



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: II Month of publication: February

DOI: <http://doi.org/10.22214/ijraset.2019.2022>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Application of Digital Signature to Achieve Secure Transmission

Reha Musale¹, Dr. R.C. Jaiswal²

^{1,2}E&TC Department, Pune Institute of Computer Technology.

Abstract: *In this application we can send encrypted text messages across various users which are registered in the application database. The registered users can secure their message from alteration and tampering. Also, the user has to register to the system in order to authenticate its identity.*

The sender of the message sends the message along with the encrypted form of the message using the sender's private key. At the receiver's side, the message is converted into hash value and the encrypted message is decrypted using the sender's private key. Both the values are compared. If both the values are same the message is not tampered.

I. INTRODUCTION

Nowadays the user authentication has become prime important in various day to day applications like e-commerce, e-business, bank transactions, etc. In order to achieve secure communication between two or more parties various dimensions like integrity, non-repudiation, authenticity, privacy, confidentiality needs to be achieved. Integrity is ability to ensure that the message sent across is not tampered or altered by any third party. Authenticity is the ability to verify whether the sender or receiver is a certified or registered user or not. Privacy is the ability to limit the information sent across to a particular client or a fixed no of users. The following application guarantees all of the above mentioned parameters.

II. LITERATURE REVIEW

Over the years many researchers have been putting their efforts in developing models to provide security services. However, the users still face insecurity issues due to advent of various hacking techniques. In day-to-day we carry number of transactions like bank transaction, e-commerce, etc. which require privacy and confidentiality[1].

III. PROPOSED WORK

A. System Features

The application provides following features to the users

- 1) The user has to login with the username and password which is stored using MySQL database.
- 2) The application is developed on NetBeans[3] platform. It is platform independent application which means that it can work on any platform.
- 3) The user can select from four different algorithms available for encryption.
- 4) The encrypted and decrypted texts are visible to the user.
- 5) One to many type of communication can be achieved from this application.

B. System Architecture

- 1) The message to be sent is first converted into ASCII value.
- 2) The ASCII is then converted into hash value by applying hash algorithm like MD5 and SHA1.
- 3) The hash value of the message is encrypted using sender's private key.
- 4) The encrypted text and the message both are sent over a secure channel.
- 5) At the receiver's end the encrypted text is decrypted using sender's public key and the message is converted into hash value.
- 6) The decrypted text is converted into hash value.
- 7) Both the hash values are compared
- 8) If their signatures are same the text is said to maintain its integrity.

