IJITKM Volume 7 • Number 2 • Jan – June 2014 pp. 14-16 (ISSN 0973-4414)

Cryptography by Swapping Bits: Algorithm SKG 2.0

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 cryptographic method, called algorithm SKG 2.0, for data encryption and decryption of any text file consisting of N=10 or more characters at three stages (1) First, converting each character into corresponding binary code using 8-bit ASCII Code (2) Secondly, by swapping the leftmost N_1^{st} bit with N_1^{st} rightmost bit till $4N^{th}$ bit if remainder of (8N+1/N1) is zero otherwise upto $8N^{th}$ bit and (3) Finally, converting binary string obtained at stage two into corresponding characters using 8-bit ASCII Code. This algorithm can be applied to any text consisting of 10 or more characters. The results obtained after application of this algorithm are excellent and difficult to decryt.

Keywords: Encryption, Decryption, swapping of bits

1. INTRODUCTION :

The internet technology is being used almost in every field. The security and originality of data [1,2] has now become very challenging. So 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* [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 author has developed an algorithm named as algorithm SKG 2.0 which is more effective as compared to algorithm SKG 1.0 for encrypting any text/string consisting of 10 or more characters.

2. THEORY :

The algorithm SKG 2.0 is based on the concept that each character is represented by a unique 8-bit code in ASCII Code system and if one or more bits are changed in a 8-bit code corresponding to any character, then corresponding character is entirely changed. When any text of 10 characters is converted into binary form we get 80 bits which contains about 50% of 0's and 1's each. Therefore, total number of possible combinations is about $80!/(40!)^2=$ 1075×10^{20}. The Super Computer available is Teraflop which is capable of doing 10^{12} floating point calculations per second, so a teraflop super computer shall take about 3409 Years to find all possible combinations.

In the present algorithm we use following steps to encrypt any text :

(1) First, convert each character into corresponding binary code using 8-bit ASCII Code thus we get 8N bits for a text of N characters

(2) Secondly, swap the leftmost N_1^{st} bit with N_1^{st} rightmost bit till $4N^{th}$ bit if remainder of (8N+1/N1) is zero otherwise upto $8N^{th}$ bit and

(3) Finally, convert binary string obtained at stage two into corresponding characters using 8-bit ASCII Code.

ENCRYPTION ALGORITHM (MENU DRIVEN GUI PROGRAM)

```
Step 1.  Read (String) : Number of Characters
Step 2.  Count Characters (N)
Step 3.  If N<10 then Return
Step 4.  Convert each character into corresponding binary code using 8-bit ASCII Code thus we get 8N
         bits for a text of N characters
Step 5. If  ((8N+1) / N1 = 0 )
                Repeat through Step 6
         Else Repeat through Step 7
Step 6.  For S = 1,2,3,……….4N
             S = N1, L = N- 8N1+1
             Swap A(S) ↔ A(L)
Step 7.  For S = 1,2,3,……….N
             S = N1, L = N- 8N1+1
             Swap A(S) ↔ A(L)
```

Step 8. Convert binary string obtained at step 6 or 7 into corresponding characters using 8-bit ASCII Code.

Step 9. Print Output

Decryption algorithm is just reverse of the encryption algorithm.

3. RESULT AND DISCUSSION :

The algorithm SKG 2.0 is successful for encrypting any text/string consisting of 10 or more characters. Minimum time required to decryt any text/string consisting of 10 or more characters is about 3409 Years to find all possible combinations, which is sufficiently large to decrypt any text.

4. IMPLEMENTATION OF ALGORITHM SKG 2.0 :

The author has implemented the said algorithm SKG 2.0 on Java platform for different values of N_1 = 1 to 8N.

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 : Comparison of Encrypted Output Text Using Algorithm SKG 2.0 and SKG 1.0

