ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Symmetric Private Key Encryption and Decryption based on Matrix

S.Ramani[1], P. Swarnalatha[2], L., Ramanathan[3], Srinivas Koppu[4], Madhusudhana Rao[5]

Assistant Professor (Sr), School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India[1]

Associate Professor, School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India[2]

Assistant Professor (SG), School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India[3]

Assistant Professor (Sr), School of Information Technology, VIT University, Vellore, Tamilnadu, India[4]

Lecturer, Dept. of Information Technology, Higher college of Technology, Muscat, Oman[5]

ABSTRACT: A breach in network security could cost your company a great deal in lost productivity, lost data, and loss of confidence among customers, partners, and employees. But these damages are preventable. You just need a solid security strategy and a well-planned implementation. With the explosion of the public Internet and e-commerce, private computers and computer networks are increasingly vulnerable to damaging attacks. In this paper we have proposed an effective method to achieve the top-level security through Matrix Based Private Key Cryptosystem and implemented the same using 'C' programming. We have used a 32 byte symmetric keyword for encryption. The 32 byte symmetric keyword is used at three levels to perform encryption and decryption. The main advantage is that we have rearranged the encrypted data in an asymmetric way so that it is tough for cryptanalyst to identify the data.

KEYWORDS: Network Security, Asymmetric, Symmetric, Private Key Cryptosystem, Matrix.

I.INTRODUCTION

Cryptography is the art of hiding data, transmitting it and retrieving it again at the receiver side in the original form so that no intruder gets the transmitted information. The former is called the **encryption** and the latter is called the decryption. The paper deals with such an algorithm for a secret transmission of data. Encryption plays a major role in maintaining security. In this paper, we have proposed an effective method to achieve the top-level security through private key encryption and decryption.The reverse process of the encryption is done in decryption so as to get back the original text message.

Need for network security:

- Explosive growth in the use of computer systems and their interconnections via communication networks.
- Maturing of the disciplines of cryptography and network security
- The last two decades have seen huge change in requirements of information security within organizations.

With the advent of computer networks there has arisen a need for network security which is primarily concerned with protecting information during transmission.

Applications of Information Security:
It includes Communication Security, Data distribution, digital cash, Electronic mail, Electronic voting. In communication, it is the security that matters more in real time electronic links, local and wide area networks link encryption, cellular telephony, faxes and emails. In data distribution it is conditional access software distribution information bulletin boards. In digital cash it is the creation electronic payments system thatreplaces paper money and is more flexible then credit cards. In electronic voting it is secure distributed computation, elections in shareholders meeting.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Security Services:

- **Confidentiality** to ensure that the information in a computer system and transmitted information are accessible only by authorized parties.
- **Authentication** very much needed to ensure that the origin of a message or electronic document is correctly identified, with an assurance that the identity which is not false.
- **Integrity** to ensure that only authorized parties is able to modify computer system assets, settings and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delayed or replaying of transmitted messages.
- **Non-repudiation** to ensure that neither the sender nor the receiver of a message is able to deny the transmission.
- **Access control** to ensure that access to the information may be controlled by or for the target system.
- **Availability** to ensure that the computer system assets are available to authorized parties when required.

Unfortunately there is no single security mechanism that can provide all of these security services.

II. RELATED TERMINOLOGIES

Authentication:
Authentication is the foundation technology for protecting networks, servers, client systems, data, and applications from improper disclosure, tampering, destruction, and other forms of interference. The essence of an authentication system is discovering and confirming the identity of a person, an organization, a device, or more generally, of any software process on the network. Users can be authenticated by something they know, something they have, or something they are.

The most common example of “something you know” is the traditional user ID and password combination. A common example of “something you have” is an access card that is swiped through a card reader. “Something you are” can be established with fingerprint readers, retinal scanners, facial recognition systems, and hand geometry analyser’s.

Cryptography:
There is one particular common element that underlines most of the security mechanism employed today, namely cryptographic techniques. Cryptographic or encryption like transformations of computer system information is the most common means of providing the security features.

Encryption and Decryption:
Data that is being transmitted has to be converted to an unreadable form using some algorithms. This modified data is then transmitted. The algorithm will be using some value of data on basis of which encoding is done. This value is called a key, which is passed to the recipient end through some secure means. On the end the data is decrypted using the key. For this the algorithm has to be corresponding ones at both the ends. Then a random key is generated and the data is encoded and transmitted. This system is called cipher system.

