ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

SECURED VIRTUALBANKING SYSTEM USING ASYMMETRIC CRYPTOGRAPHY

Sudeepta Chakraborty[1], Durai Raj Vincent P.M[2]
[1]II[nd] MCA, SITE, VIT University,
[2] Associate Professor, SITE, VIT University.
Email: sudeeptach@gmail.com

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

Digital certificate is like a tamper free seal, and any changes can easily be detected. Digital certificates, therefore, are known for providing high-level security.RSA is an algorithm used in digital certificates. The paper focuses on implementing a secure modified RSA algorithm for virtual banking over the internet. Virtual banking requires a lot of online transactions and money transfers. Therefore, it is essential for the system to be secure. The modified RSA approach uses three prime numbers p_v,, q_v, r_v instead of two and is much more secure than the regular RSA. Implementing this modified approach increases the security of virtual banking by level 2. The paper also proposes a method to secure the values of p_v, q_v, and r_v stored in the database, in order to avoid offline hacking.

Key words: RSA, Digital Signature, OTP.

Introduction

In today's world humongous amounts of data gets transmitted through communication channels within seconds. Therefore, Security and Confidentiality of this data is very important. Cryptography is the study of theconversion of a plaintext message to an encrypted format in such a way that only intended users can decrypt the data. Many schemes regarding the same have been proposed before. Everything is done with a few keystrokes and mouse-clicks. With virtual banking, a customer can make huge transactions online within minutes. Customers can view their bank account balances, download their bank statements, order cheque books, view images of paid cheques etc. The virtual banking facility can be provided through mobile banking or e-banking. Therefore, protection of this huge amount of data is a major issue. A customer's bank account details, transactions etc is required to be kept confidential and secure in such a way that no external malpractitioner is able to gain access to his/her account. Also, transactions need to be secure so that the

customer is well assured that only a legitimized user is at the receiving end. The most efficient way of doing this is using Digital Signatures. A Digital Signature is like a tamper free seal and any tampering of the contents can be detected. It provides a mathematical scheme for proving the authenticity of a message. If a digital signature is valid then there is no question of doubt about the authenticity of the party to which the certificate is allotted. The sender cannot deny the fact that the message was sent by him. Security of data in the virtual banking area is very much important. Hackers and attackers always find new ways to hack into a security system of specially systems like an online banking system. Therefore, increasing the security in such areas becomes a major issue of concern. Virtual banking involves huge money transactions online and depositions. Any mismanagement or security problem can lead to a major loss to the client.

Therefore, optimal security is needed in such areas. Reports in past have proved, that this is the area where hackers make their maximum business. Attacks such as salami attacks are very common, which go unnoticed if the information that is being communicated between two parties is not fully encrypted and secure. It is very important to provide security in this area, as a compromise in security might lead to a huge money loss of both the client as well as the company, also it might create other issues such as money getting transferred to the attacker's account without the customer or the bank knowing. Many algorithms have already being proposed regarding the security. Such as hash algorithms, RSA etc. These algorithms have been secure, but still, an even more secure approach is required as the data set is increasing, with more and more people knowing about the online banking service. RSA algorithm is a very popular algorithm to implement security using Digital signatures. The RSA algorithm uses the concept of a public and a private key. The public key is distributed freely to everyone, but the private key is confidential to the owner. Anyone who wants to send a message can encrypt the message using the receiver's public key. Then, only the receiver can use his/her own private key to decrypt this message. No one else is able to view the message as only the receiver has the private key. If the receiver has a digital certificate which is signed by a valid certifying authority, then it is certified to be authentic on all grounds. Various performance analysis of RSA on virtual banking has been done earlier, which speak about how to secure the regular RSA is, how easily it can be cracked. Regular RSA passes the value of 'n_v', which can be decoded by the hacker, and then values of the prime numbers can be determined by factoring 'n_v'. However, this becomes much difficult when large prime numbers are chosen. This paper proposes a modified RSA approach to implementing virtual banking in a very secure way. Also, it discusses a way to secure values of p_v, q_v and r_v in the database, to prevent offline hacking. The

