ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

An ASCII Value based Optimized Text data Encryption System

Roofee Sultana[1], T.Madhavi Kumari[2]

M.Tech Student, Dept. of ECE, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India[1]

Associate Professor, Dept. of ECE, Jawaharlal Nehru Technological University, Hyderabad, Telangana , India[2]

ABSTRACT: Network security is becoming more and more crucial as the volume of data being exchanged on the internet increases. Security of data and telecommunication can be done by a technique called cryptography. Cryptography is the art and science of study of techniques for secure communication. In cryptography system encryption and decryption techniques are used to convert the plain text or original message to cipher text and cipher text to plaintext respectively. Encryption is considered as the subset of cryptography. Symmetric techniques are used to provide security at higher levels. So we can say that cryptography is an effective way of protecting sensitive information by the way that prevents intruder from reading it. In this proposal we are developing a new cryptography algorithm which is based on symmetric key encryption method. In symmetric key encryption same key is used for encryption and decryption. The main advantage of symmetric key encryption is that management of the key is very simple and easy because only one key is needed .This algorithm uses ASCII values of input data and two keys: One of variable length and other of same length as of input plaintext to encrypt the data. Further logical operation like exclusive-OR, One time padding and Watermarking i.e., Text Image generation (ASCII Art) is performed on encrypted data to increase the level of security

KEYWORDS: Cryptography, ASCII values, Symmetric key encryption, XOR, One-Time pad, ASCII Art.

I.INTRODUCTION

Cryptography has become one of the major methods for protection of data in all applications. It allows users to carry over the confidence found in the physical world to the electronic world. Increase of information transmitted through internet has increased the need of privacy and security of user's data. Cryptography is the best method to avoid unauthorized access of data.

It is the science of writing of data in secret code. It maps the original message in some random fashion which is unintelligible to unauthorized persons. Strength of cryptographic algorithm is defined from the number of attempts by hacker and time taken to break it. It not only protects data from theft or alteration, but can also be used for user authentication.

It is the science of securing data; cryptanalysis is the science of analysing and breaking secure communication. It processes data into unintelligible form, reversibly; so that, data can be recovered without data loss digitally.

The proposed system is aimed at developing a secured system with minimum execution time. The system takes in input data in the form of ASCII values, uses two keys one of variable length and the other of length equal to plaintext length. Computations like XOR, One time padding and Text image creation is used to increase the security. The proposed system is compared with the existing systems to show that the system has minimum execution time with maximum security.

II. RELATED WORKS

Two Encryption Systems are considered for the purpose of comparison of encryption times:

1. Encryption System with Fixed Key length

   The algorithm uses a key of fixed length for the purpose of encryption of the input plain text. It just uses only the XOR Operation and the encryption times are computed for various lengths of plaintext. The key is randomly generated of length 6 and this key is used for encryption process

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

2. Encryption System with Key length equal to plain text length

The standard encryption algorithms DES and AES are considered for this type of encryption system. Both the systems are implemented in Simplified format. In both the cases the key is generated randomly where each character of plain text is encrypted with this key. The key length used for DES is of 10 bit length and that of AES is 16 bit length. The corresponding encryption times are computed for the various plaintext lengths.

III. PROPOSED SYSTEM

The proposed system is mainly aimed at creating a secured system with minimum execution time. For the purpose of security and to meet the security demands of the real world the cipher is converted into text image (ASCII Art).

The proposed system uses basic computations of XOR Operation and One Time padding. The two keys used are randomly generated. The variable key length that is generated in relation with the length of the plain text is used for the XOR Operation and the one time padding operation uses the key with the length equal to plain text length. These are the basic computations that are used in the proposed system.

To show that system has minimum execution time, the system is compared with existing systems. A user interface is created where the user gets to choose between DES and AES for the purpose of comparison along with the fixed key length system.