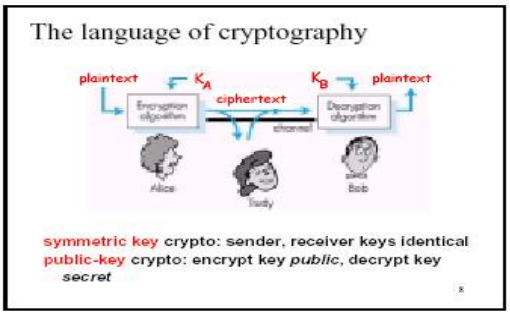

Fig.1 The language of cryptography

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, but the key that must be used with the algorithm to encrypt or decrypt the information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes. Encryption strength is often described in terms of the size of the keys used to perform the encryption: in general, longer keys provide stronger encryption. Key length is measured in bytes. There are two fundamental approaches to the application of encryption function:

(1) Link encryption
(2) End-to-end encryption

Link Encryption:

With this one, each vulnerable communications link is equipped on both ends with an encryption device. The advantage is that all traffic over all communications link is secured. The disadvantage is that for a large network, a large number of encryption devices are required. Also in packet-switched networks it is necessary to decrypt the message before entering a switch or router in order to read the address header. Thus the message is vulnerable at each switch or router.

End-To-End Encryption:

In this one, the encryption process is carried out at the two end systems. The host encrypts the data, which is then transmitted across the network to the destination where it is decrypted. On the face of it, it seems that end-to-end security relieves the end users of concerns over network and link security. However on packet-switched network it is necessary to transmit the packet header in the clear in order to support routing.

In order to achieve greater security both link and end-to-end encryption is needed. Placement of the encryption function at the transport layer provides end-to-end security for traffic within a fully integrated inter-network

STREAM CIPHER:They operate on streams of binary data. The key stream and the plain text are XORed byte by byte thus yielding a data stream that is quite unintelligible. Then the key stream and the cipher text are XORed to obtain the original plaintext. One should have very secure menus of transmitting the key stream. Once one has the key stream then it is child's play to decipher the cipher text.

BLOCK CIPHER:Instead of encrypting each byte blocks of data are encrypted. The size of the block and key can be exchanged beforehand. The drawback is that by finding patterns in the text can give code breaker an advantage of breaking the code.

SYMMETRIC KEY ENCRYPTION:

Only sender and receiver know the key ("secret key" encryption). In symmetric-key encryption, a private key is an encryption/decryption key known only to the party or parties that exchange secret messages. Implementations of symmetric-key encryption can be highly efficient, avoiding any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with onesymmetric key cannot be decrypted with any other symmetric key. Symmetric-key encryption is effective only if the two parties involved keep the symmetric key secret. If anyone else discovers the key, it affects both confidentiality and authentication.

e-key = d-key (i.e. symmetric)

ASYMMETRIC KEY ENCRYPTION:

Asymmetric encryption (also called "public key encryption") involves a pair of keys – a public key and a private key - associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key.
e-key! = d-key
e-key is called the "public key"
d-key is called the "private key"

III.IMPLEMENTATION

In this paper we have proposed a method to do **Private Key Encryption and Decryption** using C. The 32 byte symmetric keyword is used at three levels to perform encryption and decryption.Here we have implemented a 32-byte private key encryption. The sender and receiver only know the keyword. The key is got from the user and is store as **key1.** An internal second key is generated by rotates the key1 through right.

LEVEL1:

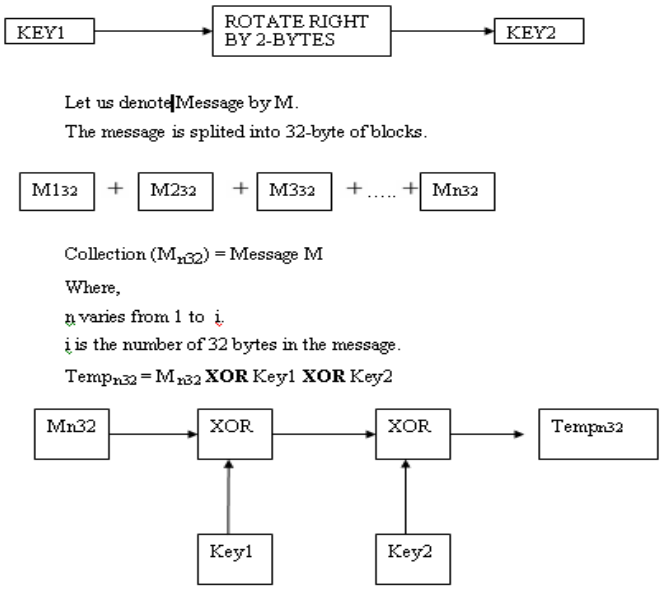

Fig.2Private Key encryption using 32 byte

Key1 is the 32-byte keyword.
Key2= Rotate (Key1) through right by 2-byte

LEVEL2:

Then each $temp_{n32}$ is arranged as a 4 X 8 matrixes and then each be rearranged in an asymmetric way so as to improve security.

