Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2

Satish Kumar Garg
Govt. P G College Ambala Cantt - 133001
Haryana, India

Abstract - In the present work the author has introduced a modified symmetric key cryptographic method, called algorithm SKG 1.2, for data encryption and decryption of any file using symmetric key at two stages (1) by swapping the characters in the string of text and (2) by shifting the characters to left or right. The present method can be applied to encrypt any data consisting of 30 or more characters. The results obtained after application of algorithm SKG 1.2 are excellent and difficult to decryt.

Keywords: Encryption, Decryption, swapping of Characters, Shifting Characters to Left or Right

I. INTRODUCTION

In today's global scenario, the internet technology [1,2] is used almost in every field, specially for transmission of information. So it has become a real challenge for the sender to send confidential data from one computer to another computer. The security and originality of data [1] has now become very challenging because there is always a possibility that anyone may intercept our data. It is not safe to send confidential data from one computer to another computer. The confidential data may be bank statements, bank transaction, military information, confidential data of companies etc. So, the data should be protected from any unwanted intruder otherwise any massive disaster may happen all on a sudden. In order to make secure the system one should consider the security primary attributes such as confidentiality, integrity, availability etc. and secondary attributes such as authenticity, non-repudiation, accountability etc. There are a large number of methods and techniques to achieve security goals, one of these is Cryptography. Cryptography [3,4] is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques. The cryptographic algorithm can be classified into two categories: (i) Symmetric Key Cryptography where one key is used for both encryption and decryption purpose. (ii) Public Key Cryptography where two different keys are used, one for encryption and the other for decryption purpose. Due to massive computation the public key crypto system may not be suitable in security of data in sensor networks [5]. The author has developed an algorithm named as algorithm SKG 1.0 which is successful for encrypting any text/string consisting of 30 or more characters [6]. In the present work, modified algorithm SKG 1.2 is obtained by interchanging the steps 1 and 2 of algorithm SKG 1.1.

II. THEORY

We know that N characters can be re-arranged in N! ways. In the present work, the author has selected one such re-arrangement of N characters in two stages :

Stage 1 : By swapping integral multiples of leftmost N1st character with integral multiples of rightmost N1st character, such that if (N+1) is divisible by N1, swapping should be implemented upto N/2 characters otherwise upto Nth character.

Stage 2 : By shifting N2 leftmost characters to rightmost in circular queue or vice versa.

ENCRYPTION ALGORITHM (MENU DRIVEN GUI PROGRAM)

// Read the text input and check length of Input, if less than 30, give error message

Step 1: Start
Step 2: Read input text N
Step 3: If (N.length()< 30)
Print error message that program is not applicable;

// Interchange the leftmost integral multiple of N1 characters with corresponding rightmost N1 characters

Step 4: initialize integer j (to store length to be traversed [loop through])
Step 5: Read value of N1
Step 6: integer r = remainder of (N+1)modulus N1

Step 7: if (r==0)
j = N/2;
else
j = N;
Step 8: for(i=1;N1*i<=j;i++)
{
ch = charAt(N1*i-1);
Replace/ set charAt((N1*i)–1)th position with charAt((N+1)-(N1*i))th position;
Replace/ set charat(N+1)-(N1*i))th position with char stored in variable 'ch';
}
// Shift leftmost N2 characters to rightmost of the string of characters and vice versa)
Step 9: Read value of N2 and Shifting
Step 10: initialize array a1[l]// of length of total characters stored in step 8
Step 11: If shifting rightmost characters to leftmost, then go to step 13
Step 12: If shifting leftmost characters to rightmost
for each character starting from (N2+1) to N
copyeach character bit to array a1
for each character starting from 1st character upto N2
copy(append) each character to a1
Step 13: for each character starting from ((N+1)- N2) to N
copy each character to array a1
for each character starting from 1st character to (N-N2) character
copy (append) each character to a1
Step 14: print and return final result to output file **// return the final string**
Decryption Algorithm is just reverse of the Encryption Algorithm

III. RESULT AND DISCUSSION

The algorithm SKG 1.2 is successful for encrypting any text/string consisting of 30 or more characters. Any text/string consisting of 30 characters will on the average contain 6 or more different characters, so minimum number of possible re-arrangements shall be $30!/(5!)^6 = 8.88\times10^{19}$. The available Super Computer is teraflop computer which is capable of performing 10^{12} floating point calculations per sec, so to perform all 8.88×10^{19} calculations, time required is 1028 days, which is sufficiently large to decrypt any text [6].

