap on the size of cipher text generated and there is a scope to further extend the definition of encoding matrix to higher dimensions in the similar way if even longer receiver identities are required to be allotted.

1.1. Some Definitions

Encryption [2] is an algorithmic procedure to alter the original form of information into a code which can only be interpreted by its intended recipient and none others without the knowledge of algorithm used for the task. The encrypted code is technically known by the term cipher text.
Decryption [2] is an algorithmic procedure to retrieve the original form of information from its encrypted code. The decrypted code is technically known by the term plaintext.
Private Key [2] is that secret associated with encryption algorithm which does not allow the cipher text to be transformed back to plaintext without its knowledge.
Ceiling Prime Number for an integer n is the smallest prime number greater or equal to n.
Floor Prime Number for an integer n is the largest prime number less than or equal to n.

2. PROPOSED METHOD

Obviously, the bare minimum requirement to send any information by the server would be to know the receivers

identification. At the start, each receiver is given a unique alphanumeric receiver identity and all these receiver identities are listed in the sender database. Suppose the information to be sent is $(D_1, D_2, \dots, D_L)$ for some L where D_i is an ASCII character for each $i \in \{1, 2, \dots, L\}$ and say the recipient is assigned with an alphanumeric receiver identity say $(B_1, B_2, \dots, B_m)$ for some m. Then the encryption would be done as explained below.

2.1 Encryption

2.1.1 First Step - Creating The Ceiling Prime

First of all, the alphanumeric receiver identity is converted into its ASCII equivalent number sequence. Let the ASCII based number conversion of receiver identity is $(b_1, b_2, \dots, b_m)$. Further, a random number sequence of the same length as the alphanumeric identity is generated by the sender say $(r_1, r_2, \dots, r_m)$ and it is added to the alphanumeric receiver identity to obtain the key $(c_1, c_2, \dots, c_m)$
i.e.

$$(b_1, b_2, \dots, b_m) + (r_1, r_2, \dots, r_m) = (c_1, c_2, \dots, c_m) \quad (1)$$

The numbers of this key sequence are added to obtain a k digit number. For this k digit number, a k digit ceiling prime number is selected say λ
i.e.

$$\lambda = \text{Ceiling prime number for } (c_1 + c_2 + \dots + c_m) \quad (2)$$

In case, such a k digit ceiling prime number is not possible for $(c_1 + c_2 + \dots + c_m)$ then λ will be taken as k digit floor prime number for that k digit number $(c_1 + c_2 + \dots + c_m)$. For example: ceiling prime for 9982 is 10007 but there is no 4 digit ceiling prime for 9982. So in such a case the 4 digit floor prime will be taken as value of λ which is 9973.

2.1.2 Second Step – Generating $k \times k$ Encoding Matrix

Define $a_{11}, a_{12}, \dots, a_{1k}$ as the k digits of above number λ respectively. Now we construct a $k \times k$ matrix $A = [a_{ij}]$ whose first row is $a_{11}, a_{12}, \dots, a_{1k}$ and i^{th} row is given by $a_{ij} = a_{(i-1)(j+1)}$ for $j \in \{1, 2, \dots, k-1\}$ with $a_{ik} = a_{(i-1)(1)}$ for all $i \in \{2, 3, \dots, k\}$.

2.1.3 Third Step - Encoding Plaintext (Actual Message) With This Encoding Matrix

The information to be communicated is converted into its ASCII equivalent number sequence. Let this ASCII equivalent of the plaintext message $(D_1, D_2, \dots, D_L)$ be $(d_1, d_2, \dots, d_L)$ for some L including every white space character (if any). A $k \times n$ matrix say B is developed whose entries are taken from the above sequence of numbers where n is decided based on the length of plaintext to be communicated to Bob. $n = \text{ceiling}\left(\frac{L}{k}\right)$ where L denotes length of plaintext including the white space (if any) and ceiling(x) denotes the least integer greater or equal to x. If L is not a multiple of k then, minimum number of characters falling short in preparing matrix B can be taken to be white spaces or any fixed character. Now j^{th} column of A is added to p^{th} column of B for every integer p of type $kq + j$ for $q \in \mathbb{N}$ until this is done in all columns of B. Label this matrix by C. Mathematically speaking; a matrix Y of size equal to matrix B is made using A and then B and Y are added to get matrix C. Finally we obtain matrix $D = AC$. So the ciphered information to be sent is the row-wise element sequence of the matrix D, say, wriiten as $(e_1, e_2, \dots, e_L)$.