Matrix Arrangement:

A0	A1	A2	A3	A4	A5	A6	A7
A8	A9	A10	A11	A12	A13	A14	A15
A16	A17	A18	A19	A20	A21	A22	A23
A24	A25	A26	A27	A28	A29	A30	A31

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

The flow of the matric rearrangement is shown in the below figure. It initially starts from right side from A_7.

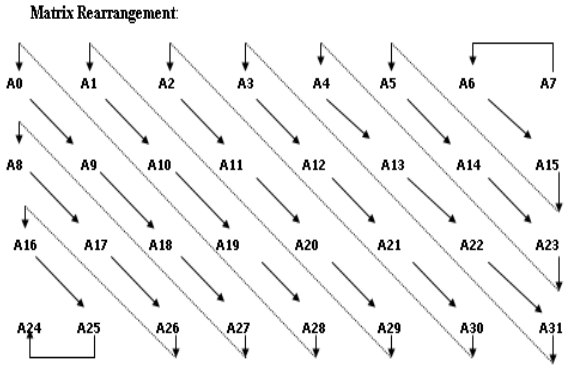

Fig.3 Matrix Rearrangement flow

Using the flow shown above the below given matrix is represented.

Rearranged Matrix:

A7 A6 A15 A5 A14 A23 A4 A13

A22 A31 A3 A12 A21 A30A2 A11

A20 A29 A1 A10 A19 A28 A0 A9

A18 A27 A8 A17 A26 A16 A25 A24

If the data is not of 32-byte length then reverse the block. Let the rearranged data is stored as Mat_{n32}.

LEVEL3:

The each Mat_{n32} is broken into LHS_{n16} and RHS_{n16}

$RHS_{n16} = RHS_{n16}$ ADD $Key1_{16}$ **(if n=1)**

$RHS_{n16} = RHS_{n16}$ ADD $Key1_{16}$ ADD $RHS_{(n-1)32}$ **(if n≠1)**

$LHS_{n16} = LHS_{n16}$ XOR $Key1_{16}$

$RHS_{n16} = RHS_{n16}$ XOR LHS_{n32} ----------(1)

For the end of file if Mat_{n32} has less than or equal to 16 bytes, then take the whole as RHS_{n16}.
$LHS_{n16} = LHS_{n16}$ XOR $Key1_{16}$ ----------(2)

The RHS_{n16} (1) and LHS_{n16} (2) together forms the encrypted data.

ALGORITHM

- Here encryption is done using a 32-byte keyword to encrypt text files using Turbo C.
- The program gets a 32-byte keyword from the user to encrypt the text message (Key1 [32]).
- If the user doesn't enter a 32-byte (Key1 [32]) keyword the program itself allocates a default keyword.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

- An internal generation of the second key (Key2 [32]) is done by rotating the keyword towards right by using _rotr ( ) function
- Encryption is done in three levels.
- The text message is separated into number of 32-byte.
- Each 32-byte is XOR with the two keys (Key1 & Key2).
- Then each 32byte data is arranged in an asymmetric way as shown below using matrix_4x8 ( ) function.
- The first 16 are taken as the LHS (x1 [16]) and the next 16 are taken as the RHS (xr [16]) of the block.
- The RHS (xr [16]) is then ADDED with the first 16 bytes of the key entered and is stored in the name add [16] array.
- Then the LHS is XOR (x1 [16]) with the first 16 bytes of the key and then RHS (xr [16]) part with the resultant LHS (x1 [16]).
- If the final part of the message is less than or equal to 16-bytes (Key1 [16]) then consider it as the LHS (x1 [16]) and perform XOR with the (Key [16]).
- Finally all the resultant RHS (x1 [16]) and LHS (xr [16]) collectively give the encrypted data.
- Then the reverse process of the encryption is done so as to get back the original text message.

IV. RESULT AND DISCUSSION

The results that are obtained are shown below. Fig.4 represents the encryption technique using 32 byte. We give a text file as the input and the encryption is done. Key is used to perform the encryption.