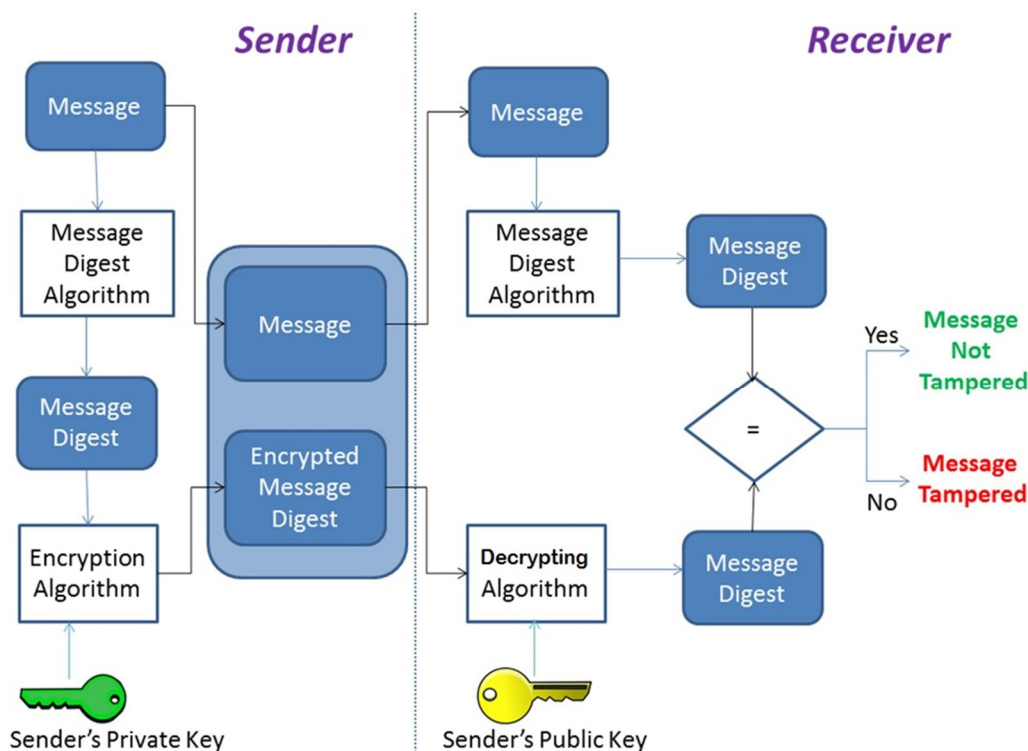


Figure 1 :- Block diagram

C. The Following Steps Were Used To Design The Applicaton

1) **Registration:** If the user is not registered for the application following process must be followed:-

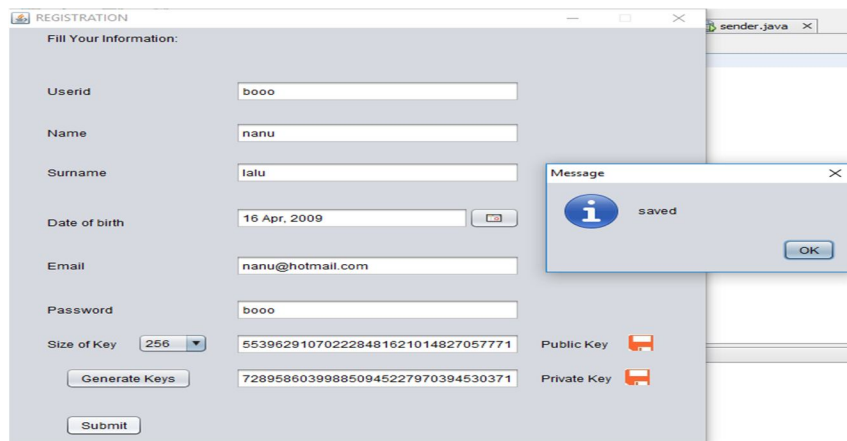
- a) User must enter valid User-id , Name , Surname , Date of Birth email id and password
- b) User must enter the size of the keys to be generated. After clicking on "Generate Keys" button Private key and public key are created. The key values remain stored in the database for a user with unique id.

2) **After Registration**

- a) All the username and password of the logged in clients are store in the db.xml file which has the database for the previously logged in users.
- b) If the user is not logged in , user has to go to "New User" menu and save the credentials. These values are updated in the database table present in the db.xml file.
- c) When the "Start Server" button is pressed on the server side, server socket is created on the default port number which is given by the user.
- d) The server waits for the client to get connected.
- e) On the client side user has to enter server's ip address and port number in order to get connected to the server.
- f) The server is ready for communication once the client's ip address and port number are verified.
- g) The message to be sent is first entered in the text box .
- h) Each sender has an unique pair of "Public" and "Private" keys.To generate a public key user should click on "Generate Public Key" option.
- i) In order to generate digital signature for a particular message , the user must select the encryption algorithms available like RSA[4] , DHA [2] , AES.
- j) Once the algorithm is selected , the desired digital signature appears in the box.
- k) By clicking on "Send" button , the digital signature and the message are sent to the receiver.
- l) On the receiver's end the digital signature appears in the text box .It is also stored in the file a.txt.
- m) The message is converted to hash value and the digital signature is decrypted . Both the values are displayed in the text box.
- n) To check the result the user must click on "verify" button.
- o) If the result is successful a dialog box displaying "Signature integrity do not change" appears.