modified RSA approach uses 3 prime numbers, p_v, q_v and r_v instead of 2. It is more secure than the regular RSA algorithm since the public key and the private key can be found only if the values of the three prime numbers p_v, q_v and r_v, are known. These values can only be known if thevalue of 'n_v' is found since thevalue of 'n' equals to $p_v*q_v*r_v$. In the modified RSA 'n_v' is not passed in any of the key parameters, instead of that another variable, 'X_{ran}' is passed. This 'X_{ran}' is not depending directly on the value of p_v, q_v, r_v or n_v. It is a random number chosen between a specified range. Therefore finding values of 'e_v' and 'd' becomes close to impossible, also, this enables total encryption of transactions. With the implementation of the new modified version of RSA, using 3 prime numbers, the security is increased by level 2.

Literature Survey

In the paper [1], Ying-yu Cao and Chong Fu have proposed an n-carry array-based method for large calculations used in RSA encryption and decryption. This works by generating RSA public and private keys randomly using the C++ large number library functions. Finally, it was concluded that if the RSA key length was 1024 bits, then it can be generated within 2 minutes, whereas the encryption and decryption for 1024 bits are done within 2 seconds. KT Ng WN Chau, and YM Siu, in [8] have focused on providing secure communications over the internet. Their approach involves the concept of session keys to enhance security and performance of RSA. JDBC tools were used to provide client-server connection and data access. The session key exchange between the client and server is provided using the secure socket layer protocol. Chen Tianhuang and Xu Xiaoguang, [2] pointed out the security concerns in E-commerce. Therefore they provided adigital signature as a means of implementing security in e-commerce sites. An improved DSA algorithm was hence proposed, which focused on making the current DSA more efficient, thus providing high security. In [3], authors E.Madhusudhana Reddy, K.Suresh Kumar Reddy and M.Padmavathamma have designed a digital signature scheme for useful and secure communication between 2 or more parties. This research was based on the application of the Jordon-Totient function on RSA digital signature scheme. It used one public key and two private keys. The performance and time taken for encryption and decryption using this new approach were compared and an analysis was performed on the same.Later on, P. Kitsos, N. Sklavosand O. Koufopavlou in [4], proposed a VLSI implementation of digital signatures. It is based on a combination of the secure hash function and the 512-bit RSA cryptography algorithm. It discusses how thehash function can be used as an efficient means for providing security, by comparing the computed checksum with the derived checksum.In the year 2015, Liangliang Wang, Kefei Chen, Yu Long, Xianping Mao and Huige Wang in [5],

proposed a method to prevent private key attacks. This method involves generation of a partial private key, i.e, a part of the private key is generated by the private key generation center and the another part is a secret value that is chosen by the user itself. In [6], authors Chen Hai-peng, Wei Wei and Shen Xuan-jing aimed at providing a more advanced hash function named HRFA. This algorithm used a self-certified public key method using RSA, which involved four steps: system initiation, user registration, signature creation, and signature verification. Security algorithms in areas likeID based verifier signature scheme were proposed by various authors including Shifeng Sun, Qianyan Wen, Zhengping Jin, and Hua Zhang in [7]. Itwas based on the bilinear Diffie-Hellman assumptions.Later , in 2015, Soram, Ranbir, and Engudam Sanahal Meitei in [16], presented a paper on the detailed performance of RSA on virtual banking and the possible attacks and challenges on the RSA scheme.

Proposed System

Since hackers have developed ways to find the private keys used in RSA algorithm. Therefore in this paper, a more secure modified RSA is used for Virtual banking or online banking. This secure RSA uses 3 random large prime numbers p_v, q_v and r_v, instead of two as used in the regular RSA algorithm. It is more secure than the regular RSA algorithm since the public key and the private key can be found only if the values of the three prime numbers p_v, q_v and r_v, are known. These values can only be known if value of 'n_v' is found. The algorithm passes a variable 'X_{ran}' in the key parameters instead of 'n_v'. Also, the values of p_v, q_v and r_v are 3 random 512-bit prime numbers, therefore it is very difficult to guess all the three prime numbers correctly.