Encryption time Comparison: DES, Fixed length System, Proposed System (sec)

Length of Plain text	DES	Fixed Key length	Proposed System
40	0.0672	0.0035	0.0032
60	0.0829	0.0042	0.0043
80	0.1098	0.0068	0.0052
100	0.1372	0.0071	0.0062

Encryption time Comparison: AES, Fixed length System, Proposed System (sec)

Length of Plain text	AES	Fixed Key length	Proposed System
40	0.58	0.0032	0.0033
60	0.87	0.0052	0.0042
80	1.15	0.0064	0.0053
100	1.44	0.0069	0.0064

For enhancing the security of the system the cipher so produced after One- time padding is converted into a text image i.e., an ASCII Art is created using a cover image and the cipher so produced and in this form the cipher is very much difficult to be recognised by the cryptanalyst.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

Algorithm:

Encryption:

1. Input the Original Plaintext
2. Get the ASCII values for each characters of the input string
3. Find the minimum ASCII value of the input data
4. Apply the modulus operation on each ASCII value with minimum ASCII value from step 3 and store the resultants in mod content arrays.
5. Generate a key of variable length depending on the length of the input plaintext
6. Get the ASCII values of the generated key
7. Find the minimum ASCII value from step 6
8. Apply modulus opeation on key ASCII values with the minimum value obtained from step 7
9. Perform the right shift of the key one time
10. Now add minimum ASCII value from step 3 to shifted mod key values to obtain key 1
11. Add each mod content of data to final key obtained from step 10
12. Generate the Intermediate cipher 1 from the ASCII Values obtained from step 11
13. Apply the XOR Operation on the intermediate cipher 1 so as to get the intermediate cipher 2
14. Generate a key of length equal to plaintext length for the One time padding which becomes key 2
15. The Intermediate cipher 2 is XORed with the key 2 . This cipher as as the input for the watermarking (ASCII Art) Procedure
16. A cover Image is taken for the purpose of generating an ASCII Art. It is converted into a Grey Intensity Image
17. The Grey Image is resized according to the desired resolution
18. The Grey image is convereted to an Index Image and this is displayed in the command window. This Text Image is the Final Cipher.

Decryption:

1. The ASCII Art Cipher acts as the input .
2. The unique pixel values from the grey cover image are extracted and mapped to the corresponding ASCII Value matrix of the ASCII Art Image (Characters are converted to their corresponding ASCII Values)
3. This gives the ASCII values of lowest pixel values to highest pixel values.Convert this string of ASCII values to characters gives the One time padded Cipher(Intemediate Cipher 2)
4. This Cipher is XORed with key 2 to get Intermedaite Cipher 1(decryption of One Time padding)
5. Reverse XOR operations is performed on this cipher with key 1 and difference between the ASCII values of ciphertext and ASCII values of key 1 is computed
6. Add the minimim cipher to each of the difference to generate the plaintext ASCII values.
7. Obtain the plaintext with the help of these ASCII values.

IV. PERFORMANCE FACTORS

1.Levels of Security: There are three basic levels of security, they being XOR Operation, One Time padding and Watermarking.

XOR operation is provides security in a sense as manipulations are done at the bit level . One time padding generates a random key which varies from one itteration to another itterartion. At the end the cipher is watremarked i.e., it is converted to a text image representation to enhance the cipher's look so that its becomes difficult for the cryptanalysist to extract the cipher from the art.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

By this the security is provided to the cipher in such a way that the attacker cannot recognize the cipher just by looking at it.

2. Security against Brute force attack:

As the two keys generated are completely random and uncorrelated, obtaining only one key does'nt help the attacker to get the plaintext.

As the proposed system has been designed to takes input in sentential format ,as the length of the plaintext increases the number of alternate keys generated also increases

- In case of key1 , let us assume for a plaintext of length 100 the length of key produced is 4+2*(l/10)=24 ,hence key produced is of length 24 characters , the number of altermate keys produced are 24!= 6 x 10^{23} . Typically, only 50% of these need to be exhausted to yield the correct key, hence only 3 x 10^{23} keys need to checked. If we assume the rate of decryption as 1 Decryption/µs ,
  then 3 x 10^{23}µs=9.5 x 10^{11} years. Time required at 10^6 decryptions/µs is 9.5 x 10^5 years.

- In case of key 2 , the length of key produced is for a plaintext length of 100 characters is 100 characters. The number of alternate keys produced are
  100! = 9 x 10^{157}. As only 50% of keys are to be checked then the number of keys are 4.5 x 10^{157}. The rate of decryption as 1 Decryption/µs ,
  then 4.5 x 10^{157}µs= 1.4 x 10^{146} years. Time required at 10^6 decryptions/µs is 4.5 x 10^{140} years.

As huge number of keys are produced and the time required to decrypt them is beyond the time limit for decryption , the proposed algorithm is indeed very much secure and shows less vulnerability to the attacks.

