IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Secure Mailing System

Niti Sharma

Student, Computer Science and Engineering, Delhi Institute of Technology Management &Research, Faridabad, India

Abstract: Thanks to the Internet, because of which the use of E-mails have become faster and easier. More and more companies are using it for better communication. However they are not aware about the risk they are going through .Obviously when you send a letter you know about the confidentiality but when it comes to E-mail system it involves a lots of information security risks. This paper proposes a theory on secure Emails. It develops a theory of CRYPTOGRAPHY In Cryptography ,encryption is a process by which message is encoded in such a way that only authorised user can access it .Encoded message is called Plain text and anonymously decoded message is called Cipher text and the process is called Decryption. For technical reasons, encryption scheme uses a pseudo random key, that is generated by an algorithm .This paper makes use of an algorithm called RSA algorithm for security related issues.

Keywords: RSA, Cryptography, Encryption, Decryption, Information Security.

I. INTRODUCTION

Secure emails are safe and efficient in comparision to regular emails, post and fax .Secure mail system is a process of sending and receiving the secured mails via a secure route. Secure mail is an end to end protection and yes encryption is the only way. To achieve this encryption scheme, the RSA algorithm has been used.RSA is a symmetric public key cryptosytem that make use of two keys. One of the key is called public key ,second is called private key .Public key is used to encrypt the message whereas private key is used to decrypt the message. The implementation make use of two prime numbers as input that is only known to intended recipient after decrypting the message. The RSA algorithm is extensively used in applications for secure data transmission. Typically the application can be categorised as key exchange and digital signatures. When you visit a website like '' //https:''it is likely that your browser is using RSA algorithm to validate the remote server with secure key transmission. The extra feature being added is the concept of cryptography together with RSA in our mailing system. In secure mailing system when you click on send button, the information contained in it is encrypted so it can only read by the intended recipient. Unlike in regular emails, the information is intercepted and can be easily read by everyone. Email security is very essential for all the businesses, to protect our information from threats, hackers and phishing etc. Secure mails is a multitiered discipline that involves the use of many security packages, softwares and security algorithms. Implementing these alogorithms provides us with secure communication.

II. PROPOSED WORK

As organisation is growing at a fast rate ,there is a need for an efficient system between the different employee of different departments.The proposed system "Secure mailing system" serves the organisation's need in consistent and effective manner[3].It allows the user to coomunicate with each other in the most effective and efficient manner.It serve the need of information sharing between the sender and the intended receiver.It involves all the items of an email system like inbox,draft etc.Thus it fulfills all the needs of an organisation.Delivered as a email attachment ,the mails are affected by devastated hackers.which then destroy our data in all aspects.Secure mailing system is a solution to all such problems it sets an password for encrypting the mail and intended recipient use the same password to decrypt the mail .Thus in this way it poses a security to our end to end users .

III.SCOPE

Over the decades the use of internet has increased at a fast rate .Unfortunately, authorised and illegal distribution of digital data has increased.So, there is a vast need to secure our data from such illegal access.So, the solution of this problem is the use of secure mailing system while sending and receving mails .Basically the term secure[1] means the translation of data into a form that is meaningless without deciphering mechanisms.The system termed out to be called as "Secure mailing system".The secure mailing system is meant to keep the security of our mails sent between the users in Lan.The implementation is based on the use of RSA algorithm .The user can easily encrypt the mail by using algorithm .The user sets a password after encrypting the mail and on decrypting enters the same password .Thus unauthorised access is denied .Our data is protected between the sender and the receiver .A user can also easily insert the topics to see the views on a Lan.User can also search for the other member if he knows the emailed or contact

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

number.The main concern of this project is to improve the efficiency and effectiveness of the whole system.To meet the above concern the following methods have been followed .

A. Feasibility Study

The feasibility study is carried out to check the effectiveness of our whole system.During the study the problem definition has been done and aspect of the problem has been determined which are to be included in the study[2].The cost and benefits has been described to determine the accuracy of the whole system.An outline o the procedures and methods followed by the coverage of objectives and file structure of the whole sytem.Special recommendations regarding the project schedules and target dates etc has been determined[4].Our system works to minimise human errors,take less time and proper interaction with the users over the network.