2.2 Decryption

2.2.1 First Step – Key Generation

Once the encrypted data is received along with already used random number sequence $(r_1, r_2, \dots, r_m)$, then using the random number sequence and recipient's receiver identity, the key is generated by their addition.

2.2.2 Second Step - Obtaining Secret Decoding Matrix

Using the key generated in previous step, the encoding matrix generation procedure is followed to obtain a matrix (say) E. Then its multiplicative inverse F is computed. F is the secret decoding matrix with the help of which decryption will be done.

2.2.3 Third Step - Obtaining Actual Message

The matrix D is written using cipher text $(e_1, e_2, \dots, e_L)$. Then matrix $G = FD$ is computed. Finally a $k \times n$ matrix H is obtained by subtracting columns of E from columns of G as per the procedure done in Third Step of Encryption section. This gives the matrix H that has original data in the ASCII numbers form, which is then converted to plaintext format.

3. ANALYSING CIPHERTEXT DATA SIZE AND CHECKING MATHEMATICAL FEASIBILITY OF ALGORITHM

In the first step, receiver identity is converted into ASCII number sequence whose range is from 32 to 127. Then a random number sequence is added to it. The range of random numbers in the random number sequence is from 0 to 127. So the range of any number of the key sequence is from 32 to 254. Note that the length of alphanumeric receiver identity is m where $4 \le m \le 39$.

$$\therefore 32m \le \lambda \le 254m$$
$$\implies 128 \le \lambda \le 9906 \quad (3)$$

Since k denotes number of digits in λ

$$\implies 3 \le k \le 4 \quad (4)$$

Also it follows from the very definition of matrix A that

$$\implies 0 \le a_{ij} \le 9 \text{ for each } i, j \text{ where } 1 \le i, j \le k.$$

This suggests that the entries of matrix A are bounded by 9. Similarly, the entries of matrix B are bounded by 127. Therefore the entries of matrix C are bounded by 136. This further implies that the entries of matrix $D = AC$ are bounded by $4 \times 9 \times 136 = 4896$. Further, in the Decryption part of this algorithm, computation of inverse of the encoding matrix is necessary without which it will be difficult to get plaintext. So it is necessary to make sure that the encoding matrix is a non-singular matrix before using it for encryption. Therefore let us analyze matrix A for singularity. For the alphanumeric receiver identity string of length 4 to 39 characters, the λ value generated by the use of key will be of 3 digits or 4 digits only. $\therefore A$ is a square matrix of order either 3×3 or 4×4.

Case(A): If the first row elements of matrix A of order 3×3 are a, b, c then determinant of A denoted by $|A|$ is

$$\begin{aligned} |A| &= 3abc - a^3 - b^3 - c^3 \\ &= -(a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca) \end{aligned} \quad (5)$$

This implies that $|A| = 0$ if and only if choice of a, b, c is such that $a = b = c$. But the choice of a, b, c depends on the ceiling prime number and a number of type

$$aaa = 100a + 10a + a = a \times 111 = a \times 3 \times 37 \quad (6)$$

is never a prime, because 3 divides aaa and so it can never be a ceiling prime number. So the matrix A defined above of order 3×3 is always non-singular.

Case(B): If the first row elements of matrix A of order 4×4 are a, b, c, d then determinant of A denoted by $|A|$ is

$$\begin{aligned} |A| &= -(a + b + c + d)(a - b + c - d)(a^2 + b^2 + c^2 \\ &\quad + d^2 - 2ac - 2bd) \\ &= -(a + b + c + d)(a - b + c - d)\{(a - c)^2 + \\ &\quad + b - d2 \end{aligned} \quad (7)$$

This implies that $|A| = 0$ if and only if the choice of a, b, c, d is such that $a + c = b + d$ or $(a = c \text{ and } b = d)$.
Now, if $(a = c \text{ and } b = d)$, then the ceiling prime number is of type

$$\begin{aligned} abcd &= 1000a + 100b + 10c + d \\ &= 1000a + 100b + 10a + b \\ &= 101(10a + b) \end{aligned} \quad (8)$$

$\Longrightarrow$ 101 divides $abcd$, which is not possible as $abcd$ is a ceiling prime number.
Similarly, if $a + c = b + d$, then the ceiling prime number is of type

$$\begin{aligned} abcd &= 1000a + 100b + 10c + d \\ &= 1000a + 100b + 10c + (a - b + c) \\ &= 11(91a + 9b + c) \end{aligned} \quad (9)$$

$\Longrightarrow$ 11 divides $abcd$, which is not possible as $abcd$ is a ceiling prime number.

