IJEE Volume-6 • Number-1 Jan -June 2014 pp. 20-24 (ISSN: 0973-7383)

Information Security Using Controlled NOT Gate : Algorithm SKG 3.00

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 unique cryptographic method, called algorithm SKG 3.00, for data encryption and decryption of any text file at four stages (1) First, by converting each character into corresponding binary code using 8-bit ASCII Code thus we get 8N bits for a text of N characters (2) Secondly, creating a string of 0's and 1's such that total number of 0's and 1's is 8N, the consecutive numbers of 0's and 1's in this string may be from 1 to 7 (3) Thirdly, using Control NOT Gate on binary strings obtained at stages one and two and (4) Finally, converting binary string obtained at stage three into corresponding characters using 8-bit ASCII Code. The results obtained after application of this algorithm are excellent.
Keywords: Encryption, Decryption, Control NOT Gate.

1. INTRODUCTION:

The security and originality of data which is transmitted through internet [1,2] has now become very challenging because there is always a possibility that anyone may intercept our data. 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. 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. 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].

2. THEORY :

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 $80!/(40!)^2 = 1075\times10^{20}$. 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 study, the author has used Controlled NOT Gate which is basically a XOR Gate.
The truth table of a XOR Gate is as under :

Input		Output
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table 1.

From the above Truth Table 1, it is clear that if the value of X = 0, then the value of output Z is equal to the value of Y and if the value of X = 1, then the value of output Z is inverted to the value of Y.

Input		Output
X	Z	Y´=Y
0	0	0
0	1	1
1	1	0
1	0	1

Now if X is used as control signal (0, 1) and another input is Z, then output of the XOR Gate is Y´ which is equal to Y. Thus C NOT Gate is reversible Gate. This fact is used to superimpose input digital signal (corresponding to text) on carrier digital signals of varying widths. Then the digitally modulated signal is transmitted from source node A to destination node B. At destination node B, the digitally modulated signal is demodulated again using Controlled NOT Gate, e.g., alphabet **a** is represented in binary form as 0110 0001, if we use this as input and a clock pulse of width of single unit Ck = 01010101 as control signal, which is used as digital carrier pulse, then output of C NOT Gate is Y = 0011 0100 as in Table 1. Y = 0001 0100 represents 4, hence we see that **a** is encrypted into **4**.

Ck	a	Y
0	0	0
1	1	0
0	1	1
1	0	1
0	0	0
1	0	1
0	0	0
1	1	0

Table 1.

Now if we use Y = 0011 0100 as input and Ck = 01010101 as control signal, output of C NOT Gate is Y´ = 0011 0100 as in Table 2. Y´ = 0011 0100 is used to represent **a**, hence we see that **4** is decrypted into **a.**

Ck	Y	Y´
0	0	0
1	0	1
0	1	0
1	1	0
0	0	0
1	1	0
0	0	0
1	0	1

Table 2.

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, creat a string of 0's and 1's such that total number of 0's and 1's is 8N, the consecutive numbers of 0's and 1's in this string may be from 1 to 7

(3) Thirdly, use C NOT Gate on binary strings obtained at stages one and two and

(4) Finally, convert binary string obtained at stage three 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. Creat a string of 0's and 1's such that total number of 0's and 1's is 8N, the consecutive numbers of 0's and 1's in this string may be from 1 to 7

Step 6. Use C NOT Gate on binary strings obtained at steps 4 and 5

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

Step 8. Print Output

Decryption algorithm is just reverse of the encryption algorithm.

3. RESULT AND DISCUSSION :

The algorithm SKG 3.00 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, which is sufficiently large to decrypt any text.

4. IMPLEMENTATION OF ALGORITHM SKG 3.00

The author has implemented the said algorithm SKG 3.00 on Java platform for different values of Ck = 1 to 7 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 3 :