B. System Design

System design is a process of defining the components,interfaces and data of our whole system[5].The modules being used are password module,user registration module,encrypt,decrypt module,add views module,add new topic and search module.Fig 1 shows an example of home page of our project.

Fig 1. Example of homepage of secure mailing sytem

C. Implementation

The implementation make use of RSA algorithm for encryption and decryption.The project make use of two key one is public key and another one is private key also known as secret key .The public key is used to encrypt the message whereas the private or secret key is used to decrypt the message[6] .Fig 2. Explains the concept of encrypting mails.Fig 3.explains the concept of decrypting mails.

1}: System.security.cryptography namespace is being used.
2}: Initialise the textboxes with the variables.
3}: RSAcryptoserviceprovider() class is used to initialise a new instance using the default key[7].
4}: ASCIIencoding() class is being used to encode an alphabet into integers which are mostly represented in hexadecimal or binary notation.
5}: Encoding.getbyte() method is being used to encode all the characters into a sequence of bytes[8].
6}: myrsa.encrypt(new data,false) is being used to encrypt our data.
7}: Similar way is used to decrypt our data.
8}: If the password after the encryption matches with the password after decryption then the concept of RSA holds and the result is being obtained[9] .

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

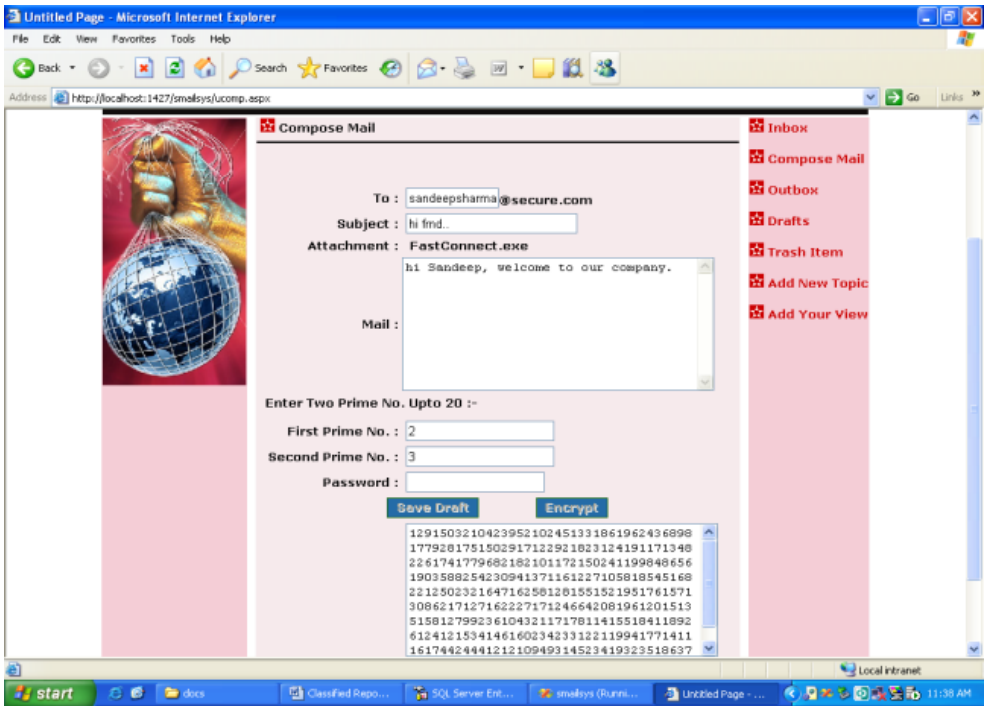

Fig. 1. Example of an encrypting mail

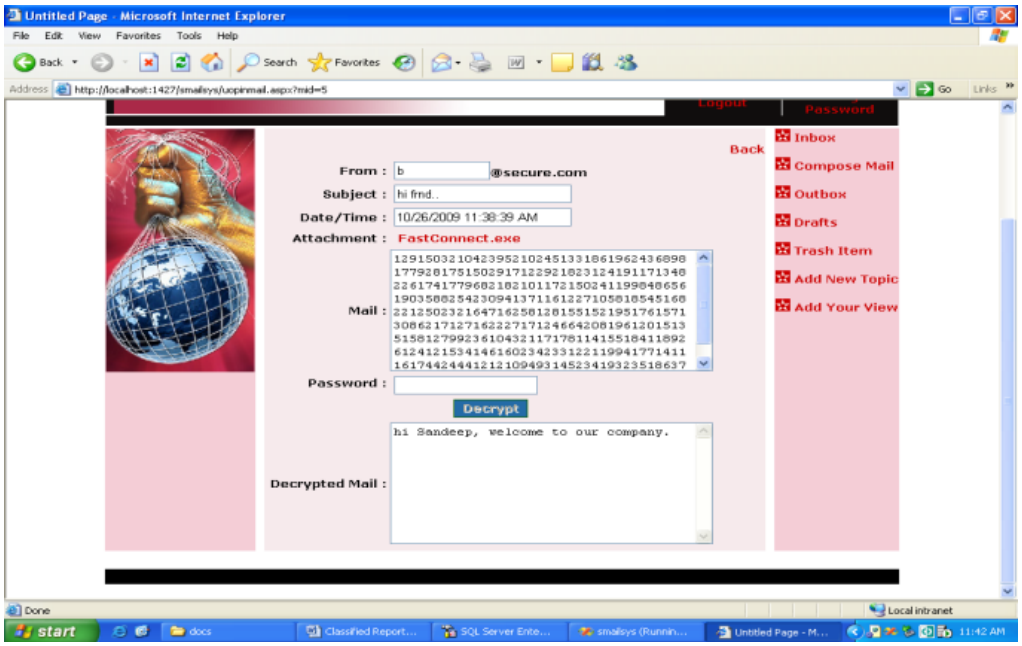

Fig. 2. Example of an decrypting mail

D. References

Examples of reference items of different categories shown in the References section include:

- example of a book in [1]
- example of a book in a series in [2]
- example of a journal article in [3]
- example of a conference paper in [4]