3. **Key Length Management:** In the encryption processing the key management is considerable and important aspect. There are two keys being used one of varaible length key and other a key length equal to plaintext length making the proposed system even more secure than those using only a single key.

V. RESULT AND DISCUSSION

Results:

Bar Graph: Encryption time Comparison: DES, Fixed length System, Proposed System

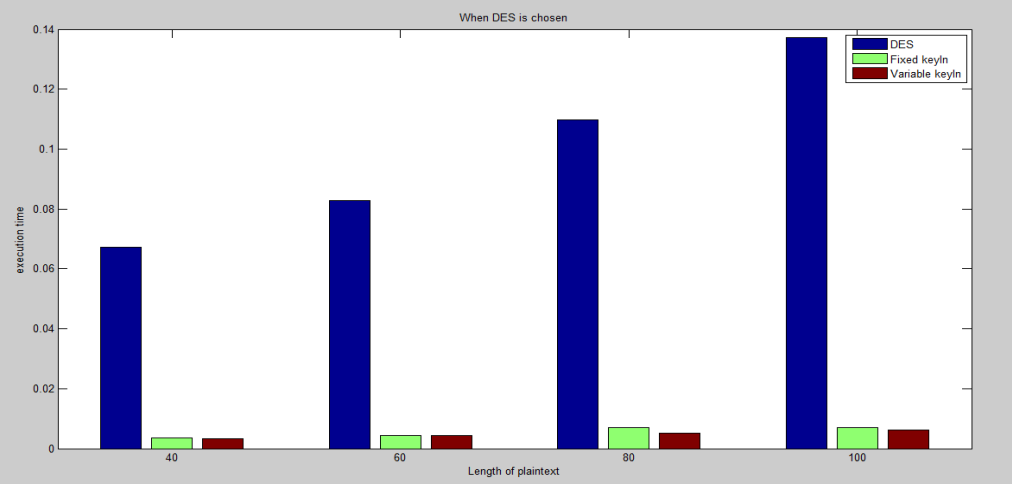

Fig 1 : Encryption time comparison of DES, Fixed length system and proposed system

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

Bar Graph: Encryption time Comparison: AES, Fixed length System, Proposed System

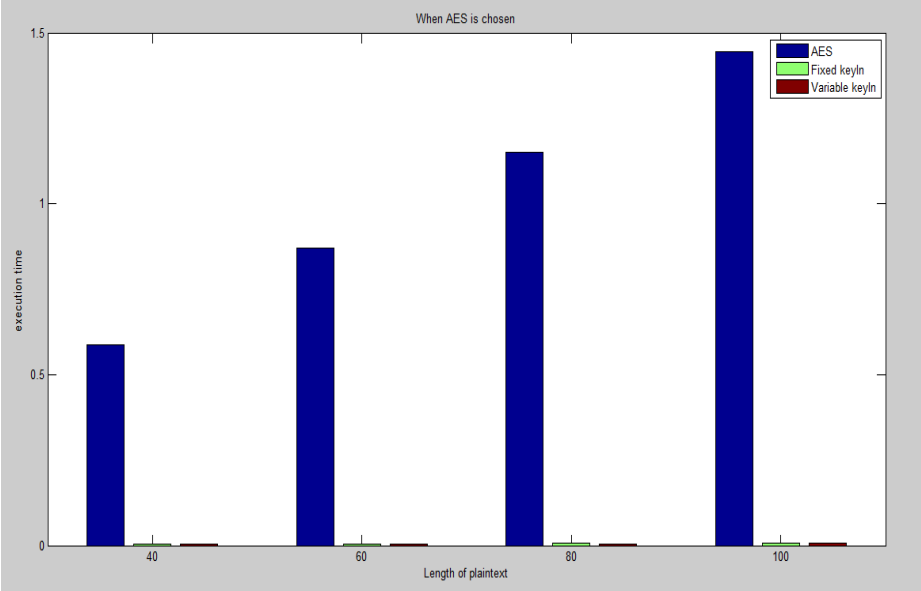

Fig 2 : Encryption time comparison of AES, Fixed length system and proposed system

The encryption times are computed without watermarking the text. This shows that the proposed algorithm has minimum execution time.