S.No	Ck	Output of Algorithm 3.00
1.	1	:64!01u<;u- ' >&=0!'4yu!=0u94;1u:3u=42"412<!4yu- ' >&=0!'4u4;<#0'&<!,u <&u4u%'08<0'u<;&!<! !0u:3u=<2=0'u904';<;2u<;u;1<4{u!&u3: ;14!<:;u&!:;0u"4&u94<1u:;u4; 4',uddyudl`bu7,u=4'4!'4!;4u'{u4?0; 10'u'4&41yu!=0u3<'&!u'0&<10;!u:3u!=0u;1<4;u0% 79<6
2.	2	□\PRGVWZ]xFAFX@[VGARG[V_R]W\Uq[RTDRWTZGR-xFAFX@[VGARf]ZEVA@ZGJZ@RCAV^ZVAZ]@GZGFGV\U[ZT[VA_VRA]Z]TZ]z]WZRzG@U\F]WRGZ\]@G\]VDR@_RZW\]yR]FRAJ QJq[RARGARG]RwAaRYV]WVAcAR@RW-G[VUZA@GcAV@ZWV]G\UG[Vz]WZR]aVCFQ_ZP
3.	3	P-¤}¢xQ®rQ?i²w¯ yµ}]çh¢<¦rçsç^¦{¦x®hë<:²n¬o¢h¦<$©u¢n®hçuç}Q·nªuµ<©o®h³ yQ¨zQ¯u¯ yçp¦n®rçuçU£ué<8³oQ¡s©x³u-©<³s¢<¦oQ«}£<-©<;¦r¦nç-@ë<@þ)Fç~ç^¦n³n³rçXé<#¦v©xµ<!µ}¦x]çh¢<®n³<!µy®x©hQ¨zQ³tçU£u©<#¢ ¥p¤
4.	4	C`ln{jk/fa/Dz}zd|gj{}n#/{gj/cnak/^i/Mgnhxnkhf{n#/Dz}zd|gj{}n/Zafyj}|f{v/f|/n/□ }jbfj}/fa|{f{z{j/^i/gfhgj}/cjn}afah/fa/Fakfn!/F{|/i`zakn{f`a/|{`aj/xn|/cnfk/`a/Enazn} v/>>#/>6:8/mv/Mgn}n{}n{an/K}!/]nejakj}/_}n|nk#/{gj/if}|{/_}j|fkja{/^i/{gj/Fakfn a/]j□zmcfl
5.	5	K®?kb¥Ðq'??jl²?ku Ü\ko¤Ð~i¥Ðy'??xp ?vs Ü\Tr³?lo¤?~'??ib³?k~á??fá? zj¨? ?n¯?vs´??h§Ðv`©? ?k¤? qn¯?\viá¹{n Þ\Vs²Ðpr¯?kn®?\l s®??p ?\sf¨?\p iáº qr ??6ðÜ\.>ôÇ\}~á²~u ? ~s¯?\[uïÐ.~m¤?zuá ~t ?P?s©?\yn³??W³?vc¤? ?h§Ðwbá¹{n ?\Mb±?-sn¢
6.	6	O?\b?ZgÐVmÐtv?Jh?Wf?MbÜw?Z#?^m?l?A?^d?^g?Vw?#»Jq? Tp?Z w?^#¥Qj?Zq?Vw?j?bÐOq?Rj?M#?Qp?Vw?KfÐPeÐWj?Wf?o?^q?Vm?j?J?[j? #¹KpÐYl?Qg?Kj?Q#?Kl?Z#?^pÐSb?[#?Q#º^m?^q?2Á#Á6Ça?A?^q?Kq?Km?-G?#¢^i?Qg?M# Mb?^gÜw?Z#?Vq?K# Mf?Vg?QwÐPeÐKk?J?[j?Q#¢Zs?]o?\
7.	7	M?d?k¥!?iÐTµt?t?z^Ð'?w¥_m?i??¯ !¾o?x·-e?n?~ì_J?u?t³d?u???h?b?l© xÜn??¡_q?b?v¥!?i?k©t?bÐp¦_i?`?z²_m?f?q©fÜn???e?fÞ??rÜa?j®`?n?qà u?i??·-rÜk?v¤_n?'º~®`?~Ð.ñS!Í>Å(àxÜE?~²-u?f?q¡_E?)ÐM¡d?c?mà/s?t?{ì_u?bÐy ©r?' m¥ h?b?kàgÜs?zà6o?n?qà-d?r?s©

Table 3 : Encrypted Output Text Using Algorithm SKG 3.00

From Table 3, it is clear that if we change Ck from 1 to 7 then output of the Algorithm SKG 3.00 is entirely different.

5. Conclusion :

The proposed scheme named as algorithm SKG 3.00 was tested in Java platform for different values of Ck = 1 to 7. 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 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.

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)