SECURE STORAGE OF DATA USING CRYPTOGRAPHY FOR NETWORK

KADAMATI SRI KRISHNA CHAITANYA

Department of Information Technology, Vellore Institute of Technology,
Vellore, 632014, India
krishnachaitanya2010@vit.ac.in

ASHUTOSH KUMAR

Vellore Institute of Technology, Vellore, 632014, India
ashutoshkumar2010@vit.ac.in

RAVI KUMAR

Vellore Institute of Technology, Vellore, 632014, India
ravi.kumar2010@vit.ac.in

Abstract :
With the increasing rate of threats in the global environments; Information security engineers are continuously starving to develop a new secure algorithm to provide secure storage of information and at the same time, enabling the information to available to the authentic user easily. For this purpose, many efficient algorithms are being developed to protect the information from several threats. Cryptography is one of the ways to provide this service. In this paper we have proposed one such algorithm to allow users to share data on a global server within an organization at the same time, allow access to genuine users. The main focus of the proposed algorithm is on the storage of data and authentication of the user

Keywords*:* Threats; security; storage; cryptography; authentication;.

1. Introduction

Cryptography is the practice and study to enable communication between two or more groups even in the presence of a third party. It deals with syntax, semantics and protocols that the authentic groups follow to communicate highly confidential information.

Lot of effort has been put in this field, for generating algorithms. The main class of cryptography is classified as public key cryptography and private key cryptography. Public key or asymmetric key cryptography, as the name implies, the key is known to everyone in the environment, Private key or symmetric key cryptography, deals with encrypting and decrypting using a cipher key that cannot be disclosed to outside the communication group.

Private key cryptography is once again subdivided into block and stream cipher. Clock cipher deals with considering a block of characters or block of code for encryption. On the other hand, stream cipher refers to encryption of continuous stream of characters individually.

2. Survey

The author in the paper [1] has proposed an algorithm with reduced computational complexity, and the author has attempted to obtain a bigger size key from a smaller size primitive key. The author has mainly focused on the multimedia content. In the paper [2], the author, has proposed a cryptography solution for S-network based environment, and trusted repository for publication of keys. In the paper [3], the author has proposed a framework for biomedical investigation, and has attempted to eliminate the requirement for third parties, for analyzing sensitive data using a cryptography hardware based setup

3. Proposed System

The proposed system is most suitable for organization where employees store data in central storage. Here the data storage is on the central server which allows access for all the employees, storing data and can be called as central storage. The main aim is to have a central storage that users can store data for exchange. Most of the

organizations that are functioning today provide employees with a central storage rather than providing storage on each and every system individually. Moreover this leads to easy exchange of data. Also, the concept of central storage eliminates the need for an employee to use the same computer every day.

Here in the architecture 'Init' is the initiator of the data i.e. the data holder or sender.

Let us consider that the data available is "Hello we are VITIANS, we are from M.Tech-IT". This can be a file or just a simple textual data.

Fig. 1. Sample text.

The given data is stored in the form of binary bits or bytes.

Fig. 2. Applying the function.

The binary data is placed into a file for storage.

Fig. 3. Stage 3 for the conversion process.

The file is encrypted with a password which is decided by the initiator. The initiator keeps track with the password that he/she has set for the files created/held by him/her.

Fig. 4. The user provides password.

The encrypted file is split into ratio of (1:9) or (10% and 90%). The purpose of this split is for protecting the data from situation such as - if an intruder successfully grabs the 10% of data, the data will be useless till the rest of the data is stored in a location which is not predefined or can be calculated by the initiator.

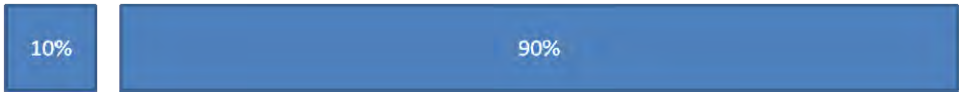


Fig. 5. The process of splitting file.

As the user stores the data on the central storage, the location pointer will be returned to him/her. The user has to store the location pointer in his local storage. The diagram below shows an instance of the pointer stored in individual computer. (A.10.f) – 'A' is the file name. Here, 10 represents the first ten percentage of the data. 'f' represents the pointer to the starting of the data sector. Similarly (A.10.l) – 'A' is the file name. Here, 10 represents the first ten percentage of the data. 'l' represents the pointer to end of the first ten percentage of the data.

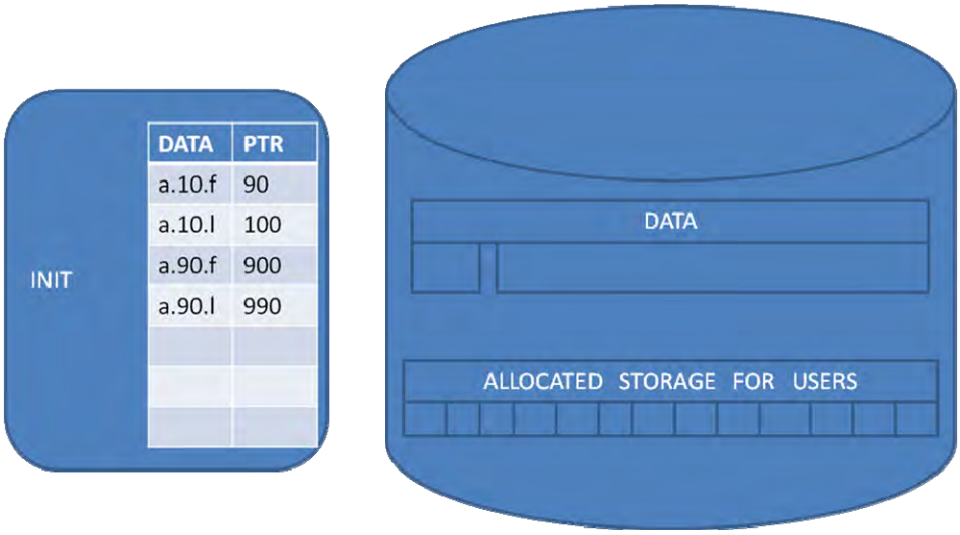


Fig. 6. Global view of the data at data center.

