Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

ASCII Based Arithmetic Operation Technique for Encryption Decryption Process (ABAOT)

Er. Suraj Arya
Research Scholar,
Baba Mastnath University, Rohtak
Haryana, India

Dr. Ankit Kumar
Assistant Professor
Baba Mastnath University, Rohtak
Haryana, India

Abstract: ***Today security is one of the major issues in the field of computers science, each and every system requires more security. Security of various networks and computer applications depends on the cryptography techniques. Many cryptography techniques and algorithms are available and they are used for security purpose in many areas such as the security of ATM cards, computer passwords, and electronic commerce. Thus cryptographic, is the need of the hour so day by day new research and inventions are required. This paper presents the design and working of a new secure cryptographic technique. The main feature of this technique is that it uses the ASCII values of the plain text, and then applies the various mathematics operations on the ASCII values to generate the encrypted text. This technique also uses a data frame which contains all the required information which is used to decrypt the message.***

Keywords: ASCII, DIVIDE

I. INTRODUCTION

Cryptography born along with the art of writing. Cryptography is a combination of two words crypto and graphy. "crypto" means secret and "graphy" stands for writing. Thus it is a technique which is used for secret writing so that a particular message cannot be read by an unauthorized person. Hieroglyph is one of the oldest techniques. 4000 years ago it was used by the Egyptians to communicate. It was a secret code and only known to the scribe who transmit message on the behalf of kings. One such hieroglyph shown in figure 1.

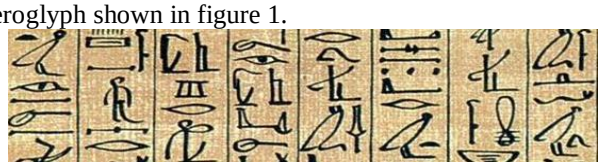

Figure 1: Hieroglyph (Source: www.tutorialspoint.com)

After that mono-alphabetic substitution was in use and starts the use of keys in cryptography system. Then Caesar shift cipher was come into existence, it was based on shifting of letters. The role of cryptography in the modern age is more important as its requirements increase day by day with the popularities of computers and internet. Currently most of the communication done through internet or any other network, so information security is the need of the hour. Cryptography based on plain text, encryption, decryption, keys and algorithms. Plain text means message to be encrypted, encrypted text cannot understand by the unauthorized receiver. Keys used in encryption and decryption process can be divided in two basic categories, symmetric and Asymmetric keys. Symmetric key are those which use same key for encryption and decryption purpose and asymmetric are those which uses different keys for encryption and decryption purpose. Algorithms process plain text in two ways as block cliper and stream cliper. Block cliper process the text as block and output also as block but stream cliper process text character by character at time. Substitution and transposition are the two principles of encryption algorithms .In substitution technique elements of plain text mapped into other elements and in transposition by rearranging of plain text encrypted message can be generated.

II. ENCRYPTION AND DECRYPTION

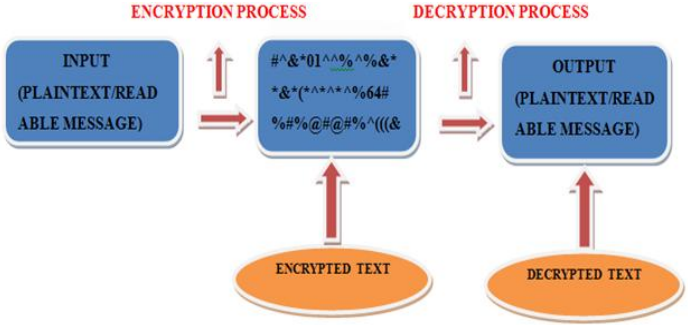

Figure 2: Encryption and Decryption process

© 2016, IJARCSSE All Rights Reserved

III. TYPE OF CRYPTOGRAPHY

- **Symmetric & Asymmetric**

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm secondly in asymmetric cryptography system use different keys for encryption and decryption purpose and the plaintext is recovered from the cipher text[Stallings W., 2005].The two types of attack on an encryption algorithm are cryptanalysis, based on properties of the encryption algorithm, and brute-force. Traditional symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into cipher text elements. Transposition techniques systematically transpose the positions of plaintext elements. Rotor machines are sophisticated recomputed hardware devices that use substitution techniques. Steganography is a technique for hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is known as enciphering or encryption; restoring the plaintext from the ciphertext is deciphering or decryption. The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code."The areas of cryptography and cryptanalysis together are called cryptology[Stallings W., 2005].

IV. SECURITY KEYS

Security keys can classify on the basis of which type cryptography methods adopted by the system. Cryptography methods based on the keys means by using key method can encrypt and decrypt the message. Thus when same key used for encryption and decryption purpose such type of encryption is called symmetric which is based on single key, secret key, and private key. on the other hand when cryptography perform using different key form encryption and decryption purpose such type of cryptography methods called asymmetric and keys used in these systems are known as two keys and public key[Stallings W., 2005].

V. SECURITY ATTACKS

A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation[Stallings W., 2005].