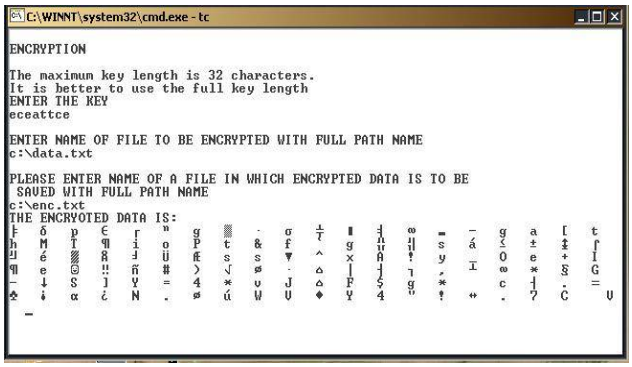

Fig.4 Encryption

The results that are obtained are shown below. Fig.5 represents the decryption technique using 32 byte. We give a text file as the input and the encryption is done. Key is used to perform the decryption. Key is common in both the case.

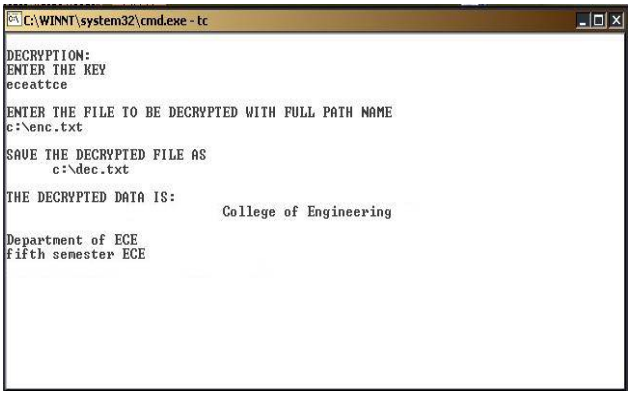

Fig.5 Decryption

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Advantages

- The advantage of this method is that we use Asymmetric arrangement of the data. Each 32-byte data is first arranged in 4 X 8 Matrix arrangements and then rearranged symmetrically. This would increase the security of the encryption.
- As this is implementation is done using Turbo C that can be even executed in DOS based systems also. This program does not depend on the operating system and does require any GUI and does use any graphics so that it saves memory and reduces the cost.
- The 32-byte keyword entered is also encrypted so that it can be transferred over any network with much security through Network Interface Card (future project).
- The encryption algorithm does not increase the memory as only the RHS (xr [16]) and the final LHS (x1 [16]) is written as the encrypted data.
- Using this Encryption technique, we can encrypt all text files, MPG files, DAT files, JPG files and MP3 files

V. CONCLUSION

This technique is mainly proposed as an add-on to the existing encryption algorithms. The advantage of this technique is that it uses the complex asymmetric 4 X 8 matrix rearrangement of data, which is very difficult to break. It would be a tough job for a cryptanalyst to decipher the original data from the encrypted data.

REFERENCES

[1] I. Mantin, "Predicting and Distinguishing Attacks on RC4 Keystream Generator", Vol. 3494, pp. 491-506, Springer, 2005.
[2] G. Gong, K. C. Gupta, M. Hell andY. Nawaz, "Towards a General RC4-like Keystream Generator,SKLOISConference on Information Security and Cryptology (CICS05), Springer, 2006.
[3] Y. Nawaz and G. Gong, WG, " A family of stream ciphers with designed randomness properties",Information Sciences, Vol. 178, No. 7, pp. 1903-1916, April 2008.
[4] H. Mohan and R. Raji,"Performance Analysis of AES and MARS Encryption Algorithms", International Journal of Computer Science Issues (IJCSI), Vol. 8, No.4. April 2011.
[5] J. Nechvatal, "Report on the Development of the Advanced Encryption Standard (AES)", National Institute of Standards and Technology, October, 2000.
[6] B.D.C.N.Prasad, P E S N Krishna Prasad, "A Performance Study on AES algorithms", International Journal of ComputerScience and Information Security, Vol. 8, No. 6,pp.128-132, September 2010.
[7]S. Tao, W. Ruli, and Y. Yixun, "Clock-Controlled Chaotic Key-Stream Generators", Institution of Engineering and Technology Electronics Letters, Vol. 34, pp. 1932-1934, 1998.
[8] L. Chang-Doo, C. Bong-Jun, P. Kyoo- Seok , "Design and evaluation of a block encryption Algorithmusing dynamic-key mechanism", Future Generation Computer Systems , Vol.20, pp. 327–338, 2004
[9] Rajan.S.Jamgekar, GeetaShantanu Joshi, "File Encryption and Decryption Using Secure RSA", InternationalJournal of Emerging Science and Engineering (IJESE), Vol.1, No.4, February 2013.
[10] AkankshaMathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJSCE), Vol. 4 No. 09, Sep 2012.
[11] Monisha Sharma, ChandrashekharKamargaonkar, Amit Gupta, "A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern", International Journal of Engineering Research & Technology (IJERT), Vol. 1, No.7, Sep 2012.