HYBRID CRYPTOGRAPHIC TECHNIQUE USING RSA ALGORITHM AND SCHEDULING CONCEPTS

Meenakshi Shankar[1]and Akshaya.P[2]

[1]Department of Electrical and Electronics Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, India
[2]Department of Information Technology,Sri Venkateswara College of Engineering, Sriperumbudur, India

ABSTRACT

The RSA algorithm is one of the most commonly used efficient cryptographic algorithms. It provides the required amount of confidentiality, data integrity and privacy. This paper integrates the RSA Algorithm with round-robin priority scheduling scheme in order to extend the level of security and reduce the effectiveness of intrusion. It aims at obtaining minimal overhead, increased throughput and privacy. In this method the user uses the RSA algorithm and generates the encrypted messages that are sorted priority-wise and then sent. The receiver, on receiving the messages decrypts them using the RSA algorithm according to their priority. This method reduces the risk of man-in-middle attacks and timing attacks as the encrypted and decrypted messages are further jumbled based on their priority. It also reduces the power monitoring attack risk if a very small amount of information is exchanged. It raises the bar on the standards of information security, ensuring more efficiency.

KEYWORDS

RSA Algorithm, Cryptography, Priority Scheduling, Encryption & Decryption, Information Security.

1. INTRODUCTION

Message passing in a confidential manner is the key feature of any successful cryptographic technique. Cryptography plays a major role in data protection and authenticity in applications running in a system connected to a network. It allows people to communicate or transfer data electronically without worries of deceit and deception (confidentially)in addition to ensuring the integrity of the message and authenticity of the sender. There is a need for cryptographic algorithms because of the exponential increase in electronic transfer of data in several fields such as, e-commerce, banking, finance, etc. [1].

Curiosity is one of the most common human traits, matched by the wish to conceal private information. People often resort to information hiding to pass messages securely, sometimes deliberately including misleading information. Steganography, a mechanism for hiding information in apparently innocent pictures, may be used on its own or with other methods [2].
Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient [3]. Cryptanalysis is the science of analysing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of

DOI : 10.5121/ijnsa.2014.6604

mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis [4].
Cryptography is broadly divided into two categories depending upon the Key; which is defined as the rules used to convert an original text into encrypted text: - Symmetric Key Cryptography and Asymmetric Key Cryptography [5]. In symmetric key cryptography, the encryption and decryption are done using the same key (symmetric key). In asymmetric cryptography, encryption and decryption are done using different keys.

Encryption fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process. These processes depend on particular algorithms, known as ciphers [6].

A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, like a password. However the functionality of a key lies in its usefulness in determining the mapping of the plain text to the cipher text.

This paper proposes the implementation of RSA algorithm with encryption according to priority and cypher text transfer in parts, alternatively using round-robin technique.