IV. IMPLEMENTATION OF ALGORITHM SKG 1.2

The author has implemented the said algorithm SKG 1.2 on Java platform for different values N(=30 to 1000) each for different values of N1 (= 1 to N/3) and N2 (= 1 to N-1) .
e.g., for input text :
Located in Kurukshetra, the land of Bhagwadgita, Kurukshetra University is a premier institute of higher learning in India. Its foundation stone was laid on January 11, 1957 by Bharatratna Dr. Rajender Prasad, the first President of the Indian Republic.
The output is given Table 1. From Table 1, it is clear that if we change even a single variable (N1, N2 or direction of shifting the characters either Left or Right) then output of the Algorithm SKG 1.2 is entirely different. Further for the same values of N1, N2 and direction of shifting the characters, output of algorithms SKG 1.1[7] and SKG 1.2 are entirely different.

V. CONCLUSION

The proposed scheme named as algorithm SKG 1.2 was tested on Java platform for different values of N (=30 to 1000) each for different values of N1(= 1 to N/3), N2 (= 1 to N-1) and left /right directions of shifting the characters. In all cases the result came as per the literature. It has been estimated that to crack the code we will require more time than the data will reside on the medium to travel. So, it can be said that the proposed scheme will produce an efficient secured algorithm for data transfer in both wired and wireless networks.

S. No.	N1	N2	Encrypted Output Text Using Algorithm SKG 1.2	Encrypted Output Text Using Algorithm SKG 1.1
1.	3	3 Left	atbd en nurdks etta,othn lindroftBhigwedg taa Krrurshntra U.iv rsttytisaa re ie9 i,st tuae af nigderllearnengtinnIntian Ifs tou.dadio s oni was aih oh Jonutryi11n 1r57mbypBh ra rainaeDrn Rajeedek Puas,d,itha fars P esadeet f rhehInuiaK Ripuelic. Loc	atLd cn bureksnetda, tht londnofiBhrgwtdgitae K ruashrtrr Univars.ty ista treaie i st9tu,e f aigaernledrnlngaineIntian Its noufdatio. sdon w s iaia o Jhnuhryo11t 1i57nbyrBhmrapra na Dri Rejendea Peaskd,uth, firsa Paes de t af ehe Inriah RupuKlii. eoc

2.	5	3 Left	aled iR Kurdkshehra, he lind o Bhafwadg ta, aurukehetra UniDersiay isaa prbmier1inst tutenof hogherllear ing sn Intia. ots fIundadion itonenwas aid in Ja uaryi11, 957 ey Bh ratrttna vr. Rajendsr PrKsad,ithe girstfPresadenttof tte Inuian nepubtic. Loc	ated.in KuruksnetraI the landnof Beagwasgitae KurdkshePra Univer ity as a tremiBr in7titu,e ofrhighJr ledrnins in nndian Itsdfoun atio. stoIe wag laia on eanua y 11t 195s by eharapratni Dr.sRajender trasau, th, firdt Prhside t of the ,ndiah Republic Loc
3.	10	3 Right	c. Localed iR Kurdkshehra, he lind o Bhafwadg ta, aurukehetra UniDersiay isaa prbmier1inst tutenof hogherllear ing sn Intia. ots fIundadion itonenwas aid in Ja uaryi11, 957 ey Bh ratrttna vr. Rajendsr PrKsad,ithe girstfPresadenttof tte Inuian nepubti	c. Lpcatea in urukfhetre, thr lanr of hhagwadgit , Kueuksh.tra nniveasity is a5prem1er iastit te oi higaer loarniog innIndis. Ita fou datinn stene whs lafd onuJanunry 1i, 19 7 by BharrtratUa Dre RajrnderaPrasad, tBe fidst Peesidant os theKIndidn Reoubli

Table 1 : Comparison of Encrypted Output Text Using Algorithms SKG 1.2 and SKG 1.1

REFERENCES

[1] Satish Kumar Garg, "Review of Secured Routing for Wireless Ad hoc Network", *International Journal of Computing and Business Research*, Vol. 2 Issue 1, January 2011.

[2] Satish Kumar Garg, "Wireless Network Security Threats", *International Journal of Information Dissemination and Technology*, Vol. 1 Issue 2, April-June 2011

[3] T. Karygiannis and L. Owens, *Wireless Network Security*, NIST Special Publication, 2002

[4] William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 5th Edition, 2011.

[5] R. H. Karpinski, "Reply to Hoffman and Shaw", *Datamation*, Vol. 16(10) p. 11 (Oct. 1970)

[6] Satish Kumar Garg, "Information Security By Interchanging Characters: Algorithm SKG 1.0", *International Journal of Information Technology and Knowledge Management*, Vol. 6 Issue 2, 2013.

[7] Satish Kumar Garg, "An Integrated Symmetric Key Cryptosystem : Algorithm SKG 1.1", *International Journal of Information Technology and Knowledge Management*, Vol. 76 Issue 2, 2014.

