Secure Data MessageCrypt with SSL and SRSA

S. R. M. Krishna, N.Seeta Ramanath, K. V. Ramana Reddy and S. C. K. MahaLakshmi

Abstract: --As the internet grows in popularity and therefore also in size more and more transmission takes place mainly because the technology is more readily available and applications have become more user friendly allowing entry to less sophisticated user over a broad spectrum. Most data transfer is mainly text based not secure and vulnerable to various forms of security risks. So this encryption algorithm is mainly designed for having a secure file transfer in the low privilege servers and as well as in a secured environment too. This methodology will be implemented in the data centre and other import and a tatransaction sectors of the organization where the encoding process of the software will be done by the data base administrator or system administrators and his trusted clients will have decoding process of the software. Data is protected as the content of file undergoes data encryption & the same is decrypted using the application at the receiver's end. For enhancing the security we introducing SSL protocol through which file will be transmitted with double encryption mode.

Index Terms – RSA,NumberConversion, DigitalEncoding(Block Coding), SSL protocol.

I.INTRODUCTION

This model that uses SSH with SSL for securing channel like intranet/internet which provides client authentication encryption and decryption with high degree of security by transferring the data in an encrypted format, up on this model enhances the efficiency of data transmission by encrypting or decrypting the data with AES in Counter Mode. And This algorithm comprises of RSA , Number conversions (Binary, Octaletc...), digitalencoding (4B/5B,blockencoding), Allthese process will provide a secured encrypte dout put of the data which will prevent the hacker from viewing the data when they are transmitted over the network kat the same even if the hacker gets the encrypted data it will be many thousands of years to get a clueu ponit. This algorithm aims at providing security within a network of its operation.

S. R. M. Krishna, Dept of C.S.E, G.V.P.College of Engg,Madhurawada, India , N.Seeta Ramanath, Dept of I.T,JNTUK University, India., K.V.Ramana Reddy, Dept of C.S.E, JNTUK University, India, S.C.K.Maha Lakshmi, Dept of C.S.E,JNTUK University, India. Email:krishna.murali564@gmail.com

II. SRSAALGORITHM

Thesteps ofusingthis encryptionmethodologyareasfollows:

STEP1:-

InthefirststeptheRSAalgorithmwillbecarriedwiththefollowingmodifications.

i. Considertwoprimenumbers as 11and13–(1)
ii. N=P*Qi.e. 143
iii. M=(P-1)(Q-1)i.e.120
iv. DisthedecryptionkeyExample3 whichisaprimenumber
v. E=Dinverse(modn) i.e.47
vi. Letthepasswordbe"Hello"takethe ASCIIvalueofthepasswordcovertitas7269767679 .
vii. ConcatenatethisASCIIvaluewitha SALT value (Randomlygenerated number)say 34i.e.247172101086
viii. Finally multiplythis withthe Encryptionvalue toget finalencryptedword9886884043440

ModificationandRequirementinRSAAlgorithm:

I(i) Original message transmitted through SSL resultant gives input to the improved RSA.

i. TheminimumrequirementforP andQvaluesinRSAisbitswhichgivesthe utmostsecuritytothefile thatisbeingtransferred.
ii. Modification isinclusionof ASCIIvalue conversionandSALT value.Here SALTisbeing left**userdefined**.

The P and Q values are also**user defined**thatisalsoamodification

iii. At this you can use anyencryption algorithmswhicharebeingupdated.

STEP2:-

The abovearrived resultthroughRSA– **9886884043440**willbe convertedinto 0's and1'susing numberconversion.

Theabove**encrypted data**(9886884043440)willbe converted as into binary i.e.

100101101101110010100100101010011011000010010110111001010010010010110110111001010010010100110110000100101101101110010100100101010011011000010000.Thisisfor binary inthe samewayitcanbedoneforoctal/hexadecimal

STEP3:-

This number conversionwillbemodifiedusing DigitalEncoding(EitherLineorBlockEncoding). Advantage:- Rearrangesthebitsofdatai.e.0'sand1's.

