IJITKM Volume 7 • Number 2 • Jan – June 2014 pp. 17-19 (ISSN 0973-4414)

An Integrated Symmetric Key Cryptosystem: Algorithm SKG 1.1

Satish Kumar Garg
Govt. P G College Ambala Cantt - 133001 (Haryana) India
E-mail : sat.phy@gmail.com

Abstract
In the present work the author has introduced a new symmetric key cryptographic method, called algorithm SKG 1.1, for data encryption and decryption of any text file using symmetric key at two levels (1) by shifting the N_1 leftmost characters to right in circular in circular queue or vice versa and (2) by swapping the N_2^{th} leftmost character in the string of text with N_2^{th} rightmost character. This method can be applied to encrypt any data consisting of 30 or more characters. The results obtained after application of this algorithm are difficult to decryt.
Keywords: Encryption, Decryption, swapping of Characters, Shifting Characters to Left or Right

1. INTRODUCTION :

With the increased use of technology specially internet [1,2], 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. Hence the data should be protected from any unwanted intruder otherwise any massive disaster may happen all on a sudden. There are a large number of methods and techniques to achieve security goals, one of these is Cryptography. Cryptography is the process used to make a meaningful message appear meaningless. It [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 cryptography 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, algorithm SKG 1.1, the author has added another level of security, that is, at first level there is shifting of the characters to left or right and at second level there is swapping of characters. The algorithm SKG 1.1 is more effective as compared to algorithm SKG 1.0 for encrypting any text/string consisting of 30 or more characters.

2. 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 at two levels : Level 1 : By shifting N1 leftmost characters to right in a circular queue or vice versa. Level 2 : By swapping N_2^{nd} leftmost character with N_2^{nd} rightmost character in integer multiples of N_2, such that N_2 is not equal to 1, 2 and if (N+1) is divisible by N_2, swapping should be implemented upto N/2 characters otherwise upto N^{th} character.

ENCRYPTION ALGORITHM (MENU DRIVEN GUI PROGRAM)

Step 1. Read (String) : Number of Characters
Step 2. Count Characters (N)
Step 3. If N<30 then Return
Step 4. Shift N1 leftmost characters to right in circular queue or vice versa
Step 5. If (N1 ≠ 1) AND (N1 ≠ 2)
Step 6. If ((N+1) / N1 = 0)
Repeat through Step 7
Else Repeat through Step 8
Step 7. For S = 1,2,3,…….N/2
S = N1, L = N- N1+1
Swap A(S) ↔ A(L)
Step 8. For S = 1,2,3,…….N
S = N1, L = N- N1+1

Swap A(S) ↔ A(L)

Step 9. Print Output

Decryption algorithm is just reverse of the encryption algorithm.

3. RESULT AND DISCUSSION :

The algorithm SKG 1.1 is successful for encrypting any text/string consisting of 30 or more characters. Minimum time required to decryt any text/string consisting of 30 or more characters is 1028 days, which is sufficiently large to decrypt any text [6].

4. IMPLEMENTATION OF ALGORITHM SKG 1.1 :

The author has implemented the said algorithm SKG 1.1 on Java platform for different values of N_1 = 1 to N-1, shifting N_1 leftmost characters to right or vice versa and N2 =3 to N/3.

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 :

