THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Data Encryption and Decryption Using RSA: A Review

Parshotam
Department of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India
parshotam.22738@lpu.co.in

Jeevan Bala
Department of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India
jeevan.25233@lpu.co.in

Abstract

SSL is a cryptographic protocol that is now primarily used to connect securely to the server. It depends on the practice of cryptographic purposes towards achieve a secure connection.Authentication is the initial purpose that makes it easier for the server to be classified and vice versa[6].Several other functions were used for the same purposes, such as encryption and security integrity.RSA algorithm is the best shared cryptographic algorithm used to ensure security.So far, it has numerous security holes to be allocated.This paper discussed the enhancement of this.Inthispaper,analterationofRSA, use of fingerprint to generate RSA key and generation of RSA key using permutation function is discussed thatwouldgive moresecurecommunication.So,it will give an idea to the readers about in how many ways the security of SSL can be improved by modifying the RSA algorithm forsecurecommunication.

Keywords
SSL,RSA,Fingerprint, Permutation

1. INTRODUCTION

Secure Sockets Layer (SSL) is the most widely used Web cryptography protocol. SSL uses a grouping of cryptographic processes to ensure secure network communication. It protects data message by providing encryption, integrity and authentication messages. Secure Socket Layer specification approved the annoying elements in order to support the solutions to encryption, authentication and honesty. [7]

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

This is a protocol used to establish secure data contact between a transmitter and receiver. There are various bowsers like Netscape,Internet Explorer, Firefox, Google chrome and Safarisupports the versions of SSL.SSL is essentially situated between the protocols TCP and HTTP [8].HTTP is simplified to HTTPS (Secure),that is now the normal encoded solution to contact on the World Wide Web.

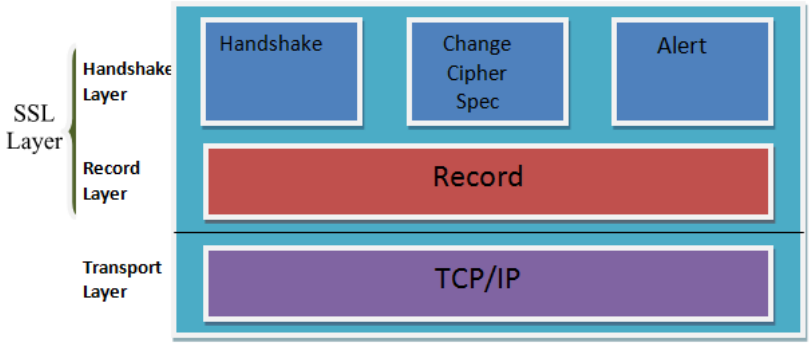

Figure1.SecureSocketLayer

The SSL code of behavior purpose is to use mutually dependent cryptographic tasks called Authentication, Encryption and Integrity. [9]The first feature used in SSL is Authentication.This task is primarily aimed at identifying and authenticating the two parties involved in the interaction. This functionality is accomplished through a public key encryption and a digital certificate from the reliable Certificate Authority [10].

The next objective of the SSL protocol stands to encrypt; this only makes the intentional receiver recite the message.SSL can use messages to encrypt as opposed to encryption algorithms.The client and the server consult the algorithm to be used throughout the SSL handshake process that takes place at the beginning of respectively SSL session.AES, RC4, Twofish and Blowfish are different examples of SSL-supported encryption algorithms. [17]

Integrity is the third objective of the SSL protocol to ensure that the server receives a harmless and complete message sent by a client.To confirm the message's integrity, the client uses a hash function to digest the message and send it to the server.The server also digests and compares the digestion.And if the outcome of the correlation isn't the same, somebody changed the message.Examples of a SSL-based hash function are SHA1, SHA2 and MD5[17].

The suppliers can encryption and decryption utilizing the RSA calculation. Given the computational grouping of the RSA calculation, the utilization of the equipment ought to give huge execution enhancements over programming cryptography. The use of RSA encryption and decryption hardware permits the request to take to use additional secure key sets such as key sets that are stored on the card and that retain the delicate secluded key alwaysexisting in the clear.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

The goal is to preserve confidentiality of communications use a symmetrical encryption scheme.Symmetric encryption means the sender and the recipient share the similar key.Symmetric encryption is usually used to decrypt client-server messages and not asymmetric encryption (public key), because symmetric schemes are quicker than asymmetric schemes.To toggle the symmetric keys between both the parties asymmetric method is used. [8]Therefore, a secure public key must be used to protect the symmetric keys which are then used to encrypt the messages.RC4 and AES are the symmetrical cipher used to encrypt the transmitted messages.Integrity is the third and last function used in SSL. The role of this function is to protect the integrity of the data against invasion. [17].

In addition to authentication, the use of RSA in SSL also confirms data security [12]. The exchange of messages in this situation will be established.Using a superior size of RSA keys to avoid such attacks is widely recommended.[13].And at the moment, the key size calculated to be protected is 3072 bits wide.