Results of proposed system when cipher is water marked for a plaintext of length 98 characters

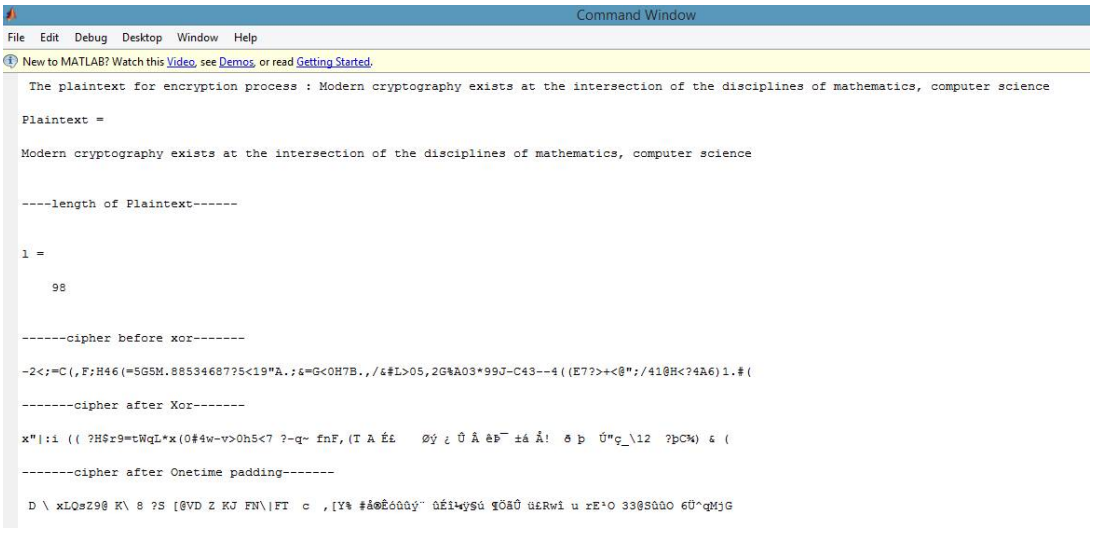

Fig. 1 Ciphers produced while Encryption

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

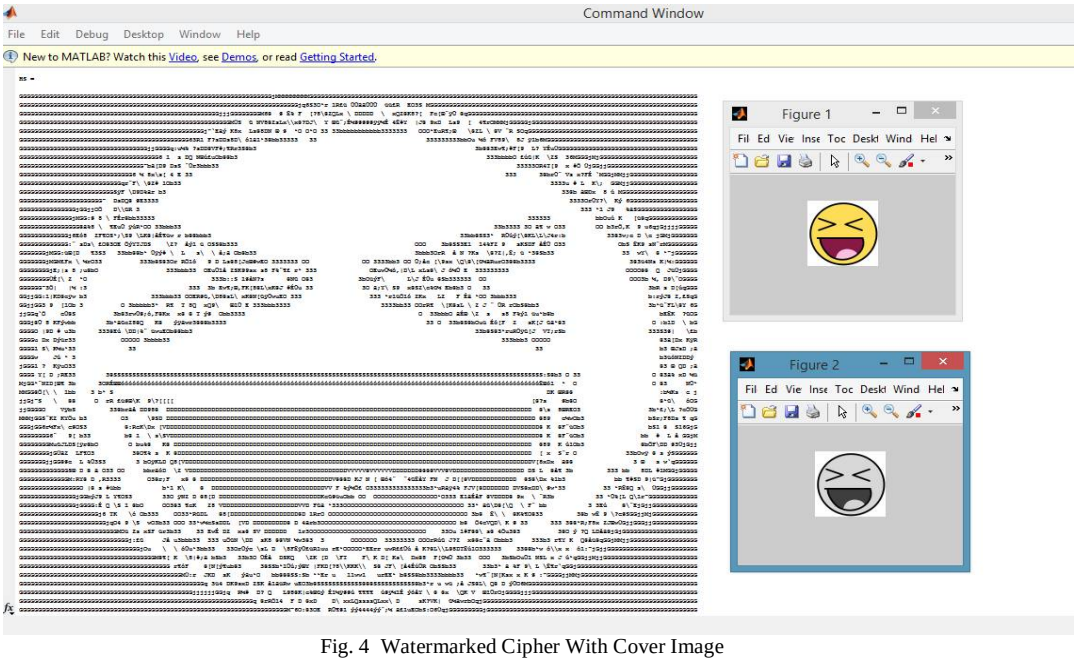

Fig. 4 Watermarked Cipher With Cover Image

```
-------cipher after decrypting watermarking-------

 D \ xLQsZ9@ K\ 8 ?S [@VD Z KJ FN\|FT  c  ,[Y% #å®Ê©ûûý¨ 3Éi¼ÿ§ú ¶ÖãÛ üÉRwî u rE¹O 3û@S:`O 6Ü^qMjG

-------decrypted one time pad--------

x"|:i (( ?H$r9=tWqL*x(0#4w-v>0h5<7 ?-q~ fnF,(T A É£    ØýB¿ Û Â èÞ¯ ±á Å!  ð þ  Ú"ç_ 12I ?þC¾) & (

--------dectypted Xor--------

-2<;=C(,F;H46(=5G5M.885346877?5<19"A.;&=G<0H7B.,/&#L>05,2GiA03*99J-C43--4((E7?>+<@";/ü1@ §?4A6)1.#(

de_plaintext =

Modern cryptography exists at the intersection of the dis iplines of mathematics, co puµÐr science


------- Execution time for variable keylength with Watermarking-------
   10.0278

>>
```

Fig 5 Decryption of ciphers and getting plaintext back

Discussions:

- The main aim of comparison of execution times is to show that the proposed system has a very less execution time although it has more levels of encryption (more number of security levels)
- The cipher is watermarked so as enhance the cipher text in such a way that the cryptanalyst find it difficult to trace the ciphertext from the Text Image(ASCII Art)
- The advantages & disadvantages are:

Advanatges:

1. Can take input data in sentential format.
2. A very much secure system and shows less vulnerability to cryptanalyst attacks

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

3. The keylength changes from one itteration to another itteration making it difficult for attackers to know the key and its length.

Disadvantages:

1. The encryption time of system is a bit more when cipher text is watermarked.(of the order of seconds as compared to milliseconds when not watermarked)
2. The cover image must be resized in accordance with that of the length of input plaintext length.

VI.CONCLUSION

From the results, we analysed that the proposed encryption algorithm producing better results as compared to existing encryption algorithms. Hence the time for encryption and decryption of our proposed algorithm is lesser than existing approaches. As the complexity of the encryption algorithm increases, security also increases but speed decreases.