IV. RESULT

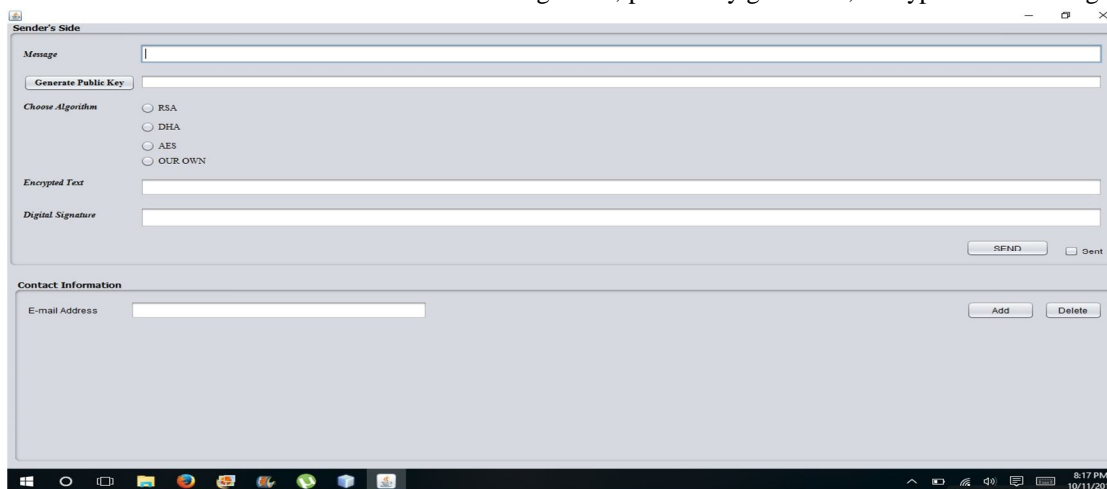
The figure below shows the UI design for registration at the user's side. It is mandatory for any user to register before starting with the application.



The screenshot shows a 'REGISTRATION' window with the title 'Fill Your Information:'. It contains several input fields: Userid (filled with 'booo'), Name (filled with 'nanu'), Surname (filled with 'lalul'), Date of birth (filled with '16 Apr, 2009'), Email (filled with 'nanu@hotmail.com'), and Password (filled with 'booo'). There are also fields for 'Size of Key' (set to 256) and two long alphanumeric strings for 'Public Key' and 'Private Key'. A 'Generate Keys' button is located between these two strings. A 'Submit' button is at the bottom. A small 'Message' dialog box with an information icon and the text 'saved' is overlaid on the right side of the registration window.

Figure 2 Registration of new user

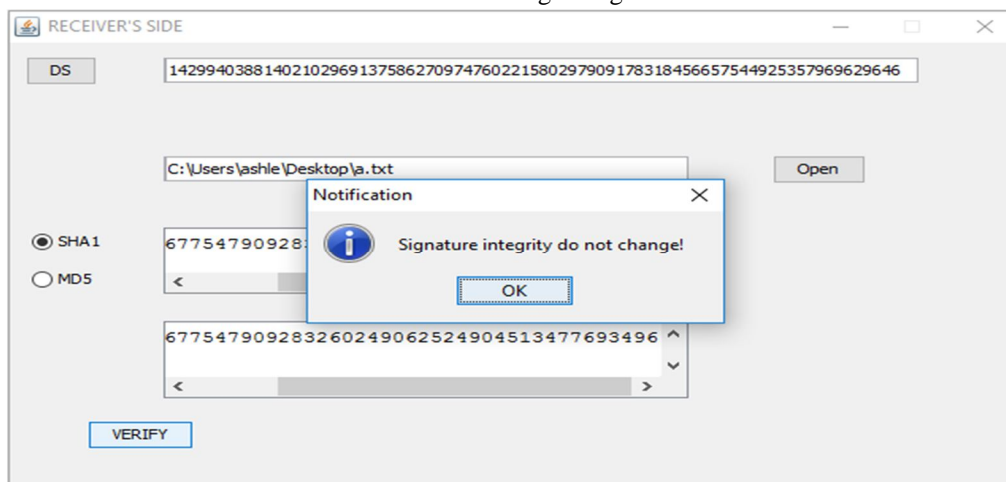
The figure below shows the UI at the sender's end. It has message box, public key generator, encrypted text and digital signature.



