International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

ASCII BASED ENCRYPTION DECRYPTION TECHNIQUE FOR INFORMATION SECURITY AND COMMUNICATION

Er. Suraj Arya[1] , Dr.Ankit Kumar [2]

[1]*Research Scholar,Baba Mastnath University, Rohtak, Haryana,(INDIA)*

[2]*Assistant Professor,Baba Mastnath University, Rohtak,Haryana, India*

ABSTRACT

Network communication Security is the emerging field as most of the communication of daily life executes through the internet or any network so network security is the major challenge. Many labs, companies and researchers continue working on it and try to improve the security standards. This paper also presents a cryptography technique which is also used to encrypt decrypt the information. It is an ASCII values based technique which uses the string length and some numerical calculation to perform encryption and decryption.

Keywords: ASCII, RC2, RC4, RC5, DES.

I. INTRODUCTION

The process of encryption and decryption of cryptography can be implemented through different algorithms which have different way to encrypt and decrypt the data by using various types of keys[2][3]. On the basis of these keys cryptography algorithms can be divided in to two major categories semantic and asymmetric algorithms [1]. Algorithms uses the same key for encrypt and encrypt the data is called symmetric algorithms [1].

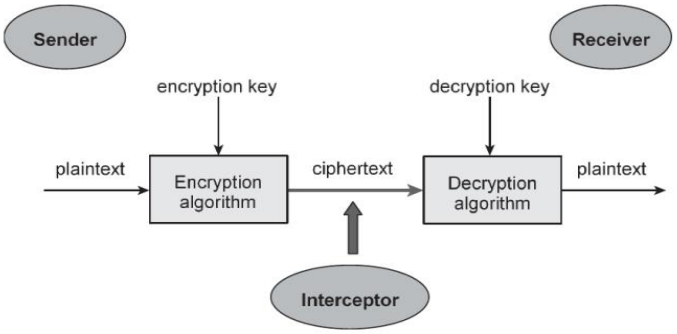

Figure 1: Model of a cryptosystem (Source: www.tutorialspoint.com)

The use of different keys for encrypt and decrypt the data comes under asymmetric cryptography algorithms like RSA, Digital Signature. Block Cipher,strem cliper,RC2,RC4,RC5, Blowfish,DES are example of the symmetric

ISSN (O) 2454-9665
ISSN (P) 2454-0663

cryptography[1] [4][5]. The two major task of cryptography first to perform encryption decryption second to perform information security from intruders. As every time intruders try to attack on the information to get it to destroy it through various type of attacks. These attacks can be divided in to two categories passive and active attacks [6][7][8]. 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 [1] [9].

1.1 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 [15] [1]. Two types of passive attacks are the release of message contents and traffic analysis. The release of message contents is easily understood [1].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 [10] [1].

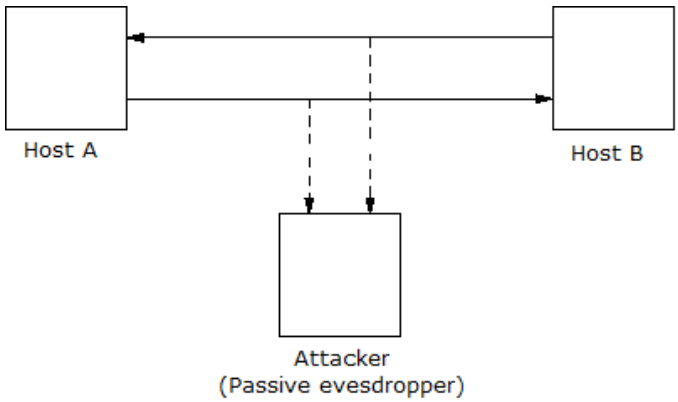

Figure 2: Passive Attacks (Source: Www.Tutorialspoint.Com)

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. The common technique form asking contents is encryption [11] [1].

I.II 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 [14] [1]. 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 [12] [1]. 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 [13] [1].