If any user emphasis on security then they can use our proposed method. The main advantage is that it uses two keys, one of variable length key and other being a key of same length as plain text to make it difficult for intruder to identify. And the generated key is unpredictable till it is not generated. So the security aspect is high and the execution time is lesser as compared to above discussed existing encryption systems. Moreover the cipher produced after performing the XOR operation and One time padding, the obtained cipher is enhanced by transforming it into a text image i.e., ASCII Art creation.

The system can be further extended to encrypt the multimedia data such as audio files, video files and images etc.

REFERENCES

[1] Paramjeet Singh, Shaveta Rani, Efficient *Text Data Encryption System to Optimize Execution Time and Data Security*, IJARCSSE Volume 4, Issue 7, July 2014, ISSN: 2277 128X

[2] Udepal Singh, Upasna Garg, *An ASCII value based text data encryption System* ,IJSRP , Volume 3, Issue 11, November 2013, ISSN 2250-3153

[3] Akanksha Mathur, A Research paper: An *ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms* ,IJCSE, Vol. 4 No. 09 Sep 2012, ISSN : 0975-3397

[4] W.Stallings, *Cryptography and Network Security: Principles and Practices*, Prentice Hall, 1999

[5] V. Vasudha Rani, K. Kanaka Vardhini, *Secure and efficient key ciphering through ASCII codes*, International Journal of Systems, Algorithms & Applications(IJSAA), Volume 3, Issue ICRAET 13, March 2013, ISSN Online: 2277-2677

[6] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption algorithms", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[7] Md. Mizanur Rahman, "Any File Encryption by Translating ASCII Value of Characters", International Journal of Advanced Research in Computer Science(IJARCS), Volume 3, No. 2, March-April 2012, ISSN No. 0976-5697.

[8] V. Gupta, G. Singh, R. Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, Issue 1, January 2012, ISSN: 2277 128X.

[9] Pranab Garg, Jaswinder Singh Dilawari, "A Review Paper on Cryptography and Significance of Key Length", International Journal of Computer Science and Communication Engineering, IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012.

[10] CISSP All-in-One Certification Exam Guide, ch-08: Cryptography.

[11] D. Sravan Kumar, CH. Suneetha, A.Chandrasekhar, "A Block Cipher using Rotation and Logical XOR operations", International Journal of Computer Science, Volume 8: Issue 6,No 1, November 2011.