The screenshot shows the 'Sender's Side' window. It has a 'Message' input field at the top. Below it is a 'Generate Public Key' button. Under 'Choose Algorithm', there are radio buttons for RSA, DHA, AES, and OUR OWN. Below that are 'Encrypted Text' and 'Digital Signature' input fields. A 'SEND' button is on the right. At the bottom, there is a 'Contact Information' section with an 'E-mail Address' input field and 'Add' and 'Delete' buttons. The Windows taskbar is visible at the bottom of the screen.

Figure 3 Result at the Sender's side

The image below shows the UI at the receiver's end. It shows the digital signature and the verified value.



The screenshot shows the 'RECEIVER'S SIDE' window. At the top, there is a 'DS' (Digital Signature) input field containing a long alphanumeric string. Below it is a file path 'C:\Users\ashle\Desktop\ja.txt' and an 'Open' button. Underneath, there are radio buttons for 'SHA1' (selected) and 'MD5'. Below these are two more input fields, the first containing '67754790928'. A 'Notification' dialog box is overlaid in the center, displaying an information icon and the text 'Signature integrity do not change!' with an 'OK' button. At the bottom of the receiver's side window is a 'VERIFY' button.

Figure 4 Result at the receiver's side

V. CONCLUSION

Using this application we have can transfer messages on locally insecure protocol ,which could be further used in small scale industries, etc. High security is obtained by using MD-5 to convert the message to hash value. Higher security is achieved using RSA algorithm . It is difficult to crack RSA algorithm as it involves factorization of prime numbers which are difficult to factorize. This application can be configured on any communication protocol as it is platform independent.

VI. ACKNOWLEDGEMENT

I would express my deep sense of gratitude towards my mentor , DR R.C Jaiswal for his valuable guidance , keen interest and constructive criticism and encouragement at various at various stages . He gave this paper the insight and the expertise it needed for making it a presentable one.

REFERENCES

- [1] R. Kaur, A. Kaur, "Digital Signature", *Computing Sciences*, pp. 295-301, 2012.
- [2] W. Diffie, M. Hellman, "New directions in cryptography", *IEEE Trans. Inform. Theory* IT-22, pp. 644-654, Nov. 1976.
- [3] Ying Bai, "Introduction to NetBeans IDE" in *Practical Database Programming with Java 1*, Wiley-IEEE Press, pp. 155-315, 2011.
- [4] Xin Zhou, Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption", *Proceedings of 2011 6th International Forum on Strategic Technology*, pp. 1118-1121, 2011.
- [5] Wielenga Geertjan, *Beginning NetBeans IDE: For Java Developers*.
- [6] William Stallings, *Cryptography and Network Security*, Prentice Hall.
- [7] Fan Yingguang, "Digital Signature Technology in E-commerce Security", *Fujian Computers*, vol. 2, pp. 58, 2009.
- [8] Hu Chengjun, "A Brief Introduction to Electronic Signature in E-commerce", *Information Age*, vol. 3, pp. 63-64, 2009.
- [9] Dorothy E. Denning, *Digital Signature with RSA and Other Public-Key Cryptosystems*, Communications of the ACM, 1984.
- [10] Steve Burnett and Stephen Paine, *The RSA Security's Official Guide to Cryptography*, CA USA: Osborne/McGraw-Hill, 2001.
- [11] Kenneth L. Calvert and Michael J. Donahoo, *TCP/IP Sockets in Java: Practical Guide for Programmers*, Second Edition, USA: Elsevier Inc.
- [12] Behrouz A. Forouzan, *Data Communications and Networking*, 4th Edition, :McGrall Hill.
- [13] Geertjan Wielenga, *Beginning NetBeans IDE: For Java Developers*
- [14] H Siregar, E Junaeti, T Hayatno, "Implementation of Digital Signature Using Aes and Rsa Algorithms as a Security in Disposition System af Letter", *IOP Conference Series: Materials Science and Engineering*, vol. 180, pp. 012055, 2017.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)