The modified RSA algorithm is as follows: Begin:

1. Choose the values of the 3 prime numbers p_v, q_v and r_v.
2. Calculate the value of 'n_v',

   Where $n_v=p_v*q_v*r_v$,
3. Calculate $\phi_v(n_v)=(p_v-1)*(q_v-1)*(r_v-1)$
4. Calculate the value of the integer 'e_v' now, Where, $\sqrt{n_v} < e_v < \phi_v(n_v)$, also GCD $(e_v, \phi_v(n_v))=1$, where e_v and $\phi_v(n_v)$ are co-primes.
5. Now compute the value of 'X_{ran}', If $p_v > q_v$, Then X is chosen such that:

   $n_v - p_v <$ 'X_{ran}' $< n_v$, Else If $p_v < q_v$,Then X is chosen such that, $n_v - q_v <$ 'X_{ran}' $< n_v$

6. Calculate the value of d, where d is the private exponent,
7. $d = e_v^{-1} \bmod \phi_v(n_v)$
8. The public key PU (e_v, X_{ran}), is used for encryption,And the private key PR (d, X_{ran}) , is used for decryption,
9. Encrypt plaintext where M_{en}, such that $M_{en}<n_v$,Using, $C_{pl} = M_{en}^{e} \bmod (X_{ran})$
10. Decrypt the cipher text using ,$M_{en} = C_{pl}^{d} \bmod (X_{ran})$, End.

The paper focuses on eliminating key hacking, as the private key(d), will only be present with the receiver. Therefore, only the receiver can decrypt the encrypted session key. Finding the value of 3 large random prime numbers is close to impossible. They can be known only if 'n' is known. But here, instead of 'n', another variable 'X' is passed, which does not directly depend upon these prime numbers

The following procedure is followed when theabove-modified RSA is applied on virtual banking:

If Alice (client) wants to make an online transaction using virtual banking then:

1. Alice will have to send a transfer request to the bank server, using which she wants to make the transaction. She does this by logging into the bank server's website. This acts like a request that Alice wants to initiate an online transaction. The server responds by sending Alice its Digital Certificate. This Certificate will contain the server's public key.
2. As Alice makes the entry in the username and password column, the bank server, checks the credentials against the bank server's Database. The bank server has a list of all the valid customers in the bank. If the username or the password entered by Alice is found in the database, then the bank server reciprocates with an "Authorized access" message. If the client is authentic, then the bank server sends its own Digital certificate as a mark of its authenticity. The Digital certificate that is sent by the bank server, has to be authentic, and there can be absolutely no temptation with the certificate. Any changes made in the certificate can be identified immediately, and the connection will be ended, as the bank server might be under an attack. It is not possible for a vulnerable bank server to send a digital certificate which is valid.
3. Now the client browser side generates a random six digit OTP and encrypts it using the server's public key, that was sent in the digital certificate. The encryption process here is carried out using the modified RSA approach. The encrypted session key is then sent over to the server side.

4. The server upon receiving the encrypted key uses its own private key to decrypt it. Only the bank server can decrypt the key with its own private key. Again the process of decryption of the encrypted session key is performed using the modified RSA.
5. Now both, the client browser(Alice) and the bank server will have the same session key.
6. A secure connection between these two parties is established now, and data transfer for the particular session can now begin.

A secure tunnel is created at the end of the process using a strong modified RSA encryption. The communication in this tunnel cannot be seen by any outside party. Only the parties at the two ends of the tunnel will have access. The Session key expires as the user logs out of the particular session.

Offline Security of p_v, q_v and r_v. : The values of p_v, q_v and r_v calculated in the beginning of the entire process are stored in the database before the virtual banking process starts.

