IJITKM Volume 6 • Number 2 • July-December 2013 pp. 129-131

INFORMATION SECURITY BY INTERCHANGING CHARACTERS: ALGORITHM SKG 1.0

Satish Kumar Garg

ABSTRACT: In the present work the author has introduced a new symmetric key cryptographic method, called algorithm SKG 1.0, for data encryption and decryption of any file by interchanging the characters in the string of text. The present method is a block cipher method and it can be applied to encrypt any data consisting of 30 or more characters. There is a scope to further enhance the present method of encryption.

Keywords: Encryption, Decryption, Interchange of Characters.

1. INTRODUCTION

Due to massive development in internet technology [1,2] in the last few years, now it is a real challenge for the sender to send confidential data from one computer to another computer. There is no guarantee that between sender and receiver there is no one who is intercepting those confidential data. The security and originality of data [1] has now become a very important issue in data communication network. One cannot send any confidential or important message in raw form from one computer to another computer as any hacker can intercept that confidential message or important message. For example, the teachers send question papers over the mail, Bank transaction, Bank statement or any other confidential matter. 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 and availability, and secondary attributes such as authenticity, non-repudiation and accountability etc. To get rid of this problem one has to send the encrypted text or cipher text from client to server/to another client. 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. The merits of symmetric key cryptography is that the key management is very simple as one key is used for both encryption as well as for decryption purpose. In case of symmetric key cryptography the key must be secret. In public key cryptography the encryption key remains as public but the decryption key should be kept as secret key. The public key methods have got both merits as well as demerits. The problem of public key cryptosystem is that one has to do massive computation for encrypting any plain text. Moreover in some public key cryptography the size of encrypted message may increase. Due to massive computation the public key, crypto system may not be suitable in security of data in sensor networks [5,6]. In the present work, the author has developed an algorithm named as algorithm SKG 1.0. The algorithm SKG 1.0 is successful for encrypting any text/string consisting of 30 or more characters. Various existing schemes have been highlighted in [7-10].

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 by interchanging $N1^{\text{th}}$ character from Left with $N1^{\text{th}}$ character from right in integer multiples of $N1$, such that $N1$ is not equal to 1, 2 and if $(N + 1)$ is divisible by $N1$, interchange/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: If $(N1 \neq 1)$ AND $(N1 \neq 2)$
```

Govt. P G College JIND - 125102 (Haryana) India
E-mail : sat.phy@gmail.com