Table 1 : Encrypted Output Text Using Algorithm SKG 1.1

S.No.	Comparison of Encrypted Output of Algorithm 1.1 and Algorithm 1.0
1.	Encrypted Output Text of Algorithm 1.1 for N_1= 3 & Left Shift, N_2= 3
	ctLc lb per nsidtI ,hthfoltnddiferh twrig eat Kdauarh rrdnUjav .sD yntsrt raeB eb i59t ,u1 ra nag nr dealnsag enotn naitIdn ofusta .oidsI ni wni rail oehJihufoyet1ti1sn7 ryimhrpaa ai atirreRine aetePsksru, ,htifdasgaPB so ena e t earnehakuRuKuniideoa
2.	Encrypted Output Text of Algorithm 1.1 for N_1= 3 & Right Shift, N_2= 3
	bipeo ntid I htrfostntdi,erh tlrid eft hdawarg radnKjau .hD rntUrtvrasB yb s59 ,e1 erainat nu d al sag erote nnitgdnnofnsta .Iid I ui aniorasl nehwih foietotiJsnu ryim1rp1a 7i ytihreaina aaterskRrue ,etiPdasga,B ho fnas ePt sareeh ku uKenindeaacRLcul
3.	Encrypted Output Text of Algorithm 1.1 for N_1= 5 & Left Shift, N_2= 3
	tdconciubukeRenaadnt e t no oneBisgrPdtstif ehr ,sastrP reineraRt.ri aatartaiah ys 7t91e,1f yiaueaJlnordinl iawIenits nostaonudf itI .aodn ns gain ae rnhgrh 1o tu5itbniBrermerp n sD y isjevdnU araehdkutuK ,arig aweahd ft dfalhehI ,irt hspurlK Li ae
4.	Encrypted Output Text of Algorithm 1.1 for N_1= 5 & Right Shift, N_2= 3
	pbR caicnIeehi fK tuedhserP sref aht ,d saaP aediej,R urDkanearaarnhBeybi75 1 11pyrmunrJ no iiat sow hnohs oiaadiuo s I dai.nItnifgnnnrtelnretgie fa elutdtsni aeiaer a,si9yt sr viaU trtths ur.K aatngdrwgrhBafo dnel ihtt,arteisknruo nt d tadoLnileu
	Encrypted Output Text of Algorithm 1.0 for N_1= 3
	colbtpe n idrI shttfo,tnhdilerd tfrih ewt gdaaarK rudnhjar .UD vntsrtyrasB b e59e ,i1 trauna n dgalrsae enotg nnitndnaofIst .uidaI oi sninrawl ehiihofoJetutiysn1 r1im7rpya hi atiareainr aRteeskeruP ,sti,dahgafB so Pnas eet ar ehekunuKaniRdeuaciL
5.	Encrypted Output Text of Algorithm 1.1 for N_1= 3 & Left Shift, N_2= 5
	atLdiinuKerunsietIae t eolanddofeBPagsaigieat KdrsksPerranUjiv rrita ts t rreBiyr 7n9ti,u1e rfuhiJhnr dearnsnw in tndnai Idsufo ntat.oi sIone gai lail oe gan aoy t1t 1s5i be mhapaarainy Ds.eRane det hrauau, ,ht fdrwt hr si ent fhth, rndhak Rup bl ceoc
6.	Encrypted Output Text of Algorithm 1.1 for N_1= 3 & Right Shift, N_2= 5
	lipLRcaaed i hurfk heeri, rh lrnf oh haawadg te, euauk.hDtrn aniaeasi ybis5a1pr1m erainst toteiol hag erolsaroitg nnoInsiI. atd f uidaninn et nehwis fa d uniJanu ryi1e, 9 7 ytBhrrvtrUtaa ers RrjKndariPrasgd,Btfe diastePtesadtntsou tKenInditn oecub
	Encrypted Output Text of Algorithm 1.0 for N_1= 5
	LolauedRin KdrIkshe ra nheilend os Bfaewa gdtaa Pureknhear UDiaeraity asBa br7mi1r,in trtuneJofohdghlrsle rnins nn tndiao tsIf.undaIioi gtoneawa eaii n atuaiys11 e95e py hiratrstnv nr.aRtjesdur Kr,sai,dthg hirft Pras dett,oftthe unuian eptbcic
	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

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 1.1 is entirely different.

5. CONCLUSION :

The proposed scheme named as algorithm SKG 1.1 was tested in Java platform for different values of N1 (= 1 to N-1) and N2(= 3 to N/3). In all cases the result came as per the literature and work seems to be satisfactory based on security metrics. It has been estimated that to crack the code we will require 1028 days which is much more time than the time for which 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.

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.