So from the above two cases, it is clear that, if the first row elements of matrix A are the digits of ceiling prime number and remaining rows are made as per recursion defined in the "PROPOSED METHOD" then the matrix A is always non-singular. So there is no need to keep any additional restriction here.

4. ILLUSTRATION

Suppose Alice wishes to send information "ARREST THE PRINCESS" to Bob and say Bob is assigned with an alphanumeric receiver identity say AMD7. Then the encryption would be done as shown below.

4.1 Encryption

4.1.1 First Step - Creating The Ceiling Prime

ASCII conversion of AMD7 will be (65, 77, 68, 55). Further, a random number sequence of length 4 is generated at the Alice end say (29, 7, 70, 41) and it is added to the alphanumeric receiver identity as under:
Alphanumeric receiver identity (65, 77, 68, 55) + Random number (29, 7, 70, 41) = (94, 84, 138, 96) (key).
These numbers on addition give a 3 digit number 412. The ceiling prime number for 412 is $\lambda = 419$.

4.1.2 Second Step – Generating 3 × 3 Encoding Matrix

Define a_{11}, a_{12}, a_{13} as the three digits of above ceiling prime number respectively i.e. $a_{11} = 4, a_{12} = 1, a_{13} = 9$ and i^{th} row is given by $a_{ij} = a_{(i-1)(j+1)}$ for $j = 1, 2$ with $a_{i3} = a_{(i-1)(1)}$ for all $i = 2, 3$.

$$\therefore A = \begin{bmatrix} 4 & 1 & 9 \\ 1 & 9 & 4 \\ 9 & 4 & 1 \end{bmatrix}$$

4.1.3 Third Step - Encoding Plaintext (Actual Message) With This Encoding Matrix

The ASCII conversion of "ARREST THE PRINCESS" including every white space character is (65, 82, 82, 69, 83, 84, 32, 84, 72, 69, 32, 80, 82, 73, 78, 67, 69, 83, 83).

$$\therefore B = \begin{bmatrix} 65 & 82 & 82 & 69 & 83 & 84 & 32 \\ 84 & 72 & 69 & 32 & 80 & 82 & 73 \\ 78 & 67 & 69 & 83 & 83 & 32 & 32 \end{bmatrix}$$

Now, j^{th} column of A is added to p^{th} column of B for every integer p of type $kq + j$ for $q \in \mathbb{N}$ until this is done in all columns of B. Label this matrix by C.

$$\therefore Y = \begin{bmatrix} 4 & 1 & 9 & 4 & 1 & 9 & 4 \\ 1 & 9 & 4 & 1 & 9 & 4 & 1 \\ 9 & 4 & 1 & 9 & 4 & 1 & 9 \end{bmatrix}$$

$$\therefore C = B + Y = \begin{bmatrix} 69 & 83 & 91 & 73 & 84 & 93 & 36 \\ 85 & 81 & 73 & 33 & 89 & 86 & 74 \\ 87 & 71 & 70 & 92 & 87 & 33 & 41 \end{bmatrix}$$

Finally, matrix $D = AC$ is obtained which is given below:

$$\therefore D = \begin{bmatrix} 1144 & 1052 & 1067 & 1153 & 1208 & 755 & 587 \\ 1182 & 1096 & 1028 & 738 & 1233 & 999 & 866 \\ 1048 & 1142 & 1181 & 881 & 1199 & 1214 & 661 \end{bmatrix}$$

So the ciphered information sent to Bob is (1144, 1052, 1067, 1153, 1208, 755, 587, 1182, 1096, 1028, 738, 1233, 999, 866, 1048, 1142, 1181, 881, 1199, 1214, 661).