Begin:

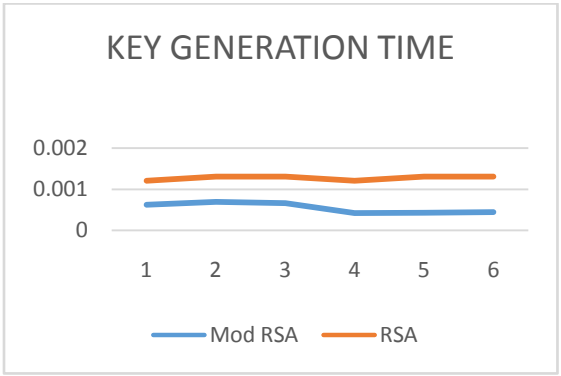
1. Calculate values of p_v, q_v, r_v, ϕ, e_v, $X_{ran}$and d.
2. Connect to the database. The values calculated in step 1. are then to be stored in the database tables. Therefore, insert the values of p_v, q_v, $X_{ran}$and ϕ in the first table T1.
3. Insert the values of r_v, e_v and d in another table T2 of the database.
4. Next, the process of virtual banking begins. When the OTP generated needs to be encrypted, the values of $X_{ran}$and e_v are retrieved from the respective tables and the encryption is performed.
5. The session key at the bank server end is then decrypted. Again the values of d and X_{ran} are retrieved from the various tables and the decryption process is performed.

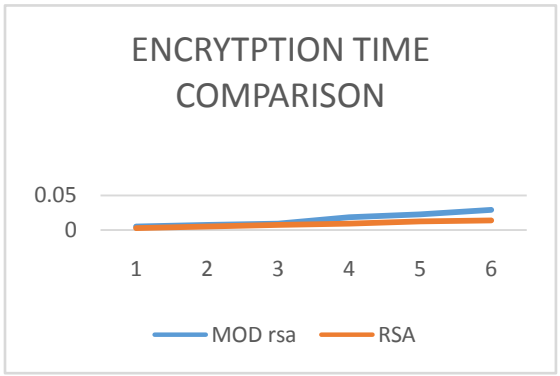
End

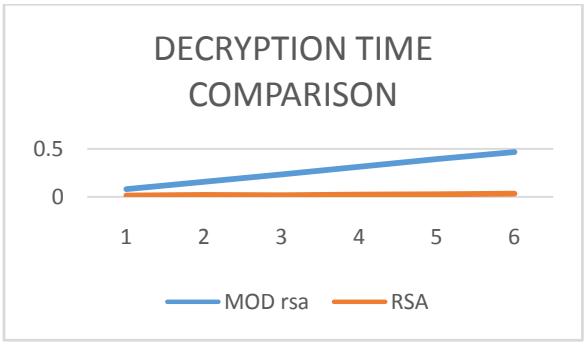
The above algorithm provides security if a hacker tries to access the values of p_v, q_v and r_v , by hacking the database in which they are stored. The values of the various variables are calculated in the first step and stored in different tables, so that even if the hacker hacks one of the tables, he will not be able to find the values of all the variables in the same table. Hacking both the tables simultaneously is very difficult. This offline security scheme takes place before the entire transaction process begins.

Result and Analysis

1. Modified RSA, when implemented on virtual banking, increases the security of online transaction by a factor of 2.
2. Client validation in the first step, authenticates the client, so as to ensure that the client is genuine.
3. Modified RSA, takes much lesser time than regular RSA, for key generation, therefore the entire process is fast enough.
4. Digital certificate sent by bank server, and its verification on the client side, ensures that the message is received by the original bank server and is not hoaxed. Digital certificate provides a tamper freeseal and any changes in it can be immediately detected.
5. A six digit OTP is generated in each session, which is used to launch the session by encrypting it with the public key of the server. This OTP expires when the session ends.
6. The session key can be decrypted only by the bank server, as only the server will have the decryption key.
7. Encryption and decryption time in modified RSA is higher than regular RSA.







The above graphs are generated after calculating the encryption and decryption time with messages of various lengths.

Conclusion and Future Work: In this paper, the modified RSA algorithm is presented to increase the security in the virtual banking area. The modified RSA provides twice as much security as is provided by regular RSA. The values of

