International Journal of Computer Applications in Engineering Sciences
[VOL I, ISSUE III, SEPTEMBER 2011] [ISSN: 2231-4946]

Remedial Measure in Cryptography

K. Nandhini

School of Computing, Sastra University, Thanjavur, Tamil Nadu

nandhinik7@gmail.com

***Abstract*— Cryptography is one the most important areas of the computer networks. Encryption and Decryption allows an application to secure its data from being accessed by hackers. This paper presents a new proposed solution in RSA (Rivest, Shamir and Adleman). Many of its characteristics (applications domain, performance and implementation structure) are similar to those of common RSA algorithm. These proposed features are expected to provide high security level with enhancement in throughput. The aim of this paper work is to track the hacker from a website and to block the hackers host address. The highlighting feature of this new algorithm is secure and safe transfer of data from sender to receiver. This algorithm is a panacea for all the cons present in data. This paper titled "Remedial Measure in cryptography" deals with sending of authenticated information from one person to another in safe and secure manner. For additional security water marking can be done. RSA algorithm is used to encrypt the plain text into encrypted format and similarly decrypt the data so that hacking can be minimized.**

***Keywords*—RSA Algorithm, Encryption, Decryption, Hacker, Security**

I. INTRODUCTION

The security of sensitive information transmitted via the Internet has been the focus of modern cryptographist's attentions. Many of them require that their data be secured from unwelcome users. Different types of applications require specialized security levels. Security is the primary concern of all those people who deal with activities, which involve protection of risk.

A network is a series of individual elements transmitting and receiving various data. Whenever sensitive or confidential information is transmitted, there is the possibility of an unauthorized third party "eavesdropping" on a transmission and learning the contents of the sensitive message.

This possibility is unacceptable in many scenarios. Cryptography is the process of translating a message into a form which is unreadable to everyone except the intended recipient. This is typically done with the use of keys. A cryptographic key is roughly equivalent to the concept of a physical key which can unlock a lock. Many locks are made with many different keys, but only the correct key can unlock the correct lock. In cryptography, keys are used to encrypt a message into a format which would appear as unreadable random information to an unauthorized third party. Cryptography, then, is a required element of security for any sensitive communications. Cryptography is defined as the conversion of the given plain text to encrypted format using the encryption algorithm and converted back to decrypted format using decryption algorithm.

In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI). In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key. See public key infrastructure (PKI) for more information. The above mentioned algorithm has been broadly classified into 3. They are block cipher, stream cipher and hash algorithm where block cipher converts one symbol and stream cipher converts a group of symbols.

The rest of this article is organized as follows: section 2 deals about the existing systems, section 3 deals about proposed work, section 4 deals about application work environment. Section 5 deals with future enhancements. Finally we make a conclusion in section 6.0

II. EXISTING SYSTEM

Nowadays, the information security has achieved a great importance, both when information is sent through a non-secure network (as the Internet) and when data are stored in massive storage devices. For this reason many algorithms are developed for encryption and decryption which provides high security. All these algorithms are kept open to the public and the secrecy of the algorithm lies entirely in the key. This paper stands different that

the development of algorithm addresses the user needs in specific, there by more flexible.

Each algorithm has certain advantages such as password hashing, encryption speed, available to all users, security and many more. Though it has number of advantages it is limited to certain factors such as the above mentioned disadvantages. The structure of most algorithms is based on the Fiestel network structure. Each algorithm was developed by different person in different year with varying key size and block length. The major categories of keys used are public and private key.

A. Encrypting Methods

1. Block Cipher: A block cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. The main alternative method, used much less frequently, is called the stream cipher. So that identical blocks of text do not get encrypted the same way in a message (which might make it easier to decipher the cipher text), it is common to apply the cipher text from the previous encrypted block to the next block in a sequence. So that identical messages encrypted on the same day do not produce identical cipher text, an initialization vector derived from a random number generator is combined with the text in the first block and the key. This ensures that all subsequent blocks result in cipher text that doesn't match that of the first encrypted form.

2. Stream Cipher: A stream cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. This method is not much used in modern cryptography. The main alternative method is the block cipher in which a key and algorithm are applied to blocks of data rather than individual bits in a stream.