```
Step 5: If ((N+1) / N1 = 0 )
        Repeat through Step 6
        Else Repeat through Step 7
Step 6: For $S$ = 1,2,3,.........$N$/2
        $S = N1, L = N - N1 + 1$
        Swap $A(S) \leftrightarrow A(L)$
Step 7: For $S$ = 1,2,3,.........$N$
        $S = N1, L = N - N1 + 1$
        Swap $A(S) \leftrightarrow A(L)$
Step 8: Print Output
```

Decryption Algorithm is just reverse of the Encryption Algorithm.

3. RESULT AND DISCUSSION

The algorithm SKG 1.0 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 $30!/(5!)^6 = 8.88 \times 1019$. The available Super Computer is teraflop computer which is capable of performing 1012 floating point calculations per sec, so to perform all 8.88×1019 calculations, time required is 1028 days, which is sufficiently large to decrypt any text.

4. IMPLEMENTATION OF ALGORITHM SKG 1.0

The author has implemented the said algorithm SKG 1.0 on Java platform for different values of N = 30, 40, 50, 60, 70, 80, 90, 100 and so on each for different values of N1 = 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. It is spread over 400 acres of land on the south bank of the holy Brahmsarovar, 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 below:

S.No.	*N1*	*Encrypted Output Text*
1.	3	otcibueRrnasdnte,t ho lnedisfrPhtswifgeha ,KasurPhrerneUaRv.rs aytastaahe ye 7i91t,1u y au aJgnordiel nawgenntsnnoatatnusf ptia,rovoras0haaB elooelt do nnahhsuotebtkofnahfhsyrcr 0m4 reva d erssoidI.iid I oinisraal eh ihnforet1ti sn5 rbimBrprarintiDreinjadteskarud, ttidarga B eodnateftharIehikuuKpnilde.acL
2.	4	oc .edlbneRruaiheIa,thetandiofrPhasrad eta ,KusaksrtrneUn RerDt ytasa rprBie 7in1 it1 e au hJ he dlelniw iotInnoa.ad iofsptiadravera40haac ys h lt d k tbsuothehannoofnahefoolerBr 0ms rovo, erssuntItiid s nneg nas raai rongianforytu1, ts95 rbymehaatrinaisr.viajadeehPrurad, thigfiwgt B esdenlofthertndsknuKpuiicta L
3.	5	L ca.eiiueurnkiheIre, ho lnndoePhaswidgett, dusukPhrtrnjni ersiay tista rprBmyer7i9st,t1terou hJgnerdlaarsiwgnnt Innii.Id us ptea, aver s00a aB rel hf ha d nnthtoushebakoofntleoosycr hm4arovord irssfointataod s oie nan lei oh ianfa y u1i 1n5 bi eha a rantDr.vRaUeadeesraraK, ahifar gtB rfsideateftthatndsauRKpnbldcto
4.	6	ocatci in eRruksdntra,thelnedofrPhagwifgita, KururPhetrneUniv.rsitytas a ahemie 7inst,1ute au hignor lelningenn Innoa. Itnussptiadovor 40haa cr eloof lt d onnahesuothbt k ofnahe h sy Br 0msarevar, ersfoida tiidsto iwa sraaid eh Janfory 1ti 195 rbyBrpratrinaDre Raj aderskasad ,the darst B esidnatoftheIehianuKpublde. L
5.	7	ocateilin Ku nkshet e, the tandoerBhagwifgita,,duruksrtraUaRversian is araremie 7insti11te ofnaigherdiearniw in I nia.Itnusspri d overa400 aBesofehandoknthesuothba n of tlholyrcrahm srovar,aetsfoidatiodnsto ne gnaslal on Jhuaryut, 195 rbyBhpatratyt Dr. injendeehPrasaK the darst P fsidenl of tharIndiaurRepubdc.L
6.	8	ocatedlbnKuruaihetra,thelandiofBhasradgita ,KuruksrtraUnRersitytas a prBier in1 itute au highedlearniw in Innoa.Itiofspreadraver 40haacres h land k the suothbannoofthefooly Br 0msarovo , its sundatiidstonegna slaironJanfory 11,ts957 bymeharatrinaDr.viajendeehPrasad ,the fiwgt Pres dent oft heIndsknRepuiic. L
7.	9	Loc ted bnKRruksdetre, tholaedofrBhaswadgeta,,KurursheeraUaivers itytis a pre ier7inst,tuty of aighorlelrni wgintIndoa. Itnisprea, ovor 40h ac es o la d onnthehsoutba k ofnthefholyrBra0msarevard itssfoudatiin s one nasaaid en Jhnuare 11i 195 bymBharatrana Dr. RnjendtrPkasadthifirgt P esidnntefthaInhianuepuilic.a
8.	10	LocateiiuKurukiheIra, tholnnd of Phaswadgitt, durukshrtrnUniversiay is arprBmier i9st, tuteouh Jgherlaar singint Innia. It us pread aver 400 aBrel of la d n the toushbankoofnthehosycrahmsarovor, itssfoindatiods one wan leid on ianfary 11i 1n57 by ehaatratnt Dr. RajeadeePrasaK, ahefirgt Bresideatef the tndsan Repnbldc.
9.	15	Locatei in Kurnkshetre, the lnnd of Phagwadgeta, Kusukshetrn University istapremyerinst,tuteouhigherdlearniwg in Innia.It us sprea, over s00 acrel of la d on thsouthebankofnthehosy Brahm4arovard its foindatiod stone naslai on Janfary 11i 1957 biBhararatna Dr. Rajead erPrarad, thi first Bresideat of thaIndiauRepubldc.
11.	20	Located in KurukiheIra, the land of Phaswadgita, Kurukshrtrn University is arprBmier institute ouhJgher learning intInnia.It is spread aver 400 acres of la d n the south bankoofnthe holy Brahmsarovor, its foundatiod s one was laid on ianfary 11, 1957 by ehaatratna Dr. Rajea dee Prasad, the firgtBresident of the tndsan Republic.
12.	25	Located in eurukshetra, he land of Phagwadgita, durukshetrajniversity ista premier i9stitute of hJgherlearniwg in India.Id is spread aver 400 acrel of land onnthe south ba k of the hosyBrahmsarovor, its fountation stone nas laid on ianuary 11, 1n57 by Bhararatna Dr. RaUenderPrasaK, the first Bresidentoftthe Indian RKpublic.

From the example cited above, we find that for small values of N1 the output text contains large number of jumbled characters and output text is more unreadable.

5. CONCLUSION

The proposed scheme named as algorithm SKG1.0 was tested in Java platform for different values of N (= 30, 50, 70, 90, 100, 125, 150 and so on) each for 10 different values of $N1$(= 3 to $N/3$). In all experimental 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 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.

Acknowledgements

The author is thankful to Dr. Ashwani Kush, Associate Professor and Head of Computer Science and Application, University College Kurukshetra (Haryana) India, for helping him during present work.

REFERENCES

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

[2] Satish Kumar Garg, "Wireless Network Security Threats", *International Journal of Information Dissemination and Technology*, **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, **16**(10) pp. 11 (Oct. 1970).

[6] G. Dantzig, "Linear Programming and Extensions", Princeton Univ. Press, N.J. Princeton, (1963).

[7] L. Lamport, "Password Authentication with Insecure Communication", *Comm. of ACM*, **24** (11), pp. 770-772, 1981.

[8] A. Kush, S. Taneja, Divya, "Encryption Scheme for Secure Routing in Ad Hoc Networks", *International Journal of Advancements in Technology*, **2,** No 1 pp. 22-29. Jan 2011.

[9] Arash Partow, "General Purpose Hash Function Algorithms", www.partow.net.

[10] L.L. Beck, "A Security Mechanism for Statistical Databases", *ACM Trans. on Database Syst.* **5**(3) pp. 316-338 (Sept. 1980).