4bit value nibble	5 bit value symbol	4bit value nibble	5 bit value symbol
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Figure 1: 4B/5BSubstitutionBlockEncoding

Letus consider4B/5BBlock Encoding

10011011101101111010101100101010110100111011111110100110111011011110101011001010100110111011101111010101100101010110100111011111110101101111010101100101010110100111011111110

STEP4:-

Inthis steptheconversionsofdatainto4B/5Bwill be converted back into numbersusingnumberconversions.ThisisreverseprocessofStep2.

STEP 5:-

Final the resultant of above steps double encrypted with SSL protocol which encrypts data with powerfull encryption algorithm AES.This enhances the greater security for plain text.

III. ADVANTAGE OF USING DIGITAL ENCODING, NUMBER CONVERSION AND MATHEMATICAL SERIES

1. ThemainadvantageofStep2,3,4isinStep 2 the encrypted data obtainedbyRSAisconvertedinto0'sand1's.Thenby usingDigital EncodingtherearrangementofBit'saredone.Finallyi n Step 4 thereverse process of number conversion.
   What it does? Thehacker willnevergetaclueofthisprocessthatis beingcarriedunlesshegetsanideaaboutthisalgorith m.
2. ThenStep5alsoavitalroleasherethenumber X i.e. the valueobtained from Step4hastobedeterminedbythehacker,forwhichhes houldwhatisused,iffound whatmathematicalseries usedwhichwill takesagestorefine.

Butfor an organization toencryptanddecryptwillbeasimpleastheprocess involvedineachdata encryptionwillbestoredintheirdatabase.Sothistwist inthealgorithm willbe playingthe most important inpreventingthehackingofdata's.

How thismethodologygivesutmostsecuritytothefileatthesametim eincreasesthe complexityin identifyingthecontentbytheintruder.Thesearebeing describedbelow.

If theIntrudergets this encryptedwordthefollowingthingsaretobedetermined.Deter mining those values is a longprocessand finding thosewill take many years in order to arrive attheconclusion.

i. ThevalueofNi.e.thelengthoftheserieshastobedeterm ined.
ii. AfterfindingNvaluesthevalueofX has to be determinedthat has beensubstitutedintheseries.
iii. In the line encoding processthe split up of the bits hasto be determinedlike4bits,8bitsandsoon.
iv. Afterdeterminingthis,thetypeof encodinghastobe determinedand the substitutionused as in theB8SZ where 8 bit value is substitutedinplaceofcontinuous8zero's.

Based upon which the entire two stagescanberevealedfromthisthefirststage

v. stagescanberevealedfromthisthefirststagecanbeproc eededthatisRSA insteadof that AES, SHA,MD5anyencryptionalgorithmcanbeused.
vi. The speciality of RSA isin determining the primenumbers P andQwhichitselfwilltakemany yearstodetermine.

Theendusercanbeadatacenter,searchengineetc whichwillgetutmostsecuritybecauseoftheusage of LineEncodingandMathematicalseries.Theline coding will convert the original encrypted word into duplicate encryptedwordby usingthe following:

i. binary/octal/hexadecimal the encryptedwordisconvertedas 0'sand1's.
ii. Then lineencodingsisused.Thiswillactasaprotection.This willbeevenmoreprotectivebyusingthemathemati cal series. Onthewholethe methodology willbeasecurepathforthetransfer of data's.

TimeforgeneratingtheEncryptedfileusingthismethod willbecomparativelylessinthehighend PC'swithdualcoreprocessorandabovewith2GBRAMwithpro cessorspeedof2.2GHz.TheRSAencryptionofaboutbitswilltak etimeother stepswilltakefractionofsecondsforgeneratingthe desiredoutput.

IV. OBSERVATION-TIME REQUIREMENT TOGENERATE ENCRYPTED DATA

1. FileSize:1KB
2. Noofwords(Includingsymbols):50
3. TotaltimetakeforRSA:
   a. 86millisec
4. Forotherprocesshardly:212millisec

V.RECOMMENDEDSERVER CONFIGURATION

HPProliantDL320G5

1. MinimumHDDCapacity72GB(2SASHDD)
2. RAID0+1(Mirroring)asaredundancy
3. 2GBRAM
4. Dual CoreXeonProcessor
5. Processor Speed1.73 GHzandabove

Why thisspecification?