5.1 Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis. The release of message contents is easily understood .A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. Cryptography prevents an opponent from learning the contents of these transmissions. A second type of passive attack, traffic analysis, is subtler. A way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

5.2 Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect [Stallings W., 2005]. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

VI. ASCII BASED ARITHMETIC OPERATION TECHNIQUE (ABAOT)

In which technique sender provide the string then input string read by the method and find the corresponding ASCII values accordingly. Secondly find the string length for example if the string length is 18 then multiply string character's values by 18.In this technique the ASCII values of "DIVIDE" word like D = 68, I = 73, V = 86, I = 73, D = 68, E = 69 then multiply product of these values 68* 73* 86*73*68*69= 146221450464 now message is ready for receiver end. Thus this message consists three parts.

Part 1	Part 2	Part 3

MULTIPLE PRODUCT IS 68*73*86*73*68*69=146221450464

First part shows it is a divide operation it means that original message encrypted with the help of divide operation second part of the data frame show that input string length which is also based on ASCII values. The third part of the frame

© 2016, IJARCSSE All Rights Reserved

shows the encrypted message. Now on the basis of data frame information receiver reads third part and applies the information of part one and two on it. Thus by performing the arithmetic operation on the encrypted message original ASCII values can be generated and further on this basis message can be decrypted.

VII. ADVANTAGES

- No specific key required
- Data frame contains all required information
- Secure as message cannot be decrypted without complete data frame knowledge.3

- **Encryption Process**

Table 1: ASCII values of plain text

S.no	Plain Text	ASCII values
1	R	82
2	a	97
3	m	109
4	Blank Space	32
5	i	105
6	s	115
7	Blank Space	32
8	a	97
9	Blank Space	32
10	B	66
11	o	111
12	y	121

Count the String Length in this example string length is 29.
K =29
Then to encrypt the message multiply the ASCII values of plain text with string length and after that this multiply product consider as encrypted text.

- **Encrypted Message with Header**

146221450464	29,2378,2813,3161,928,3045,3335,928,2813,928,1914,3219,3509

Figure 3: Encrypted Message

Receiver will understand that the multiply product 146221450464 is for divided operation and string length is 29.these two information covers under the first and second part of the data frame.

- **Decryption Process**

Table 2: Decryption Process

S.no	Plain Text	Encrypted Text	ASCII values	Decrypted Message
1	R	2378/	82	R
2	a	2813/	97	a
3	m	3161/	109	m
4	Blank Space	928/	32	Blank Space
5	i	3045/	105	i
6	s	3335/	115	s
7	Blank Space	928/	32	Blank Space
8	a	2813/	97	a
9	Blank Space	928/	32	Blank Space
10	B	1914/	66	B
11	o	3219/	111	o
12	y	3509/	121	y

VIII. CONCLUSION

This technique uses the mathematics properties and ASCII values of the plain text. In this technique the first Step is to find out the ASCII values of the plain text characters including blank spaces then find out the ASCII values of the mathematics operation which is used to encrypt the message and perform the multiple product of the same. Then multiply the string length with the ASCII values of plain text. This technique has a data frame which contains three parts. First part has the details of arithmetic operation, second has string length and third contains the encrypted message. Thus at the receiver end by using header information and applying arithmetic operations on the encrypted message, encrypted text can be decrypt. Thus the major advantage of the technique is that it is not depend on a specific key as data frame has all the required information which is sufficient for decryption process.

© 2016, IJARCSSE All Rights Reserved

REFERENCES

[1] Stallings, W [2005].Cryptography and Network Security Principles and Practice, 4th Edition, Pearson Education Prentice Hall, ISBN 10: 0-13-609704-9 ISBN 13: 978-0-13-609704-4

[2] Bose,Ranjan[2008].Information Theory, Coding and Cryptography, Tata McGraw-Hill Education, ISBN 0070669015, 9780070669017

[3] Gitanjali, J.; Jeyanthi, N.; Ranichandra, C.; Pounambal M(2014) ASCII based cryptography using unique id, matrix multiplication and palindrome number,in Networks, Computers and Communications, The 2014 International Symposium on,. IEEE 2014.

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

[5] Mittal Varun., and Murli Agawarl Piyush(2011). An Encryption and Decryption Algorithm for Messages Transmitted by Phonetic Alphabets; International Conference of Soft Computing and Pattern Recognition. 978-1-4577-1196-1/11/$26.00_c 2011 IEEE

[6] Singh Udepal and Garg Upasna(2013).An ASCII value based text data encryption An ASCII value based text data encryption.International Journal of Scientific and Research Publications, Volume 3, Issue 11,ISSN 2250-3153.

[7] Uddin Palash, Marjan,Abu., Sadia, Nahid Binte and Islam, Rashedul (2014). Developing a Cryptographic Algorithm Based on ASCII Conversions and a Cyclic Mathematical Function. 3rd International Conference on Informatics, Electronics & Vision. 978-1-4799-5180-2/14/$31.00 ©2014 IEEE

© 2016, IJARCSSE All Rights Reserved