Now a day everyone is using internet and the information is passed on the network. Basically the information which is passed on the network is our private information. And on the network there are numbers of attackers is present and they want to hack our information from the network. Then they can use it for their own purpose. This leads to the loss of user's information on the network. This information may be the user account details, bank account details and may be other personal information which may be very important for them.

So that is why, now a day security is more concerned and important issue. Now to protect the information on the network, various researchers designed algorithms. When these algorithms actually implemented on the network then it will be difficult for the attackers to hack the information because the attacker do not have authorization to access the information.

2. LITERATURE REVIEW

In order to improve security, the authors concentrated on the RSA calculation. Also, they utilized OAEP that way. OAEP is one of the uncommon open key encryption frameworks that are institutionalized and generally conveyed. OAEP has been demonstrated to be IND-CCA protected, accepting that the essential doorway change is incomplete single direction. Be that as it may, it doesn't ensure a significant level of security for a viable selection of parameters. Also, later on analysts found that the circumstance is surprisingly more dreadful in light of the fact that both breaks down are led in a solitary quarter condition, for example where an adversary gets a solitary ciphertext challenge. This doesn't consider the way that different ciphertexts of related messages can be seen by a foe. The consequences of the multiuser setting propose that the ensured solid security will debase by factor of q, which is the quantity of test ciphertexts that a

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

rival can get. What's more, later on specialists propose an extremely basic adjustment of the OAEP encryption, which requests that the occasion of trapdoor stage is applied uniquely to a fragment of the OAEP change. At that point they show that this present plan's IND-CCA security is firmly identified with the arbitrary prophet model's single direction strength of trapdoor change. This implies the RSA-OAEP's tight security under the RSA supposition. Specialists accepted that this change is anything but difficult to actualize and the advantages it offers merit the consideration of standard bodies. [1]

Xin Zhou et al explained that, one of the essential methods for ensuring data security is the cryptographic procedure. In addition to the fact that it provides classified data, it additionally gives computerized signature, encryption, mystery sub-stockpiling, security of the gadget, and different capacities. The encryption and decryptionplan can along these lines assurance the privacy of data. The security of the encryption and decoding calculation depend on upon the calculation, although the inward structure of the science meticulousness additionally relies upon the key privacy. The role of key is very important for encryption calculation, which guarantees that anybody in the encryption outline can encode and decode information after the key has been released; this implies the encryption calculation is futile. In the encryption and decryption process, consequently, what sort of facts you decide to be a secret key, how to transmit the private key are significant issues. This paper recommended a total and down to earth answer for RSA encryption/decoding dependent on the investigation of general society key calculation for RSA. Moreover, subtleties on the encryption method and execution of code are given..[2]

In this paper, authors found that, in addition to technological development today, people are greatly accessing informationin order to communicate with various media using the Internet. Mass media send posts that are not necessarily safe. Someone who wants to send the sender a hidden message is often discovered, but people who are reckless will know the messages. So the sender is disappointed because only the irresponsible people know the secret message to the recipient.This is the reason to improvise the security of message content; first, the processing of image is importantbefore applying feature extraction to generate RSA keys. [3]

The authors explained that, Data encryption is essential to keep transactions and data transmission safe and secure.Data may be hacked or intruded whenever we give our card details. It should therefore only be known to that bank to ensure that we have to encrypt the data and decryption approach. It is therefore possible to use this RSA algorithm to achieve this objective. Where only intended sender and receiver can be familiar with data encryption and decryption. In the paper, the authors recommend the technique that we call it Modified RSA to make the RSA technique safer. A transposition module is designed to encrypt the data using the Row Transposition process. This transposition module will be entered before the card details are given

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

to RSA, which scrambles and rearranges the data. The transposition output will then be delivered to the updated RSA generating the cipher text to be sent via network. The RSA, along with the transposition module will be capable of providingdual security for the whole system. [4]

In this study, researchers present two comprehensive algorithms that validate the trapdoor permutation property of the RSA function $RSA_{N,\ e}(x) := x^e \bmod N$, where $N = p^r q$ is a multi-power RSA modulus with unidentifiedfactorization and r is anidentifiedpositive integer. Theexisting work gives actual certification for a prime exponent e when $e \geq 2N^{((gcd(r,\ e-1))/(r+1)2+\epsilon}$ and for a composite integer $e = e1^{s1}e2^{s2}...eu^{su}$ when $ei \geq 2N^{((gcd(r,\ ei-1))/(r+1)2+\epsilon}$ for i = 1, …, u, where e_i is a recognized prime, s_i is a positive integer, and $\epsilon > 0$ is small constant. The algorithms used Coppersmith's technique for computingunivariate modular polynomial equations and run in time $O(\epsilon^{-7}C \log^2, N)$, where $C \leq ur^2$ is a constant number.[5]

Table 1Comparison of between different approaches

Author	Year	Paper	Approach
Alexandra Boldyreva, Hideki Imai and KazukuniKobara	2010	[1]	Modification of the OAEP authentication using part of the OAEP conversion trapdoor permutation.
Xin Zhou and Xiaofei Tang	2011	[2]	Genuine answer for RSA encryption dependent on the investigation of RSA open key calculation
SayutiRahman, Indah Triana, SumiKhairani, AmruYasir, SitiSundari	2017	[3]	To generate the RSA key, use the fingerprint picture.
TusharVyavahare,	2017	[4]	Row method of

Copyright © 2019Authors

DarshanaTekade, SaurabhNayak, N Suresh kumar and S SBlessyTrenciaLincy			transformation to encrypt the data.
Xiaona Zhang, Li-Ping Wang and Jun Xu	2019	[5]	Multi-power RSA feature permutation holdings.