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

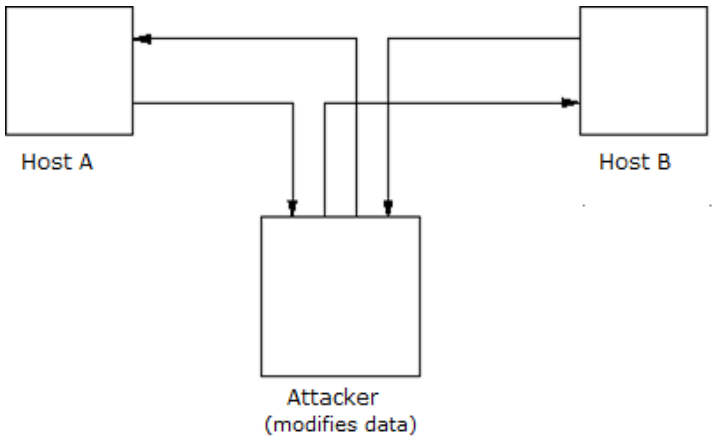

Figure 3: Active attacks (Source: www.tutorialspoint.com)

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect [1].

II. ASCII BASED ENCRYPTION DECRYPTION TECHNIQUE (ABEDT)

It is a ASCII value based technique at first it find out the ASCII value of the message and calculate the string length which is also based on ASCII values.

N= length of Input string

In this technique string length (N) adds in the ASCII values of the input string in the incremental way. For example if the string length is 26 then technique will add 26 in the first character of the first word of N and add 27 add in the second character,28,29 add in the third and corresponding fourth character thus it is a incremental addition after that technique will find out the symbols and characters as per ACSII values which is produce by the technique after addition operation. then this information sent to the receiver end. Receiver knows the original length of the string then receiver calculate these values at receiver end by performing the subtract operation which is based on string length in a way that receiver subtract 26 from the first character and 27 from second character and 28 and 29 from third and fourth character and so on till the original message not decrypted at the receiver end. Thus after completion this process decrypted message will be display on the screen.

Advantages

- This technique is not limited to any specific key and tables or symbols
- It can Encrypt and decrypt any text which has ASCII values.
- It is secure technique as intruder cannot interpret message easily.
- Lesser information required for encryption and decryption process as by knowing string length whole process can be completed.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

III. ENCRYPTION PROCESS

For example

Step 1

Plain Text: "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG"

This input string contains all alphabets.

Step 2

Characters	ASCII Values	Characters	ASCII Values	Characters	ASCII Values
T	84		32	Y	89
H	72	J	74		32
E	69	U	85	D	68
	32	M	77	O	79
Q	81	P	80	G	71
U	85	S	83		
I	73		32		
C	67	O	79		
K	75	V	86		
	32	E	69		
B	66	R	82		
R	82		32		
O	79	T	84		
W	87	H	72		
N	78	E	69		
	32		32		
F	70	L	76		
O	79	A	65		
X	88	Z	90		

Table 1: Encryption phase-1

Step 3

STRING LENGTH

K =86

Step 4

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

IV. ENCRYPTION PROCESS

Encryption Process						
T	=	84	+	86	=	170
H	=	72	+	87	=	159
E	=	69	+	88	=	157
		= 32 + 89 = 121				
Q	=	81	+	90	=	171
U	=	85	+	91	=	176
I	=	73	+	92	=	165
C	=	67	+	93	=	160
K	=	75	+	94	=	169
	= 32 + 95 = 127					
B	=	66	+	96	=	162
R	=	82	+	97	=	179
O	=	79	+	98	=	177
W	=	87	+	99	=	186
N	=	78	+	100	=	178
	= 32 + 101 = 133					
F	=	70	+	102	=	172

ISSN (O) 2454-9665
ISSN (P) 2454-0663

O	=	79	+	103	=	182
X	=	88	+	104	=	192
		= 32 + 105 = 137				
J	=	74	+	106	=	180
U	=	85	+	107	=	192
M	=	77	+	108	=	185
P	=	80	+	109	=	189
S	=	83	+	110	=	193
	= 32 + 111 = 143					
O	=	79	+	112	=	191
V	=	86	+	113	=	199
E	=	69	+	114	=	183
R	=	82	+	115	=	197
T	=	84	+	117	=	201
H	=	72	+	118	=	190
E	=	69	+	119	=	188
L	=	76	+	121	=	197
A	=	65	+	122	=	187
Z	=	90	+	123	=	213
Y	=	89	+	124	=	213