S. No.	N1	Encrypted Output	
		Using Algorithm SKG 2.0	Using Algorithm SKG 1.0
1.	3	Î¶[&G®æj~¢grM¢g$v÷$,v¢$?î$N. oîLÖbç6,D4$ÆêF¦&w¢D Æj4N"M¦df¢Lf¢LÏ2@EºTDì,Ý¬4¨E¾LÆ®t Çrvòo¶w LÎîævdnî□ öo¦$□ªf&15\g²}¦frMvâtßvL?¦$Ej$Wâ$f¶15$n ®,Ö*L7²¢·¦LF DêDº<Öê\îjvª? J,î6NÖ®^¦Òu¢,Öæ$Æêd?6@DbtvÇ2æ6.D0F *4^îDïn,Û f?15$æ.Îò"	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
2.	4	Äör`ìlä(`v Òdrôbâpldbð$(tàd°ìànl nî(Ò``ævhdv`äè¤(Jdjäbràtäj`0Lf`ætjâhlà(àr `¸`bììøìb0èî bühäìtä0fv°` `öàtb¨äì` âvðnî pö°Hædpè¶ @ìj°fväödpô`vö âtövl æpb(äpàô0ff°B ànìhòh¨0°$( °´¦(j` Bèðbølòèlæh°Tê& Jhâtîôìj¨ Ðbpâhô¤äèä v`bbô @rär`ätnd0æn(äpì° Ènìð`v° Bdàlâäðr	cocbuedR n idru ehe fa,tnheisanP ofrihaehad,dtaarKureksejtr .Un aerartyras ypr75ie ,in yitune n hdihe sle enits ioiIndna.f tsI ouidat nn gnonrawa rlagi ofoJatuarts11 r19me b aBhi atistnviDr aRaehndur P ,saig twg fB st drel det ortthskInuKani eptaliL
3.	5	F?wD|/& f"evT!#|dTrs,$t"'´ Ì`n&$n NjlDf7#df`6c¬J5bånr"wäR@`GjLV g"çL|3bíV 15!2dVl-9Åv ,gÔH6 'tÄ 15%v´L`'*uV&geöfc.ç`f2MÎdc#¾$@~#°Ff7 >ddT!□þ rv?~D1573gd# kôFfr Nän ?#ö\|s3,037§J1"FÌ@03dÖH~.e? d:,¤Vh "7îÄlz"ÐV`3#ô ¬ 6jå?Fc gô15råv @& 7nT'f$ô@orÍNlc!~?Rb'"n eÆDc3	LolauedRin KdrIkshe ra nheilend os Bfaewa gdtaa PureknhearUDiaeraity asBa br7mi1r,in trtuneJofohdghlrsle rnins nn tndiao tsIf.undaIioi gtoneawa eaii n atuaiys11 e95e py hiratrstnv nr.aRtj esdur Kr,sai,dthg hirft Pras dett,oftthe unuian eptbcic
4.	6	Îw"glæ(n wrmcgdrç$ v`$¦l nl15on@Æ `15çw dw(öi&Kve*w`Döj $M.mf dvcHva @ïs@e8Ptm,ím$iu|Hömt ç0f0owgb@îm15övhno15ov15Of$oin& ATw0mefqmw$ctïvD¦g u(,ga&gn¦B nm öi@71&!·'@fa15Dh15ty4öiTîi15Fj¦ J îuNæmR¦Pec æ$ öhd¦vHtct$@ rçsæu. t0f(4nm@Ïn$ëan¦B$ömîq"	cocatpe in idrukshttra,tnhe lerd ofrihagwt gitaarKurudnhetr .Univntsityras a b emie ,instraute n higalr le ening nn Indna. Ist fouidatioi stonrawas ehid ofoJanutiy 11 r1957rpy Bhi atrarea Dr aRajesker P ,sad,dahe fB st Pnasidet of ehe InuKan RdeubliL
5.	10	N/sE|g$ Mf" evti3xetra,$tj%°L`n$ on"hEfw!dg`va¬JuråorjeäR` UnMv	Lolated in Kdrukshe ra the lend of Bhaewa gita, Purekshetr UDiversity as a pr7mi1r instrtune of

		g2ãMl{`éW a `Vlm)åV i.cThv5tE mf°L`g(uV(neavfk.ç`n INdk!¾ $@v3 °Ffw.detioþrv/~E w!cdciôfn` Jenw !ò}(31, 0;5§jy BL`p!dVhv.aDr . Vhj %îDlr ÐV`s!ô, vhåfk2ct Rråw` f%nT of t`g`ÉNlk!~ Rg0eFdk#	hdghlr learnins in Indiao Its f.undation gtone was eaii on Jatuaiy 11, e95e by Bhiratratn a nr.aRajendur Krasad ,dthg first Prasident,oftthe Inuian Repubcic

From Table 1, it is clear that if we change N1then output of the Algorithm SKG 2.0 is entirely different.

5. Conclusion :

The proposed scheme named as algorithm SKG 2.0 was tested in Java platform for different values of N1 (= 1 to 8N). 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. Further, we conclude (1) algorithm SKG 2.0 is applicable for text containing 10 of more characters while algorithm SKG 1.0 [5] is applicable for text containing 30 of more characters (2) results are different using algorithm SKG 2.0 and algorithm SKG 1.0 and (3) time required to decryt the text may be 3409 years by using algorithm SKG 2.0 while it may be just 1028 days by using algorithm SKG 1.0.

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] 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.