3. Hash Algorithm: A hash algorithm is a function that takes a string and converts it to a numeric code. It's used in cryptography, fast data lookup and error correction codes. The algorithm is devised so that the range of values is reasonably spread and the chances of collisions (where two strings have the same hash value) is minimized. In cryptography, hashes of a password can be sent to a server and compared against the stored hash values there. This prevents the password being intercepted in plain text. Comparison of all algorithms is done in all round manner on the basis of its name, key size, block length and structure. The following are the comparison of the various algorithms which is shown in the below tabular column.

The above mentioned are the various kinds of encrypting methods.

TABLE I
STUDY OF VARIOUS ALGORITHMS

Algorithm Name	**Key Size (bits)**	**Block Length in Bits**	**Structure**
Blow Fish	128	64	Feistel network
Cast	40 to 128	64	Feistel network
Deal	128,192 or 256	128	Nested feistel structure
Triple Des	168	64	Feistel Network
Feal	64 and 128	64	Fiestel Network
Gost	256	64	Fiestel Network
Idea	64	64	Substituted Permutation Network
Loki	64	64	Fiestel Network
Misty	128	64	Nested fiestel structure
Rc5	0-2040	32,64,128	Feistel Structure
Safer	40,64,128	64	Substitution Permutation Network
Serpent	128,192,256	128	Substitution Permutation Network
Square	128	128	Substitution Permutation Network
Aes	128,192,256	128	Substitution Permutation Network
Mac Guffin	128	64	Unbalanced Feistel Structure
Mars	128, 192 or 256	128	Feistel Structure
Rc2	8-128 bits but default of 64 bit	64	Feistel Structure
Rc6	128, 196 or 256	128	Feistel Structure
Rijndael	128, 196 or 256	128	Substitution Permutation Network
Two Fish	128,192 or 256	128	Feistel network

B. Limitations of the Existing System

The existing system is concerned with the problem of private communication between sender and receiver. A number of ciphers exist which solve this problem more or less satisfactorily. One common factor behind these ciphers is the use of certain secret keys. With the advent of commercial data networks, there is a need for many pairs of users to communicate in privacy. The classical method of distributing secret keys (over a secure channel) to each user pair becomes very expensive and alternative means have to be explored. Some of the major limitations are (i) Authenticated information is being hacked, (ii) the algorithm used for encryption and decryption are easily prone to attack and (iii) Time delay. To overcome all these problems we are going for the same algorithm along with a code generator and a program for tracking the hacker.

III. PROPOSED WORK

This proposed work "Remedial Measure In cryptography" deals with sending of authenticated information from one person to another in safe and secure manner. Here RSA algorithm is used for encrypting the plain text into encrypted format. RSA algorithm is chosen such that hacking can be minimized.

This proposed work describes a method which does not require prior exchange of secret keys for private communication over a public network. Instead this system gives more security to the authenticated information and tracks hackers.

This work provides easy access to the users and helpful in the user interface. This is done by using an algorithm which does not allow all users to view the contents of the authenticated information. The information that is sent from the sender to receiver is sent in a safe and secure manner especially it is best suited in case of military. It also allows tracking of the hacker and his/her exact geographical location.

The resources needed for developing this works are Windows xp operating system, and ASP.NET as programming languages, Internet Information Server for Web Server, SQL for Web database and it is carried out with the help of HTML. TCP/IP is used for providing communication between the client and server. The Transmission Control Protocol (TCP) is often simply referred to as TCP/IP. Using TCP, client can create connections to the server, over which they exchange streams of data using Stream Sockets. The protocol is used because it, guarantees reliable and in-order delivery of data from sender to receiver. In our project the client first connects to the server using TCP/IP.

A. Modules

*1. Sender***:** This module consists of information which helps in sending information from sender to receiver. The data that is in plain text form is converted to encrypted format which is then sent to receiver.

*2. Tracking of the Hacker***:** It is used for safe transfer of data, when unauthorized persons hacks the information. It indicates the area of stay of the hacker which will be useful for persons in safety department like police and customs to trace the hacker.

*3. Code Generator***:** This seems to be the third module in our project. This program is in such a way that it will generate a new code every time we encrypt such that all can't access the data other than the authenticated person. This has an additional feature of generating the security code which has to be fed for converting the encrypted message to get the decrypted format. Also if incorrect security code is entered it will not allow the person to proceed as it will lock.

*4. Receiver***:** The last module being the receiver's module receives the encrypted format and decrypts the data sent by the sender and sends back an acknowledgement. If the hacker tries to hack the acknowledgement the sender will be able to know his fraudulence.

If additional security is required watermarking technique can be used.