3. CONCLUSION

Inthispaperafter comparing various research papers, we found that theRSAalgorithmtakesamount ofliabilitiesthatmaybebroken, thereforeeasinghackingofthealgorithm.There is therefore a need to adjust safety mechanisms in order to ruin the browbeaten breaches. Many modified RSA algorithm methods have been discussed here. After performing the comparison of various research papers we found a very good approaches in which the authors done and applied the various techniques to improve security of SSL by modifiedRSAalgorithms using Modification of the OAEP encryption, Genuine RSA encryption arrangement grounded on the investigation of RSA open key calculation, use of fingerprint image to generate RSA key, Row transformation method to encrypt the data, Permutation possessions of the multi-power RSA function.

REFERENCES

[1] Xiaona Zhang1, Li-Ping Wang2, Jun Xu2, “Certifying multi-power RSA”, IET Information Security Research Article, 2019.

[2] TusharVyavahare, DarshanaTekade, SaurabhNayak, N Suresh kumar and S SBlessyTrenciaLincy, “Enhanced rearrangement technique for secure data transmission: case study credit card process”, 14th ICSET-2017 IOP Publishing IOP Conf. Series: Materials Science and Engineering 263 (2017) 042102 doi:10.1088/1757-899X/263/4/042102 1234567890

[3] Sayuti Rahman1, Indah Triana2, Sumi Khairani3, Amru Yasir4, Siti Sundari5, “RSA KEY DEVELOPMENT USING FINGERPRINT IMAGE ON TEXT MESSAGE”, International Conference on Information and Communication Technology (IconICT) 1234567890

IOP Publishing IOP Conf. Series: Journal of Physics: Conf. Series 930 (2017) 012037

[4] Xin Zhou, Xiaofei Tang, “Research and Implementation of RSA Algorithm for Encryption and Decryption”, The 6th International Forum on Strategic Technology, 2011.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

[5] Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE, and KazukuniKobara, "How to Strengthen the Security of RSA-OAEP", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 11, NOVEMBER 2010.

[6]YogeshJoshi,DebabrataDas,SubirSaha,InternationalInstituteofInformationTechnology Bangalore(IIIT-B),ElectronicsCity,Bangalore,India."MitigatingManintheMiddleAttackover SecureSocketsLayer,2009

[7]WhatisSSLandhowtheSSLworks
http://docs.oracle.com/cd/E17904_01/core.1111/e10105/sslconfig.htm

[8]A.J.Kenneth,P.C.VanOrshotandS.A.Vanstone,HandbookofappliedCryptography,CRCpress, 1977.

[9]ITsecuritywebsite,TheSecureSocketsLayerProtocolEnablingSecureWebTransactions,http:// www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/index.html

[10]RSAwebsite,5.1SecurityontheInternet,http://www.emc.com/security/rsa-securid/rsa-authentication-manager.htm

[11]ITsecuritywebsite,therisksofshortRSAkeysforsecurecommunicationsusingSSL, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4259828&url=http%3A%2F%2Fieeexplore.ie ee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4259828

[12]H.Otrok,SecuritytestingandevaluationofCryptographicAlgorithms,M.S.Thesis,LebaneseAmericanUniversity,June2003.

[13]Bit-Stuffinghttp://en.wikipedia.org/wiki/Bit_stuffing

[14]CiscoSystems,IntroductiontoSecureSocketsLayer,http://www.ehacking.net/2011/05/secure- sockets-layer-ssl-introduction.html

[15]A.0.Freier,P.KarltonandP.C.Kocher,TheSSLProtocol,version3.0, http://www.cryptoheaven.com/Security/Presentation/SSL-protocol.htm

[16]W.Stallings,CryptographyandNetworkSecurity,2nded.,PrenticeHall,UpperSaddleRiver,NJ ,1999.

[17]H.Otrok,PhDstudent,ECEDepartment,ConcordiaUniversity,Montreal,QC,CanadaandR.Haraty,AssistantDean,SchoolofArtsandSciences,LebaneseAmericanUniversity,Beirut,Lebanon andA.N.El-Kassar,FullProfessor,MathematicsDepartment,BeirutArabUniversity,Beirut,Lebanon"ImprovingtheSecureSocketLayerProtocolbymodifyingitsAuthenticationfunctions"2006

Copyright © 2019Authors