2. CRYPTOGRAPHY

Cryptographic algorithms are classified based on the number of keys used as

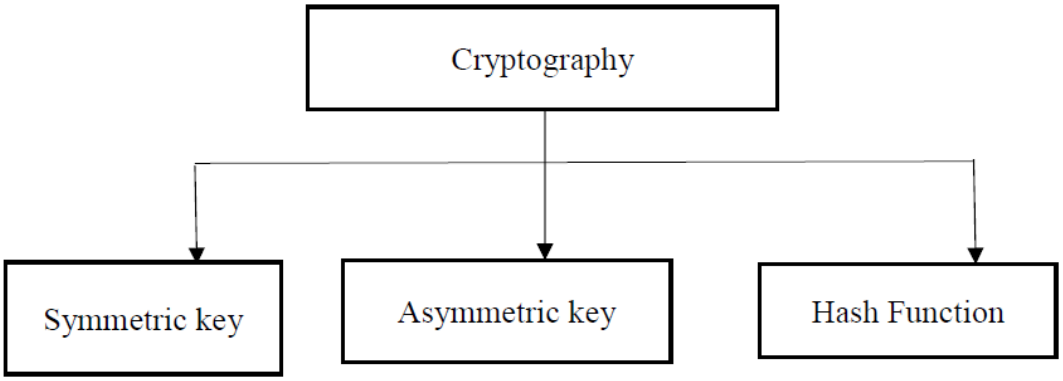


Figure 2. Types of Cryptography

2.1. Secret-Key Cryptography

In secret key crypto there is only one key. It is used for both encryption and decryption. A key refers to any code that yields plain text when applied to cypher text.This key is shared by both sender and receiver. If the key is disclosed the secrecy of the information is compromised. The key is known to both the sender and the receiver, hence does not protect the sender from the receiver forging a message & claiming is sent by sender. Lengthy keys are used to increase the security and to decrease the chances of identifying the key through brute force. It is relatively fast as it uses the same key for encryption and decryption [8]. However, more damage if can occur if the key is compromised. When someone gets their hands on a symmetric key, they can decrypt everything that was encrypted with that key. Since symmetric encryption is used for two-way communication, both sender and receiver end data gets compromised.

2.2. Public-Key Cryptography

Public-key/ two-key/ asymmetric cryptography involves the use of two keys: a public-key, which may be known to everyone, used to encrypt messages and verify signatures and a private-key, known only to the recipient, used to decrypt messages and sign (create signatures). It is called asymmetric cryptography because the key used to encrypt messages or verify signatures cannot be used to decrypt messages or create signatures [8]. Asymmetric key cyphers increase the security and convenience as private keys never have to be transmitted or revealed to anyone. Public key encryption is slow compared to symmetric encryption. It is difficult to encrypt bulk messages. Interference by a third party results in a type of attack called man-in-middle attack. Damages due loss of private key are mostly irreparable.

Digital signature is a mechanism by which a message is authenticated, proving that amessage is definitely coming from a given sender, much like a signature on a paper document.

