IMPLEMENTATION OF ASCII BASED INFORMATION HIDING TECHNIQUE TO PERFORM THE SECURE COMMUNICATION BETWEEN SENDER AND RECEIVER

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

TYPES OF CRYPTOGRAPHIC TECHNIQUES

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are in following figure. [16][17][18][19].

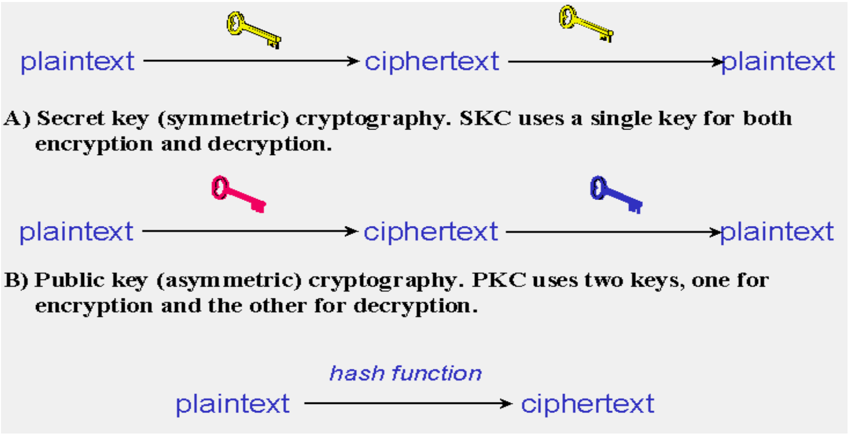
plaintext
ciphertext
plaintext
A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.
plaintext
ciphertext
plaintext
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.
hash function
plaintext
ciphertext

Figure: 1 Type of Cryptographic Algorithms (Source : http://www.garykessler.net/library/crypto.html)

I.I Public-Key Cryptography

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key[16][17][18][19].

I.II Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key (Figure 1C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file[16][17][18][19].

I.III Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key[16][17][18][19].

IV. ASCII BASED ENCRYPTION DECRYPTION TECHNIQUE (ABEDT)

It is a ASCII based technique In which sender enters the string then method find the correspondence ACSII values of the input string and calculate the string length which is also based on ASCII values then find the last digit of the string length and consider it ZERO “0” and perform the following operation.

$$N+NK$$

Where N=original length of Input string

NK= length of string after consider last digit as “0”

For example if the string length is 26 then NK=20.Addition of N+NK adds in the ASCII values of the input string in the incremental way. For example if the addition of N+NK is 26 then technique will add 26 in the first character of the first word of N then 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 and also aware about the operation N+NK then receiver calculate these values at receiver end by performing the subtract operation 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 generated 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
- ASCII based encryption decryption.
- 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.

IV.I. 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)

K =86

Step 4

New string length is(N)

N =80

Step 5

Addition of string length and new string length.

K+N =166

Step 6 Encryption Process

Incremental Addition [Character old ASCII + (K+NK) =New ASCII Value]

IV.II Encryption Process

T	**=**	**84**	**+**	**166**	**=**	**250**
H	=	72	+	167	=	239
E	=	69	+	168	=	237
= 32 + 169 = 201						
Q	=	81	+	170	=	251
U	=	85	+	171	=	256
I	=	73	+	172	=	245
C	=	67	+	173	=	240
K	=	75	+	174	=	249
B	=	66	+	176	=	242
R	=	82	+	177	=	259
O	=	79	+	178	=	257
W	=	87	+	179	=	266
N	=	78	+	180	=	258
F	=	70	+	182	=	252
O	=	79	+	183	=	262
X	=	88	+	184	=	272
= 32 + 185 = 217						
J	=	+		186	=	260
U	=	85	+	187	=	272
M	=	77	+	188	=	265

P	=	80	+	189	=	269
S	=	83	+	190	=	273
	=	**32**	**+**	**191**	**=**	**223**
O	=	79	+	192	=	271
V	=	86	+	193	=	279
E	=	69	+	194	=	263
					=	
R	=	82	+	195	=	277
	=	**32**	**+**	**196**	**=**	**228**
T	=	84	+	197	=	281
H	=	72	+	198	=	270
					=	
E	=	69	+	199	=	268
	=	**32**	**+**	**200**	**=**	**232**
					=	
L	=	76	+	201	=	277
					=	
A	=	65	+	202	=	267
					=	
Z	=	90	+	203	=	293
					=	
Y	=	89	+	204	=	293
	=	**32**	**+**	**205**	**=**	**237**
					=	
D	=	68	+	206	=	274
					=	
O	=	79	+	207	=	286
					=	
G	=	71	+	208	=	279

Table 2: Encryption phase-II

Step 7:

International Journal of Science Technology and Management
Vol. No.6, Issue No. 01, January 2017
www.ijstm.com
ISSN (O) 2394 - 1537
ISSN (P) 2394 - 1529

ENCRYPTED TEXT

úïíÉûõðùÏòÕüÙ

Step 8:

