SECURED BUSINESS TRANSACTION USING INFORMATION TECHNOLOGY

Satish Kumar Garg
Govt. P G College Ambala Cantt. - 133001
sat.phy@gmail.com

***Abstract*: In the present era of information technology, Business is enormously influenced by Information Technology. Data storage, retrieval and processing can be efficiently and accurately done by using computers. Business details and transactions are highly confidential.**

When someone feels facilitated by the digital innovations, the threats have also increased manifolds. There are a large number of techniques which can be applied for secured business transactions, one of these is Cryptography.

I. INTRODUCTION

Cryptography is a science based on abstract algebra. Cryptography makes message illegible to a hacker and it ensures safe and trustful communication among parties to avoid any threat. Cryptography techniques are broadly classified into three types :

A) Secret/Symmetric Key Cryptography (SKC)

Uses a single key for both encryption and decryption

B) Public Key Cryptography (PKC)

Uses one key for encryption and another for decryption.

C) Hash Functions

Uses a mathematical transformation to irreversibly "encrypt" information. A *hash function* is a one-way encryption algorithm that does not use any key to encrypt or decrypt the data.

In the present work the author has suggested a unique cryptographic method where bit level manipulation is done using transposition cipher. In this method, first by using Extended ASCII Code, input string of characters is converted into digital form then transposition cipher is applied on this string.

Finally by applying reverse of the Extended ASCII Code on this transposed string, bits are converted into characters. The proposed method can be applied to encrypt any data consisting of 10 or more characters. The results obtained after application of proposed algorithm are excellent and difficult to decrypt.

II. THEORY

This algorithm is based on the concept that each character is represented by a unique 8-bit code in Extended ASCII Code system and if one or more bits are changed in a 8-bit code[6], 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 $80!/(40!)^2 = 1075\times10^{20}$. 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. This time is sufficiently large for any message to reside on any network [5].

III. PROPOSED ENCRYPTION ALGORITHM

1. Read the input string of characters and Check the number of characters, N

2. If N<10, then write Program is Not Applicable

3. By using Extended ASCII Code, input string of characters is converted into digital form

4. If (8N+1)/N1 = 0, Transpose Integral Multiples of LMB with corresponding RMB upto middle of the string otherwise proceed upto 8N bits

5. By using reverse of the Extended ASCII Code, the string of bits is converted into character form

6. Output is Encrypted String i.e., Cipher Text

IV. IMPLEMENTATION OF PROPOSED ALGORITHM :

We have implemented the proposed algorithm on Java platform for different values of N1 = 1 to 8N/6. For example for the plain text given below, cipher text is shown in Table 1 for different values of the key, N1.

"Ambala Cantt is situated on the North-Eastern edge of Haryana. It is known as City of Scientific Instruments on International level. It is gate way to

S. No.	Keys N1	Cipher Text
1.	1	N?╢╬?╥ d«╢╢?R&v? ╬ª&?N6? ╞?╢? 4F?Vv? 4N?µ?&v?┬ ÷.??εª.?µ╬?.?t6ªnª66?v÷?.?vNª.v? v÷╬.vª╢ «N.╬v? ╞?f?.vª? ╞╧ f÷?.?┬╬?vε÷v╓╬?.?t?v??N? f÷ª µ&ªvNª.╬?ó┤.N÷rª. v÷&ª.?«.?╬ ╬?..v?┬?6?F╢?
2.	3	G╢ &Wε?227dL«4╢óR"d ╞$ ╞ª$?n 6WΓ ▒L4D╟rt╟*46L ╟µov^Γ *╬ªlMª,╧Γ╧╢ g╢ u2$gó4M2v≥gódNª,v▒6╥ ╟.vτ╢ ,N.^6╢ ??f╓.vε▒T╤$f≈$ n╢ REεR╢╢ rVεD.227Ep6ª ?227EfdMªdfó6J$nΩΓ┤ njds $W. v≥fª>╬¬, ▌ε╬▒o.d?Γ╟2O▒
3.	4.	H⌠≥p∞α▒B`f∞⌠▒αr bpΣdp∞Σdánn τατά╞÷≥t`4DαrtΣjf0tlμΣ▒fváPαb≡hfºª¿@Σ(αΓ Ω÷fn÷ práJατ`0μv▒╥jατnΣhv≡b0╨fΩlrΣ⌠∞nlΩ0÷fá╨f⌠lrμ≡ΣΦff≡d╕ l⌠μd∞ª P∞▒p≥ ε≡dl▒fpα0Σ■(┬p`f⌠`μαbα$0HαnΩαΓ┤ 0Hh⌠pbαpl P≥`dΣjα¿h÷∞ ╨≡dll0ªáBαrαd≡
4.	5	K?÷DL#rGdF>6┤ ╟R #} ╘T#fσd227o.$t@'b╬εR6(=D@svσRF 7d ╞d"/v?@c ²dF+.ñLt*+τJ&-g╨227a3ñf`6)4╬fbg╟dn&mf@! r▌ NZ>rσ∞ln&τ$F$ b▌ nT/rε─Tk-nΣD*.⌡╥Dn.$l\|b{≈N#$e?Va+4 ╘NjxDff)τΣr",4T`.jσΓ$" m∞`!*ul227Rredd;*ñdFn ╬─D/'4?227#w╟D#"
5.	10	C-≥Elc`Cefv4▒Mr 3yTtctσd o. t`g`╬orv(=E`stσRf %dGd"/v@c2·e fc.áMt")πjn/gJ a3ág`v90Of"cMdn4if`a`┘ Nzvrσmln4π$fl`┘ nt grεEtk/ned",⌡Rdn. m\|"i≤nc4e227va90Tn"xEff)τerj,0T`njßb$"im`a(ql Rradds(áeff ╨Edo50I!sLdk2
6.	15	Cofela0CaN44áΦr smtuaded227o. thg"North=EAstσrn gdge ov227Ha2·`nc.$Mt(ic227K./wε as$Gati0Of`cΦdnvmfac0YNS4r⌡∞dnvw$gf YnT%rεαtkmned(luVEl. Ht"kw$oade227Wa9 ⌠n"Chefdigar(, P`njeb$ Hima#(al Rrede{h aNd ╨αlow$& CasHM)2

Table 1 : Cipher Text for different values of keys for the same Plin Text

V. RESULTS AND DISCUSSION :

We have implemented the proposed algorithm on Java platform for different values of N1(= 1 to 8N/6). From Table 1, it is clear that if we change value of the key N1 then output of the proposed algorithm i.e., Cipher Text is entirely different.

VI. CONCLUSION

The proposed algorithm was tested on Java platform for different values of N (=30 to 1000) each for different values of N1= 1 to 8N/6. In all cases the result came as per our expectations. 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] S. K. Garg, Review of Secured Routing for Wireless Ad hoc Network, International Journal of Computing and Business Research, 2 (1), 2011.

[2] S. K. Garg, Wireless Network Security Threats, International Journal of Information Dissemination and Technology, 1 (1), 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) p. 11 (Oct. 1970).

[6] S. K. Garg, Information Security By Interchanging Characters: Algorithm SKG 1.0, International Journal of Information Technology and Knowledge Management, 6 (2), 2013.