- example of a patent in [5]
- example of a website in [6]
- example of a web page in [7]
- example of a databook as a manual in [8]
- example of a datasheet in [9]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

IV. CONCLUSION

Secure mailing system is made efficient by the use of RSA algorithm.In this paper we have presented the implementation and design of our proposed system.The system designing has been done in such a way that it results into an secure ,robust and integrated sytem .The .Net programming language is being used to implement the RSA algorithm into our project.Sql server has been used to maintain the tables of our module in all aspects.The separation of designing from code has made the task of user very easier .Web technologies like .net and CGI help human user to develop and maintain web applications cost effectively. Our design and architecture is well enough to maintain and secure our mails .Our system has utilized technologies and algorithms so that secure mailing system is most effective.

ACKNOWLEDGMENT

We wish to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template.

REFERENCES

[1] John Edward ,The Essential Guide to Email Security Available:http://www.itsecurity.com/features/essential-guide-email-security-051508/
[2] Praseed Pai,and Shine Xavier ,.Net Design Patterns ,Packt Publishing,Jan. 2017.
[3] Al-Sakib Khan Pathak and Saful Azad 'The RSA Algorithm'
[4] Eric Allman, "SENDMAIL – An Internetwork Mail Router", Program Documentation, 1982
[5] Uyless Black, Network Management Standards, 2nd edition, McGrow Hill, 1994
[6] Bruice Schnieer ,Applied Cryptography ,1993 " Encrypted search engine and Encrypted Database"
[7] J. Case, M. Fedor, M. Schoffstall and C. Davin, "The Simple Network Management Protocol (SNMP)", RFC 1157, May 1990.
[8] NCSA,"TheCommonGatewayInterface",http://hoohoo.ncsa.uiuc.edu/cgi/, 1995
[9] Alexis Leon and Mathews Leon , "SQL a complete reference".