B. RSA Algorithm

RSA algorithm is a typical representative and probably the most popular asymmetric cryptographic algorithm. The RSA algorithm is widely used in emerging e-commerce and e-business systems for creating "digital signature" and "digital envelope". The algorithm was developed by RON RIVEST, ADI SHAMIR, and LEN ADLEMAN at MIT and published by 1978 since then this scheme was widely implemented general purpose approach to public-key encryption. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.

1. Key Generation: Steps are as follows.

- Generate two large prime numbers, *p* and *q*
- Let n = pq
- Let m = (p-1)(q-1)
- Choose a small number *e*, coprime to *m*
- Find d, such that de % m = 1

Publish e and n as the public key. Keep d and n as the secret key.

Its security comes from the computational difficulty of factoring large numbers. To be secure, very large

numbers must be used for *p* and *q* - 100 decimal digits at the very least.

2. Theorem: It is given below

$C = M^e \pmod n$

$M' = C^d \pmod n$

$M' = M \pmod n$

where (d, e, n) is a valid RSA key, with n = pq

and $0 < M <$ minimum(p,q)

Proof is as follows where we first combine the two exponentiations.

$M' = M^{ed} \pmod n$

d and e are generated so that

$de = k(p-1)(q-1) + 1$

$M' = M^{k(p-1)(q-1)+1} \pmod n$

$M' = M.M^{k(p-1)(q-1)} \pmod n$ *****

consider $X = M^{k(p-1)(q-1)} \pmod p$

$X = \left(M^{(p-1)}\right)^{k(q-1)} \pmod p$ the Fermat/Euler theorem tells us that

$M^{(p-1)} = 1 \pmod p$

$X = 1^{k(q-1)} \pmod p$

$X = 1 \pmod p$ by a similar route,

$X = 1 \pmod q$ as p and q are distinct primes, we can combine these with the Chinese remainder theorem

$X = 1 \pmod{pq}$

$M^{k(p-1)(q-1)} = 1 \pmod n$ finally, we substitute this back into the equation marked *****

$M' = M.1 \pmod n$

$M' = M \pmod n$

Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key") cannot understand the content of the text. Encryption has long been the domain of spies and diplomats, but recently it has moved into the public eye with the concern of the protection of electronic transmissions and digitally stored data. Standard encryption methods usually have two basic flaws: (1) A secure channel must be established at some point so that the sender may exchange the decoding key with the receiver and (2) There is no guarantee who sent a given message. Public key encryption has rapidly grown in popularity (and controversy, see, for example, discussions of the Clipper chip on the archives given below) because it offers a very secure encryption method that addresses these concerns.

In a classic cryptosystem in order to make sure that nobody, except the intended recipient, deciphers the message, the people involved had to strive to keep the key secret. In a public-key cryptosystem, the public key cryptography solves one of the most vexing problems of all prior cryptography: the necessity of establishing a secure channel for the exchange of the key. The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is currently one of the favorite public key encryption methods.

C. Features

Some of the main features are (a) Remedial Measure In cryptography uses an algorithm for encryption and decryption which does not allow users other than the receiver to view the contents of the information, (b) The program written for code generation does not allow the user to view the contents in ease, (c) The main purpose of this code generation program is for safe and secure transfer of information, (d)For the purpose of tracking of hacker we use a program and this program facilitates for tracking the hacker if any (e)the incorrect security code cannot be entered more than thrice and (f) The back bone of our project is the tracing of the hacker and finding his exact geographical location.

The RSA algorithm is the most popular public-key cryptosystem. The algorithm is widely used for creating "digital signature" and "digital envelope" that can provide privacy and authentication. Both privacy and authentication are the basic security functions of the internet applications. The Security of RSA is based on its key large enough. If the key is large, then it will take more computation cost. How to implement RSA efficiently on the general web application is an important issue in the closed network (intranet). This paper proposes a method to implement RSA on web applications.

IV. APPLICATION WORK ENVIRONMENT

This paper has been developed in an application using the programming language ASP.NET. It is a web application framework developed and marketed by Microsoft to allow programmers to build dynamic web sites, web applications and web services. This application allows the user to introduce text, to manage files, to compute the sub-keys from a pass phrase introduced by the user, to configure and communicate with the FPGA, and to perform functions of encryption and decryption.