Becausewhileencrypting multipledata'sat thesametimethishardwareconfiguration willprocesstheentireencryptingoperationinlessduration.

DIAGRAMMATIC REPRESENTATION OF ENTIRE DATA ENCRYPTION PROCESS:

RSA ALGORITHM

↓

NUMBER CONVERSION

↓

DIGITAL ENCODING

↓

NUMBER CONVERSION

(REVERSE PROCESS)

⇩

SECURE SOCKET LAYER(SSL)
(Decryption Reverse Process)

VI. ADVANTAGESOFTHIS ENCRYPTIONMETHODOLOGY

1. Inthefile transferpreferablyinthelowprivilege serverswhich areanendangeredplaceofhackers.
2. IntheWANwherethedatatransferisnotthatsecured,in ordertogiveafirm security thismethodology can beadopted.
3. Thismethodologywillbe ofhighvalue inthedefencesectorwheresecurityis given high preference.Using thismethodologythehackerwillnotbeable to trace theideasunlessoruntilheiswell versed in themathematicaland electrical technique of disclosingthedata.
4. Thiswillalsoplayavitalroleinother sectorslikeBank,IT,AeroSpaceandmanymore where thedata transferisgivenmoresecurity.

33058504371496196903169 5
8948327008936921

Aspertheabovediagram,weallknow theprocess involvedinthehackingofdata.Theencrypteddata willbeintheform0'sand1'sduringtransmission. Sotherewillbeaspecialfeatureinthisalgorithm.

Yesthere isaspecialfeaturebehindthisalgorithm. Thisalgorithmwillbeframedassoftwarewiththesamepatte rnflow andwillbegiventoauthorized usersororganization.Whatarecriteria'sinvolvedintheSoft ware:

A. Thesoftwarewillbedesignedusing Javaand MySQLasbothare feasibletechnically,operationallyetc...
B. B. The software will be their only withadministrators (Systemadmin,dataadminetc...)oftheorganization.
C. Thesoftwarewillbeloadedontheserver andwillbeconfiguredforencryptinganddecryptingp rocess.
D. Flow ofthesoftwareprocessisshown below.