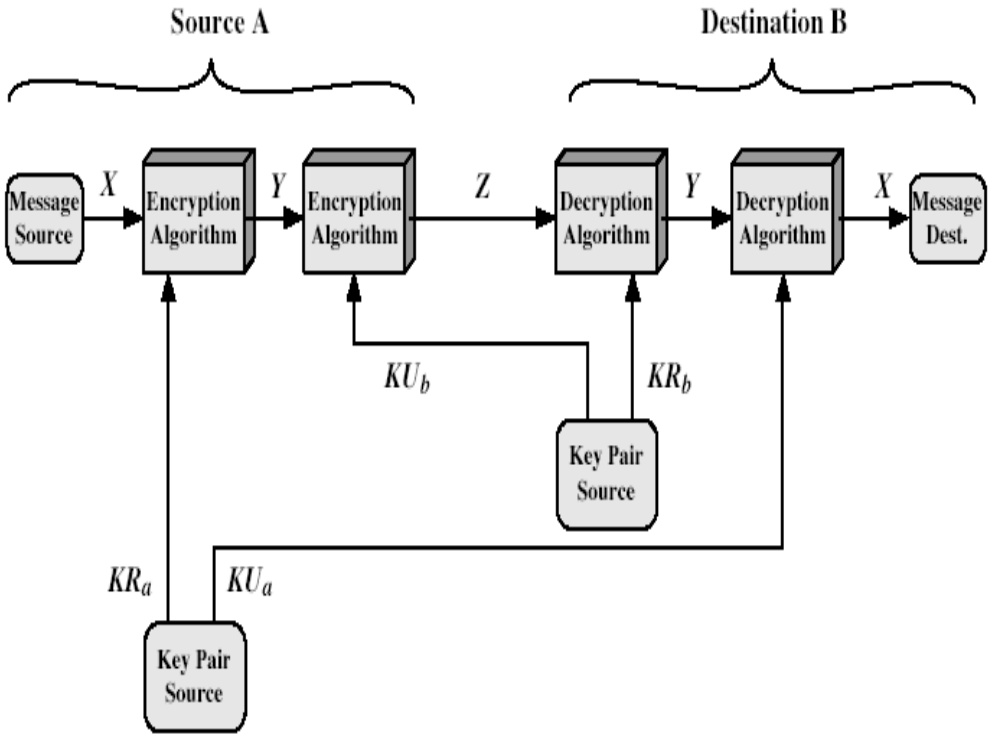


Figure 2. Public Key Cryptosystems: Secrecy and Authentication

2.3. Hash Function

The Hash Function uses a mathematical transformation to irreversibly "encrypt" information. This algorithm does not use keys for encryption and decryption of data. It rather uses a fixed-length hash value which is computed based on some plaintext that makes it impossible for either the contents or the length of the plaintext to be recovered. These algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords to provide some amount of integrity to a file [9].

2.4. Need for Cryptography

Cryptography provides privacy and information security. In this era where information has a lot of importance such techniques play an important role in several fields.Protecting access to information for reasons of security is still a major reason for using cryptography. However, it is also increasingly used for authorization or identification, authentication and non-repudiation.The identity of e-mail and web users is easy to conceal or forge and secure authentication can give those interacting remotely confidence that they're dealing with the right person and that a message hasn't been adulterated.

In commercial situations, non-repudiation is an important concept that helps in maintaining the stance of the agreeing parties under all circumstances in case of any agreement. Digital signatures and digital timestamps are used in such situations, often in conjunction with other mechanisms such as message digests and digital certificates.

The range of uses for cryptography and related techniques is considerable and growing steadily. Passwords are common but the protection they offer is often illusory, perhaps because security policies within many organizations aren't well thought out and their use causes more problems and inconvenience than seems worth it.

In many cases where passwords are used, for example in protecting word processed documents, the ciphers used are extremely lightweight and can be attacked without difficulty using one of a range of freely available cracking programs [2] [6] [7].

3. RSA CRYPTOGRAPHIC ALGORITHM

RSA stands forRon Rivest, Adi Shamir and Leonard Adlemanat MIT who first proposed a description of the algorithm publically in 1977. It is a form of asymmetric cryptography.A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message[10].

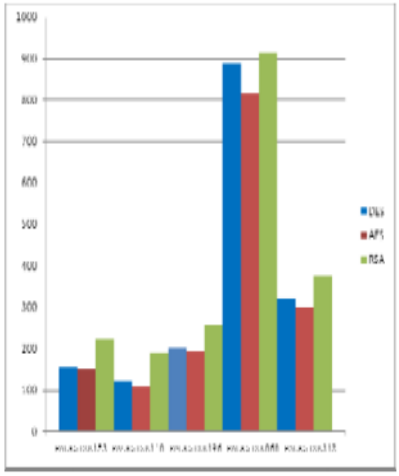
According to the patent issued by theDerwent World Patents Index, RSA algorithm is described as: The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to cipher text at the encoding terminal by encoding the message as a number M in a predetermined set. That number is then raised to a first predetermined power (associated with the intended receiver) and finally computed. The remainder or residue, C, is... computed when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver).

International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

S.NO	Algor	Pack Size (KB)	Encrypt Time (Sec)	Decrypt Time (Sec)	Buff Size
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	**DES**	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

algorithm show very minor difference in time taken for encryption and decryption process.

Figure 5. Comparative analysis of Buffer Size among DES, AES and RSA algorithm



By analyzing Figure 5 , it shows buffer size usages by AES, DES and RSA algorithm and noticed that RSA algorithm buffer size usages are highest for all sizes of document file.

Figure 3. Comparative analysis of RSA

A cryptographically strong random number generator, which has been properly seeded with adequate entropy, must be used to generate the primes p and q. An analysis comparing millions of public keys gathered from the Internet was carried out in early 2012 by Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung and Christophe Wachter. They were able to factor 0.2% of the keys using only Euclid's algorithm [11][12].