Here when the plain text is getting encrypted by clicking the encrypt button a code is automatically generated which is done to prevent the data being hacked by eavesdroppers. Once the mail is sent to receiver, the sender receives a mail which gives information regarding the secret code generated. This secret code can be intimated to the receiver either by fax or telephone.

The receiver receives a mail which has a link and on clicking which, directs us to the abstract page which has fake data. This data is also provided to deviate eavesdropper if any. And on going to next page is the security code form. If he is a true receiver he would have

already got the secret code from sender, so he will use the code and view the decrypted format.

If he/she is a hacker he/she will not know the secret code, for him/her we have provided a randomly generating code which is alpha numeric and this is also fake. We have provided this so that the hacker with the help of the random number may try the security code. Once a wrong security code is entered incorrect button is enabled. And immediately a mail is sent to the sender that the data is being hacked and the IP address of that system is displayed. But this is possible only in intranet and by hosting a web server we can track hackers all over the globe which is a future enhancement of this project.

On one hand, when an encryption is performed, the application takes the text contained in the edition window and processes the data with the selected hardware implementation, storing the result in a file that will be solicited to the user. On the other hand, the decryption is made on a file that will be solicited to the user and the result will be shown in the edition window. Furthermore, in both cases, an information message with regard to the success of the operation, the implementation used and its performance will be shown.

V. Future Enhancements

Cryptography provides many methods and techniques for secure communication. Currently there are many industry standard encryption/decryption algorithms including RSA/AES, Robust Security Network (RSN), blowfish and so forth. However they are fairly complex and requires a lot of time to comprehend and implement them. But here we have used an existing algorithm and the drawback in it is rectified. However it is only suitable for applications that do not expose the inputs and the encrypted form of the inputs to the public.

VI. Conclusion

Nowadays transmitting data securely over a network is gaining more and more importance and is triggering a need for an improvement in performance of the encryption algorithms. Hence the proposed solution for the encryption and decryption is based on the RSA algorithm which is implemented in this paper work. The final output of this work is to trace the hacker and to crash the hacker's host address. The idea was to demonstrate the possibility of obtaining a very high security level for the data which is transmitted between sender and receiver. The new solutions presented have the same security of the previous scheme with some additional features. The implementation of this concept brings the revolution in Banking and the military domain. The proposed method is secure, compact and simple.

This paper proposes an efficient method to implement the RSA algorithm on the design implementation. This proposed work integrates the existing RSA algorithm with the given functions. The result shows that the RSA algorithm can be performed efficiently on the web services. In other word, the web applications can perform the public key cryptography technologies efficiently if they include this proposed RSA algorithm.

References

[1] C.Parthasarathy,S.K. Srivasta," Electronic copyright Management System", Journal of Information Technology, 8(3), 67-73,2009.

[2] Sining Liu, Brian King," A CRT-RSA algorithm secure against hardware fault attacks", 2009.

[3] Remlunn Hwang' Feng-Fu Su' LOangShing Huang Jen-Kang Peng," Implementing the RSA Algorithm on the TI TMS32OC55x Family", 2009.

[4] Kalaichelvi.v, Dr.RM. Chandrasekaran,"FSP Algorithm for Encryption and Decryption", 2008

[5] Milan MarkoviC, Goran d ordevic, Tomislav UnkaSevit," On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length", 2003.

[6] G. Catalini, F. Chiaraluce, L. Ciccarelli, E. Gamhi, P. Pierleoni, M. Reginelli," Modified Twofish Algorithm For Increasing Security And Efficiency In The Encryption Of Video Signals" ,2003.

[7] Fahad Bin Nafey, OBV Ramanaiah," A Study on Rijndael Algorithm for Providing Confidentiality to Mobile Devices", 2009.

[8] Brian Cody, Justin Madigan, Spencer MacDonald, Kenneth W. Hsu, "High Speed SOC Design for Blowfish Cryptographic Algorithm", 2007.

[9] Haixiang Xu, Xuezhi Xi, Liyan Guo, Wei Chen, Guanglin Huang, "A Novel Algorithm of Moving Cast Shadow Suppression", 2006.

[10] Janaka Deepakumara, Howard M. Heys and R. Venkatesan, "FPGA Implementation of MD5 Hash Algorithm", 2009.

[11] K.M.S Soyjaudah, M.A Hosany, A. Jamaloodeen," Design and Implementation of Rijndael algorithm for GSM Encryption", 2004.

[12] T.Korkishko, A. Melnyk," Cryptographic processor architectures for DES algorithm", 1999.