IV.III DECRYPTION PROCESS

T	=	84	+	166	=	250	=	ú	=	250	-	166	=	T
H	=	72	+	167	=	239	=	ï	=	239	-	167	=	H
E	=	69	+	168	=	237	=	í	=	237	-	168	=	E
	=	32	+	169	=	201	=	É	=	201	-	169	=	
Q	=	81	+	170	=	251	=	û	=	251	-	170	=	Q
U	=	85	+	171	=	256	=		=	0	-	171	=	U
I	=	73	+	172	=	245	=	õ	=	245	-	172	=	I
C	=	67	+	173	=	240	=	ð	=	240	-	173	=	C
K	=	75	+	174	=	249	=	ù	=	249	-	174	=	K
	=	32	+	175	=	207	=	Ï	=	207	-	175	=	
B	=	66	+	176	=	242	=	ò	=	242	-	176	=	B
R	=	82	+	177	=	259	=		=	3	-	177	=	R
O	=	79	+	178	=	257	=		=	1	-	178	=	O
W	=	87	+	179	=	266	=		=	10	-	179	=	W
N	=	78	+	180	=	258	=		=	2	-	180	=	N
	=	32	+	181	=	213	=	Õ	=	213	-	181	=	
F	=	70	+	182	=	252	=	ü	=	252	-	182	=	F
O	=	79	+	183	=	262	=		=	6	-	183	=	O
X	=	88	+	184	=	272	=		=	16	-	184	=	X
	=	32	+	185	=	217	=	Ù	=	217	-	185	=	
J	=	74	+	186	=	260	=		=	4	-	186	=	J
U	=	85	+	187	=	272	=		=	16	-	187	=	U
M	=	77	+	188	=	265	=		=	9	-	188	=	M
P	=	80	+	189	=	269	=		=	13	-	189	=	P
S	=	83	+	190	=	273	=		=	17	-	190	=	S
	=	32	+	191	=	223	=	ß	=	223	-	191		
O	=	79	+	192	=	271	=		=	15	-	192	=	O
V	=	86	+	193	=	279	=		=	23	-	193	=	V
E	=	69	+	194	=	263	=		=	7	-	194	=	E
R	=	82	+	195	=	277	=		=	21	-	195	=	R
	=	32	+	196	=	228	=	ä	=	228	-	196	=	

T	=	84	+	197	=	281	=		=	25	-	197	=	T
H	=	72	+	198	=	270	=		=	14	-	198	=	H
E	=	69	+	199	=	268	=		=	12	-	199	=	E
	=	32	+	200	=	232	=	è	=	232	-	200		
L	=	76	+	201	=	277	=		=	21	-	201	=	L
A	=	65	+	202	=	267	=		=	11	-	202	=	A
Z	=	90	+	203	=	293	=	%	=	37	-	203	=	Z
Y	=	89	+	204	=	293	=	%	=	37	-	204	=	Y
	=	32	+	205	=	237	=	í	=	237	-	205	=	
D	=	68	+	206	=	274	=		=	18	-	206	=	D
O	=	79	+	207	=	286	=	-	=	30	-	207	=	O
G	=	71	+	208	=	279	=		=	23	-	208	=	G

V. IMPLEMENTATION ASCII BASED ENCRYPTION DECRYPTION TECHNIQUE (ABEDT)

ASCII Based Encryption Decryption Technique (ABEDT)-II, implemented with the help of PHP (Personal Home Page) programming language with the help of a example & interface, as the string enter and click on submit button then algorithm will execute and perform the encryption decryption operations.

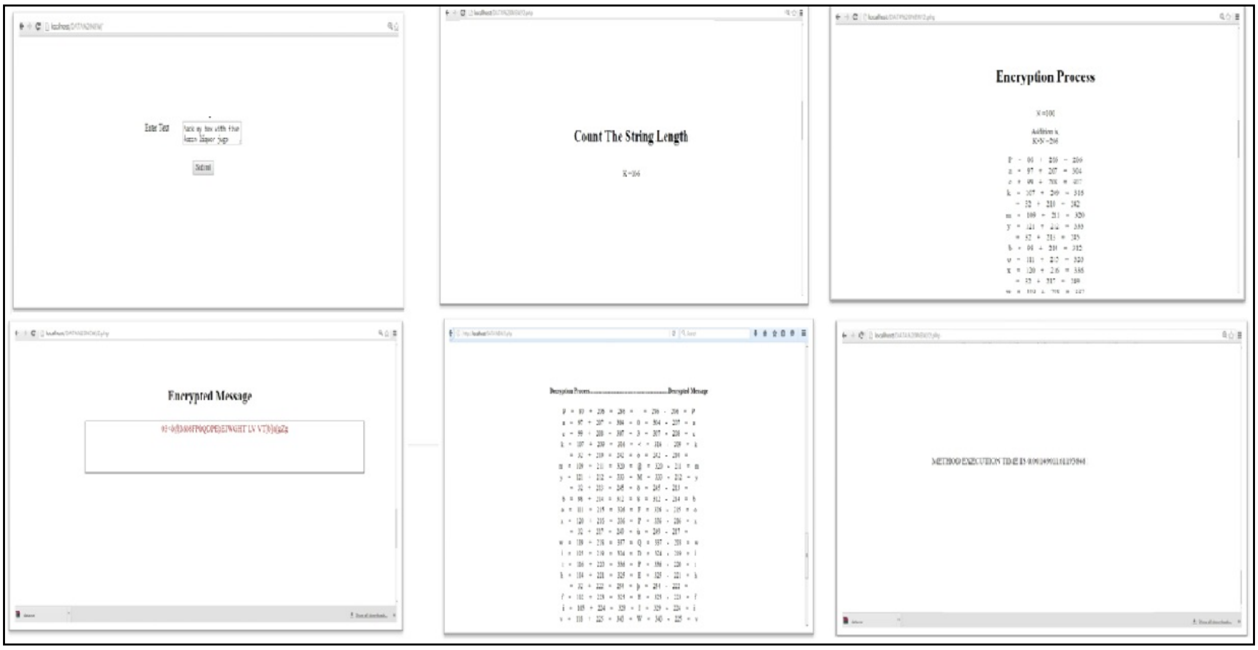

Figure: Implementation of the technique

VI. 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 unique strength of the technique.

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

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

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

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

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