4. PRIORITY SCHEDULING

CPU Scheduling is the basis of multi programming operating system. By switching the CPU among processes, the operating system can make the computer more productive. Whenever the CPU becomes idle, the operating system must select one of the processes in the ready queue to be executed. This selection process is carried out by the Short-term Scheduler are CPU Scheduler. It selects from all the processes in memory that are ready to execute and allocate the CPU to one of them. The ready queue can be implemented using one of the scheduling algorithms

Scheduling is done in terms of priority in priority scheduling. Priorities are generally some fixed range of numbers. However there is no general agreement on whether the smallest number has the

highest or lowest priority. Some systems use low numbers to represent low priority; others use low numbers for high priority. This difference can lead to confusion.

Priority scheduling can be either preemptive or nonpreemptive. When a process arrives at the ready queue, its priority compared with the priority of the currently running process. A preemptive priority-scheduling algorithm will preempt the CPU if the priority of the newly arrived process is higher than the priority of the currently running process. A nonpreemptive priority-scheduling algorithm will simply put the new process at the head of the ready queue.

A major problem with priority-scheduling algorithms is indefinite blocking or starvation. A solution to this problem is aging. It is the technique of gradually increasing the priority of processes that wait in the system for a long time.

5. ROUND-ROBIN SCHEDULING

The round-robin scheduling algorithm is designed especially for time sharing systems. It is similar to First Come First Serve scheduling, but preemption is added to switch between processes. A small unit of time called a time quantum or time slice is defined. It is generally from 10 to 100 milliseconds. The ready queue is treated as a circular queue. The CPU scheduler goes around the ready queue, allocating the CPU to each process for a time interval of up to one time quantum.

To implement RR Scheduling the ready queue is kept as a FIFO queue of processes. New processes are added to the tail of the ready queue, sets a timer to interrupt after one time quantum and dispatches the process.

One of two things will then happen. The process may have a CPU burst of less than one quantum In that case, the process itself will release the CPU voluntarily. Otherwise, the timer will go off and will cause an interrupt in the operating system. A context switch will be executed and the process will be put at the tail of the ready queue[13].

6. METHODOLOGY

The RSA Algorithm is used to create a private- public key pair. It is a type of asymmetric key cryptography.

6.1. RSA Algorithm

The steps for implementation of RSA algorithm are given below

1. Get two integers, p and q from the user.
2. Check if p and q are prime. If prime, continue the process, else exit the code.
3.Calculate (p-1)*(q-1) and name it as $\phi(n)$.
4.Calculate n=p*q.
5.Get an input e to act as private key, under the condition that $1<e<\phi(n)$ and gcd(e, ϕ (n)) =1.
(gcd-greatest common divisor)
6.Compute the value of d such that $1 < d <\phi(n)$ and $e.d \equiv 1 \pmod{\phi(n)}$.

NOTE:
The public key is (n, e) and the private key is (n, d).
The values of p, q and $\phi(n)$ are private.

‘e’ is the public or encryption exponent.
‘d’ is the private or decryption exponent.

Encryption:

The cypher text C is found by the equation '$C = M^e \bmod n$' where M is the original message.

Decryption:

The message M can be found form the cypher text C by the equation '$M = C^d \bmod n$.

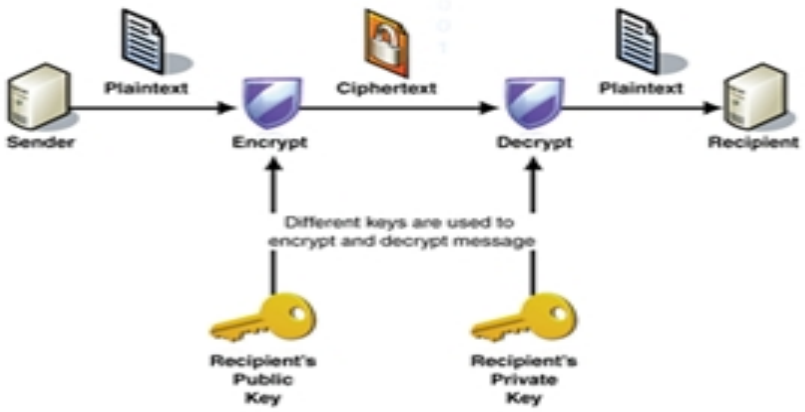


Figure 4. Communication using RSA

6.2. Procedure

This paper proposes the RSA algorithm with some variations in its implementation that will enhance the security of the information transfer. The proposed procedure is given below:

1. The input-prime numbers-(p,q) are obtained from the user.
2. n and ϕ(n) are calculated.
3.All the co-prime numbers from 1 to ϕ(n) are listed out and the user is allowed to choose 'e' from the given values, in addition to any data required for the normal implementation of the RSA algorithm.
4.The private key is obtained by calculating’d’.
5.The message that has to be encrypted is obtained from the user along with the priorities for various parts. The input message is split into low priority, medium priority and high priority parts by the user.
6.The messages are encrypted ($C = M^e \bmod n$) and sent to the receiver in parts using round-robin technique. The receiver decrypts the split messages and joins them using the proposed decryption algorithm which is essentially the reverse of the encryption algorithm and uses the RSA algorithm's decryption technique ($M=C^d \bmod n$), thus obtaining the message.

7. A software is proposed to be provided for the implementation of this technique. The back end is provided using java code

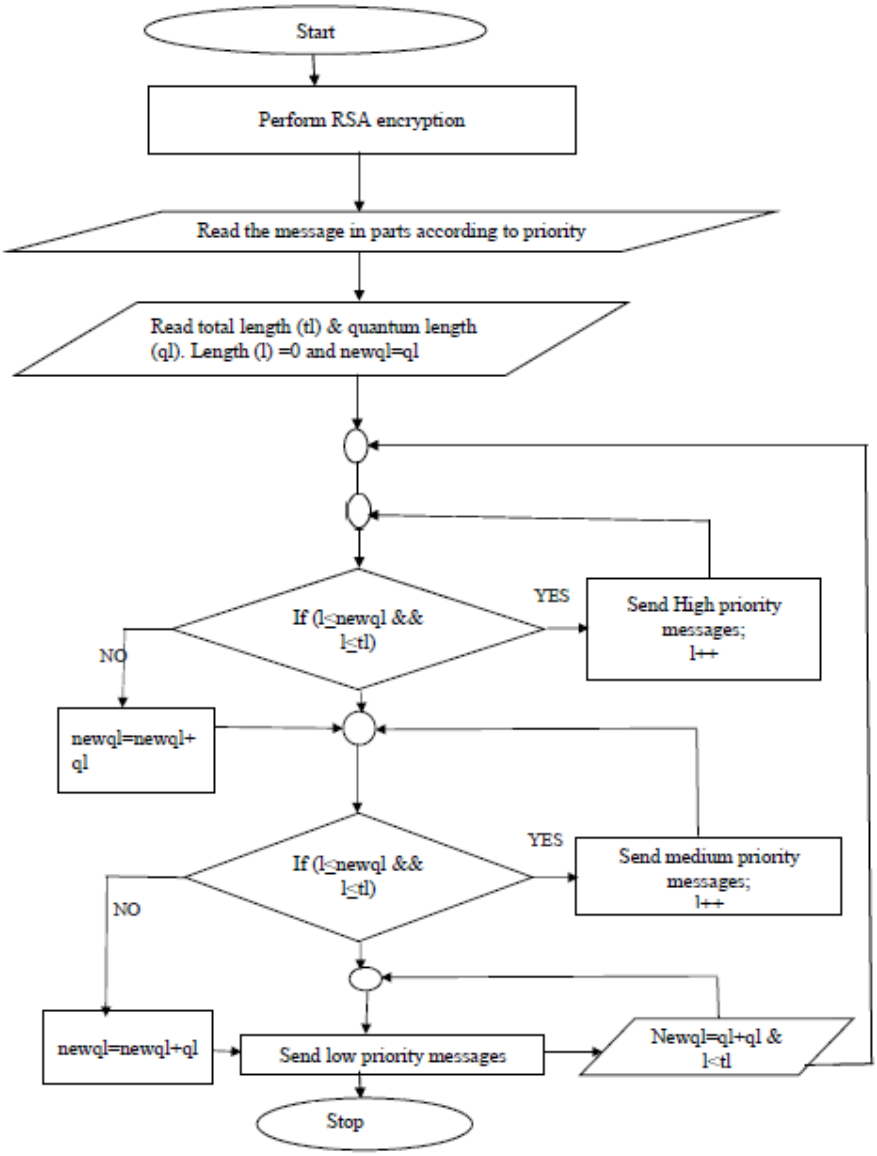


Figure 5. Flowchart for proposed algorithm

6.3. Implementation

The implementation of this hybrid algorithm is proposed using VC++. The main menu will contain options to encrypt and decrypt data. The user will then be asked to give the data, the key and specify the priority levels of various parts of the data. The output will be the encrypted message that will automatically be forwarded to the receiver through the specified mode using the proposed technique. The decryption of data can be done on the receiver's system using the same program and the key.

7. CONCLUSION

This paper presents an effective method that combines techniques that can be used to successfully communicate secretively in a network. The proposed algorithm reduces the effectiveness of intrusion and brute-force attacks as only a part of the message will be available even if the intruder interrupts any message and decrypts it. Also decrypting part of a message is not very easy. It uses RSA Algorithm, one of the most effective and commonly used cryptographic algorithms and adds more steps to it to reduce attacks. Side channel attacks will not be very effective on this technique as the power levels and leakages that are used to identify the algorithm used will vary from that of RSA algorithm. If an intruder is identified then the sending can be stopped and so, he will not receive the whole message as the messages are sent in parts. This therefore reduces the effectiveness of the man-in-middle attack. Thus, if combined with effective methods to prevent side channel and man-in-middle attacks this algorithm will prove to be very effective. This can also function effectively function as a software that can be used to encrypt/decrypt messages.