4.2 Decryption

4.2.1 First Step – Key Generation

This is done by addition of the sender generated random number sequence (29, 7, 70, 41) and the ASCII form of recipient's receiver identity (65, 77, 68, 55). Therefore the key generated is (94, 84, 138, 96).

4.2.2 Second Step - Obtaining Secret Decoding Matrix

The encoding matrix (say E) is created using key above and its multiplicative inverse F is computed.

$$\therefore F = \frac{1}{98}\begin{bmatrix} 1 & -5 & 11 \\ -5 & 11 & 1 \\ 11 & 1 & -5 \end{bmatrix}$$

4.2.3 Third Step - Obtaining Actual Message

Taking $G = FD$ we get

$$G = \begin{bmatrix} 69 & 83 & 91 & 73 & 84 & 93 & 36 \\ 85 & 81 & 73 & 33 & 89 & 86 & 74 \\ 87 & 71 & 70 & 92 & 87 & 33 & 41 \end{bmatrix}$$

Further, by subtracting columns of E from columns of G as per the procedure done in Third Step of Encryption section, we get

$$\therefore H = \begin{bmatrix} 65 & 82 & 82 & 69 & 83 & 84 & 32 \\ 84 & 72 & 69 & 32 & 80 & 82 & 73 \\ 78 & 67 & 69 & 83 & 83 & 32 & 32 \end{bmatrix}$$

In this way, a sequence of ASCII numbers thus obtained is (65, 82, 82, 69, 83, 84, 32, 84, 72, 69, 32, 80, 82, 73, 78, 67, 69, 83, 83, 32, 32). Its corresponding ASCII character conversion is “ARREST THE PRINCESS” excluding the last two space characters.

5. CONCLUSION

In this procedure, decryption is done using the recipient's receiver identity. If the receiver is the one intended to be, then with the help of this correct receiver identity, the following would imply:

$E = A \implies G = C \implies H = B \implies$ the data is decrypted successfully. But if the data is received by a wrong receiver, then the matrix E generated in above steps will be different from the actual encoding matrix A because the receiver identity will be different. This in turn will give rise to incorrect secret decoding matrix F, thereby giving incorrect G i.e. $G \neq C$ and will lead to incorrect final matrix H i.e. $H \neq B$. So the actual message will not be obtained by an unintended recipient, thus making this algorithm secured.

Also our analysis shows that no number in the cipher text string is more than 4896, so by the use of this proposed new technique we have achieved our target of extending the length of alphanumeric receiver identity from 4 to atmost 39 and also we have succeeded in controlling the size of cipher text in terms of its length.

ACKNOWLEDGEMENT

The authors would like to acknowledge with deep sense of gratitude the DST-FIST (Department of Science and Technology-Fund for Improvement of Science & Technology infrastructure) support to the Department of Mathematics, Gujarat University, Ahmedabad, where the first author is doing his Ph.D. under the guidance of the second author.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cryptography#cite_note-20.

[2] Abhijit Das and C.E. Veni Madhavan. ***Public Key Cryptography: Theory and Practice***, Pearson Education.

[3] Neal Koblitz, ***A Course in Number Theory and Cryptography***, Springer-Verlag, 1994.

[4] J. Gitanjali, Dr. N. Jeyanthi, C. Ranichandra and M. Pounambal. ***ASCII Based Cryptography Using Unique Id, Matrix Multiplication and Palindrome Number***, The 2014 International Symposium on Networks Computers and Communications, 17-19 June 2014.

[5] S.A. Ubhad, N. Chaubey and S.P. Dubey. ***Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique Id***, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 8, August 2015.

[6] S.P. Deepa, S. Kannimuthu and V. Keerthika. ***Security Using Colors and Armstrong Numbers***, National Conference on Innovations in Emerging Technology, 2011.

[7] Gayatri Kulkarni, Pranjali Gujar, Madhuri Joshi and Shilpa Jadhav. ***Message Security Using Armstrong Numbers and Authentication Using Colors***, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 1, 2014.

[8] Gordon L. Miller and Mary T. Whalen. ***Armstrong Numbers***, University of Wisconsin, Stevens Point, WI 54481, October 1990.

[9] M. Renuga Devi and S. Christobel Diana. ***Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers***, International Conference on Computing and Control Engineering (ICCCE 2012), 12 - 13 April 2012.