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

	= 32 + 125 = 157					
D	=	68	+	126	=	194
O	=	79	+	127	=	206
G	=	71	+	128	=	199

Table 2: Encryption phase-II

V. ENCRYPTED TEXT

ªŸ • y«°¥ ©□¢³±º²…¬¶À‰´À¹½Á□ ¿Ç·Å”É¾¼˜Å»ÕÕ□ ÂÎÇ

VI. DECRYPTION PROCESS

T = 84 + 86 = 170 = ª = 170 - 86 = T	
H = 72 + 87 = 159 = Ÿ = 159 - 87 = H	
E = 69 + 88 = 157 = • = 157 - 88 = E	
= 32 + 89 = 121 = y = 121 - 89 =	
Q = 81 + 90 = 171 = « = 171 - 90 = Q	
U = 85 + 91 = 176 = ° = 176 - 91 = U	
I = 73 + 92 = 165 = ¥ = 165 - 92 = I	
C = 67 + 93 = 160 = = 160 - 93 = C	
K = 75 + 94 = 169 = © = 169 - 94 = K	
= 32 + 95 = 127 = □ = 127 - 95 =	
B = 66 + 96 = 162 = ¢ = 162 - 96 = B	
R = 82 + 97 = 179 = ³ = 179 - 97 = R	
O = 79 + 98 = 177 = ± = 177 - 98 = O	
W = 87 + 99 = 186 = º = 186 - 99 = W	
N = 78 + 100 = 178 = ² = 178 - 100 = N	
= 32 + 101 = 133 = … = 133 - 101 =	
F = 70 + 102 = 172 = ¬ = 172 - 102 = F	
O = 79 + 103 = 182 = ¶ = 182 - 103 = O	
X = 88 + 104 = 192 = À = 192 - 104 = X	

ISSN (O) 2454-9665
ISSN (P) 2454-0663

	=	32	+	105	=	137	=	‰	=	137	-	105	=	
J	=	74	+	106	=	180	=	´	=	180	-	106	=	J
U	=	85	+	107	=	192	=	À	=	192	-	107	=	U
M	=	77	+	108	=	185	=	¹	=	185	-	108	=	M
P	=	80	+	109	=	189	=	½	=	189	-	109	=	P
S	=	83	+	110	=	193	=	Á	=	193	-	110	=	S
	=	32	+	111	=	143	=	•	=	143	-	111	=	
O	=	79	+	112	=	191	=	¿	=	191	-	112	=	O
V	=	86	+	113	=	199	=	Ç	=	199	-	113	=	V
E	=	69	+	114	=	183	=	·	=	183	-	114	=	E
R	=	82	+	115	=	197	=	Å	=	197	-	115	=	R
	=	32	+	116	=	148	=	”	=	148	-	116	=	
T	=	84	+	117	=	201	=	É	=	201	-	117	=	T
H	=	72	+	118	=	190	=	¾	=	190	-	118	=	H
E	=	69	+	119	=	188	=	¼	=	188	-	119	=	E
	=	32	+	120	=	152	=	˜	=	152	-	120	=	
L	=	76	+	121	=	197	=	Å	=	197	-	121	=	L
A	=	65	+	122	=	187	=	»	=	187	-	122	=	A
Z	=	90	+	123	=	213	=	Õ	=	213	-	123	=	Z
Y	=	89	+	124	=	213	=	Õ	=	213	-	124	=	Y
	=	32	+	125	=	157	=	•	=	157	-	125	=	
D	=	68	+	126	=	194	=	Â	=	194	-	126	=	D
O	=	79	+	127	=	206	=	Î	=	206	-	127	=	O
G	=	71	+	128	=	199	=	Ç	=	199	-	128	=	G
	=	32	+	125	=	157	=	•	=	157	-	125	=	
D	=	68	+	126	=	194	=	Â	=	194	-	126	=	D
O	=	79	+	127	=	206	=	Î	=	206	-	127	=	O
G	=	71	+	128	=	199	=	Ç	=	199	-	128	=	G

VII. CONCLUSION

This technique is based on ASCII values. ASCII characters are used for encryption and decryption with string length followed by numerical calculations. To break this technique intruder requires much information about the plain text only single information like string length, , is not sufficient to break this technique. The use of variant string length makes the technique more robust. Further operations apply and depend on the string length. Thus this technique is not depends on any specify key or key generation method it is the strength of the technique.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

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 Educatio*n, 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

[8]. http://www.webopedia.com/TERM/C/cryptography.html

[9]. http://www.wisegeek.org/what-is-cryptography.htm

[10].http://searchsoftwarequality.techtarget.com/definition/cryptography

[11].http://www.garykessler.net/library/crypto.html

[12].http://slayeroffice.com/tools/ascii/

[13].http://ee.hawaii.edu/~tep/EE160/Book/chap4/subsection2.1.1.1.html

[14].http://www.theasciicode.com.ar/extended-ascii-code/letter-i-umlaut-diaeresis-i-umlaut-lowercase-ascii-code-139.html

[15].www.tutorialspoint.com