p_v, q_v and r_v are extremely large and random, therefore they are almost impossible to determine. It would take a hacker years to factor and find the values of p_v, q_v and r_v . A variable 'X_{ran}' is passed in the key parameters instead of 'n'. The key generation time is much lesser in the modified RSA algorithm than the regular RSA. After the session key is decrypted on the bank server side, a secure tunnel is established between the client and the bank server. This secure tunnel enables the client and the server to communicate safely for that session. Any third party is not able to see through this secure tunnel. Only the parties at the two ends of the tunnel (i.e. the client browser and the bank server) can see the data transfer within the tunnel, for that particular session. Also, Storing the values of p, q and r separately in two tables increases the security as it prevents offline hacking. A hacker can never have access to all the three variables simultaneously. In future, the security level in virtual banking can be increased by using a modified RSA, with 4 prime numbers. Modified RSA with 4 prime numbers if implementing on online banking, should provide even greater security. It would become even more difficult for a hacker to guess 4 random huge prime numbers. Factoring and determining the value of 'n_v' from four prime numbers is even a greater challenge when the value of 'n_v' itself is not known. With the increase in the dataset, the four prime number mechanism can prove to be more secure. Also, increasing the keylength to 4096 bits will further add to security.

References

1. Cao, Ying-yu, and Chong Fu. "An efficient implementation of RSA digital signature algorithm." Intelligent Computation Technology and Automation (ICICTA), 2008 International Conference on. Vol. 2. IEEE, 2008.
2. Tianhuang, Chen, and Xu Xiaoguang. "Digital signature in the application of e-commerce security." E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on. Vol. 1. IEEE, 2010.
3. Reddy, E. Madhusudhana, and M. Padmavathamma. "MJ2-RSA Signature Scheme in E-Commerce for Fair-Exchange Protocols." Mobile Communication and Power Engineering. Springer Berlin Heidelberg, 2013. 508-511.
4. Kitsos, P., N. Sklavos, and O. Koufopavlou. "An efficient implementation of the digital signature algorithm." Electronics, Circuits and Systems, 2002. 9th International Conference on. Vol. 3. IEEE, 2002.
5. Wang, Liangliang, et al. "A Modified Efficient Certificateless Signature Scheme without Bilinear Pairings." Intelligent Networking and Collaborative Systems (INCOS), 2015 International Conference on. IEEE, 2015.

6. Hai-Peng, Chen, Shen Xuan-Jing, and Wei Wei. "Digital signature algorithm based on Hash round function and self-certified public key system."Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on. Vol. 2. IEEE, 2009.
7. Sun, Shifeng, et al. "A new efficient ID-based strong designated verifier signature scheme." Information Science and Engineering (ISISE), 2010 International Symposium on. IEEE, 2010.
8. Ng, K. T., W. N. Chau, and Y. M. Siu. "An Internet security system for e-commerce." IECON 02 [Industrial Electronics Society, IEEE 2002 28th Annual Conference of the]. Vol. 3. IEEE, 2002.
9. Dong-liang, Liu, Chen Yan-ping, and Zhang Huai-ping. "Secure applications of RSA system in the electronic commerce." 2010 International Conference on Future Information Technology and Management Engineering. 2010.
10. Hu, Gang. "Study of file encryption and decryption system using security key." Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 7. IEEE, 2010.
11. Hwang, Ren-Junn, et al. "An efficient decryption method for RSA cryptosystem." Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on. Vol. 1. IEEE, 2005.
12. P.M.Durai Raj Vincent, Sathiyamoorthy E, " A Novel and efficient public key encryption algorithm" International Journal of Information and communication technology, Vol. 9, No. 2, pp 199-211, 2016.
13. Agrawal, Monika, and Pradeep Mishra. "A comparative survey on symmetric key encryption techniques." International Journal on Computer Science and Engineering 4.5 (2012): 877.
14. Vincent P.M.D.R, Sathiyamoorthy E," A Secured and Time Efficient Electronic Business Framework based on Public Key Cryptography" in International Review on Computers and Software, Vol 9 No 10, pp. 1791-1798, 2014.
15. Patil, Anjali, and Rajeshwari Goudar. "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices." International Journal of Scientific & Technology Research 2.8 (2013): 2006.
16. Aboud, Sattar J. "An efficient method for attack RSA scheme." Applications of Digital Information and Web Technologies, 2009. ICADIWT'09. Second International Conference on the. IEEE, 2009.
17. Vincent P.M.D.R, Sathiyamoorthy E, "A novel and efficient key sharing technique for web applications" in IEEE Fourth International Conference on Computing, Communications and Networking Technologies. 2013.