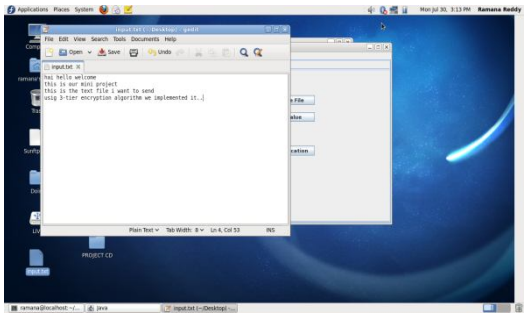

Figure 2: Input Text File

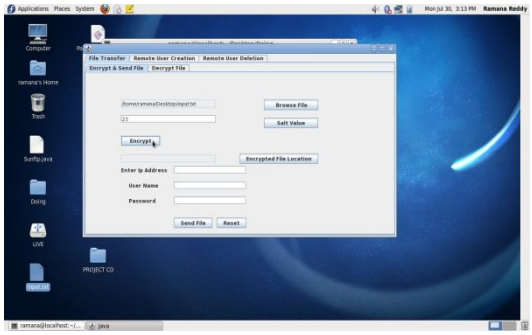

Figure 3: Encryption Process

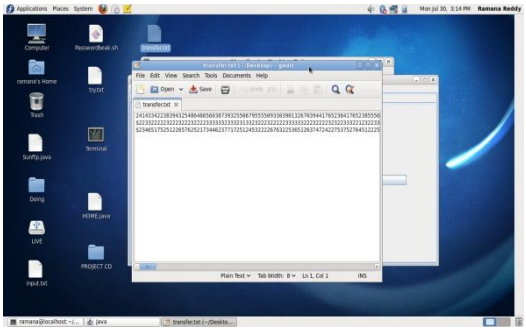

Figure 4: Cipher Text

S. No	PTRSA	CTRSA	PTSRSA	CTSRSA
1	This is my research paperis	t@&&[jku](()p	This is my research paper	PPD XAB @@67 %
2	We are from cse branch people	Cb^^ 883cd0 d3be- aafo	We are from cse branch people	Ert!!%$ $efght* *%
3	What is the impact factor of your journal ? ****	BB c 9c7632 8078b %%@!! &^..*(	What is the impact factor of your journal ? ****	VFCA XX 23##op r>>?yt

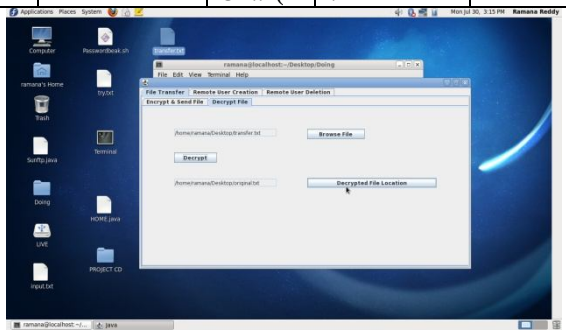

Figure 5: Decryption Process

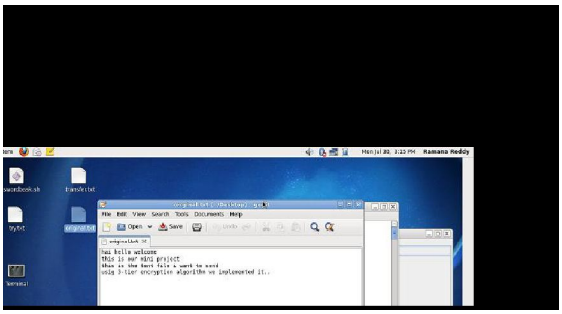

Figure 6: Decrypted File

The same way the decoding process will also be carried out. The screenshots are designed using Linux environment to show how this applications hould be customized.

VI.PRESENTAPPROACH

In this present world, many organizations go with the third party like Veri Signetc. They adoptcertain policies to give security for the datatransaction over the network. Butalongwiththatifinitiallythesystem administratordothisencryptionprocesswiththisapplicatio ntheorganizationcanbeeven moreassuredoftheirdatabeingsecured.

VII. RESULTS

S.No	Size of File	Time taken for RSA	Time taken for entire algorithm
1.	1KB	86millisec	212 millisec
2.	**6**KB	7109 millisec	24920 millisec
3	10KB	25955 millisec	86729 millisec

PTRSA → Plain text of RSA Algorithm
CTRSA → Cipher text RSA Algorithm
PTSRSA → Plain text of socket RSA.
CTSRSA → Cipher text of Socket RSA.

VIII.CONCLUSION

Thismethodologywillgivethesecurity tothefilesofanysizesand can be transmittedo verlongdistances i.e.WAN. Theserverwill have then cryption methodology and decryption process will be specified tothetrustedparties/clients.FinallyIwanttomentionthemainco mplexityitcreatesforthehackerisintheunderstandingthetype of operations used here. This methodology will definitely be an effective way to secure the files over the low privilege, which is the main goal of this project.

VIII.REFERENCES

[1]Datacommunicationandnetworksby Behrouz.A.Forouzan,FourthEdition.
[2]CryptographyandNetworkSecuritybyWilliamStallings,F ourthEdition.
[3]RSAEncryptionbyTomDavis, http:\\ www.geometer.org\mat hcircles.
[4]AnImplementationofAESAlgorithmSubmittedby:Prasha ntShah.
[5]AdvancedEncryptionStandard http: // www.vocal.com
[6]http://en.wikipedia.org/wiki/Series_%28mathematics% 29.
[7]InternationalMathematicalSeriesEd.:Rozhkovskaya,Tam araISSN:1571-5485.
[8]http://en.wikipedia.org/wiki/RSA_Security.