REFERENCES

[1] Nentawe Y. Goshwe, (2013). Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7.

[2] S. Subasree, N. K. Sakthivel, (2011), Design of a New Security Protocol Using Hybrid Cryptographic Algorithms, ICECT.

[3] P. Gutmann, (2004). Cryptographic Security Architecture: Design andVerification‖. Springer-Verlag.

[4] Ayushi, (2010). A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications (0975 - 8887), VOL.1 No.15.

[5] Suyash Verma, Rajnish Choubey, Roopali Soni, (2012).An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security. International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 7.

[6] S. D. Galbraith, C. Heneghan, J. F. McKee, (2005), Tunable balancing of RSA, Updated version of ACISP.

[7] Ravindra Kumar Chahar and et.al, (2007), Design of a new Security Protocol, IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134

[8] Willian Stallings, Cryptography and Network Security: principles and Practice. Tsinghua University Press, 2002.6

[9] Afolabi, A.O and E.R. Adagunodo, (2012). Implementation of an improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.

[10] Rivest R, Shamir A, Adleman L, (1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 (2): 120–126.

[11] Markoff, John (February 14, 2012). Flaw Found in an Online Encryption Method. New York Times.

[12] Ron was wrong, Whit is right,Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter, EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland, Self, Palo Alto, CA, USA.

[13] Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, (2012), Operating System Concepts. Wiley India Pvt Ltd, Sixth Edition.

AUTHORS

Meenakshi Shankar is a final year Electrical and Electronic Engineering and Information Technology students respectively in Sri Venkateswara College of Engineering, Sriperumbudur, India. They completed their schooling in 2011 from D.A.V Girls Senior Secondary School, Gopalapuram, Chennai. They are interested in Information Security and Cryptography

Akshaya.P is a final year Electrical and Electronic Engineering and Information Technology students respectively in Sri Venkateswara College of Engineering, Sriperumbudur, India. They completed their schooling in 2011 from D.A.V Girls Senior Secondary School, Gopalapuram, Chennai. They are interested in Information Security and Cryptography