The diagram shows that an employee places request for the data 'A'. The request is placed in the format (REQUEST ID; LOC>ADDR; PASSWORD).

Request.ID represents a code that the sender has to use for calculating reply for the pointer of first ten percentages of the data which has been explained at a later point.

The LOC->ADDR represents location on global storage (each user in the organization is allocated some amount of storage which he/she can set access policy to for another employee). The employee is allowed to set temporary access to a particular location allotted to him and revoke within certain timeout.

The PASS is used while calculating the reply for the password required for decrypting the file. Once password is set for a particular file it may not need alteration. The calculation for encryption is demonstrated later.

The reply of the data for 1st 10% is calculated by performing modulo division of the first pointer with the request.ID. So, we store the dividend and reminder. We have to inform about the calculated dividend and reminder which receiver has to use while calculating the address location for 1st 10% data.

The difference between the first and last pointer is also appended along with the reply. The receiver has to pick up the data in sequential order.

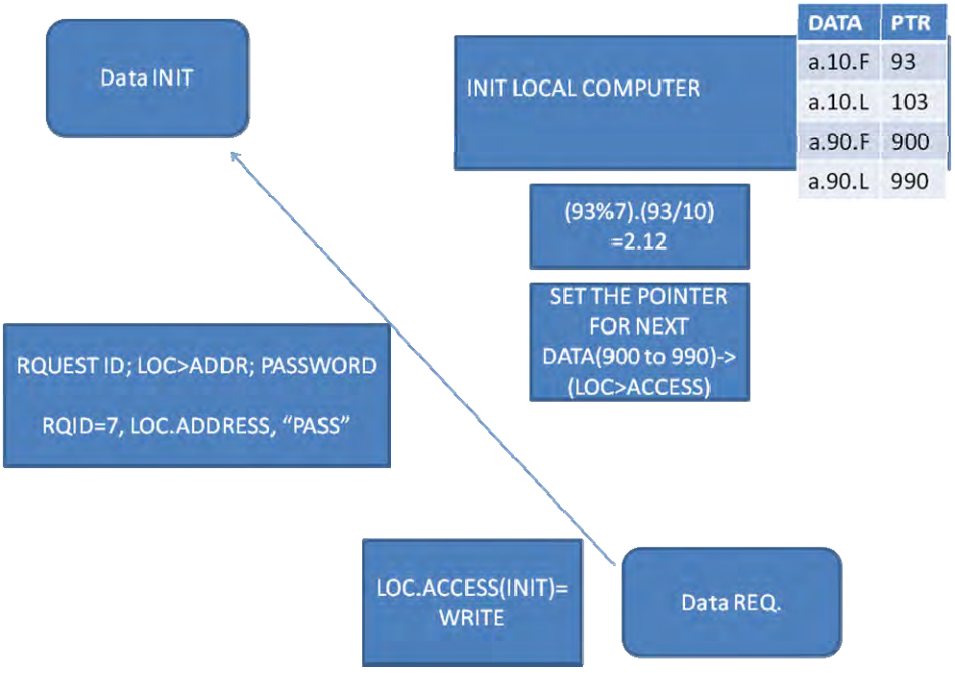


Fig. 7. Receiver side request for data.

The password calculation for the file is shown below. The initial PASS word sent from receiver which is converted to ALPHA-NUMERICAL position. The ALPHA-NUMERICAL position is converted to binary number and circular left shift is performed to obtain a new number which will be used for calculating the reply.

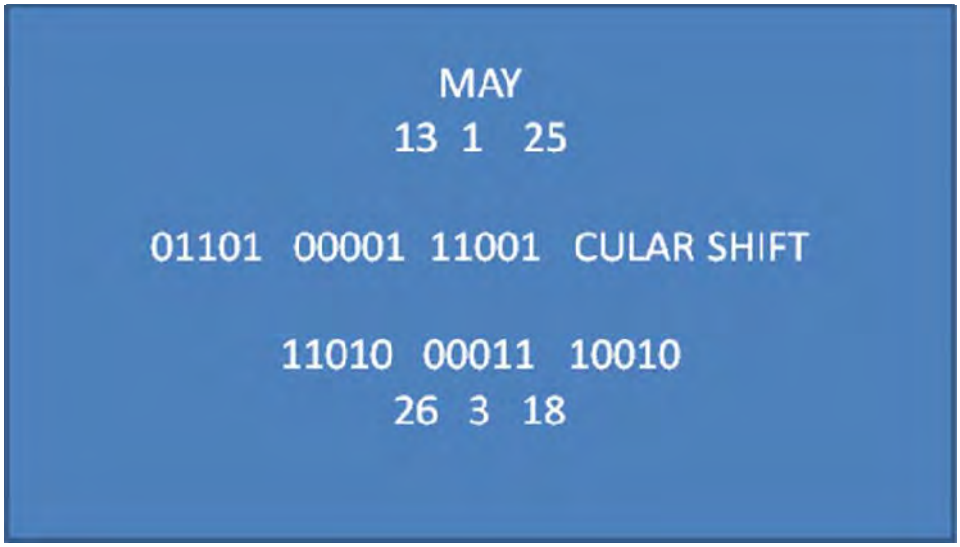
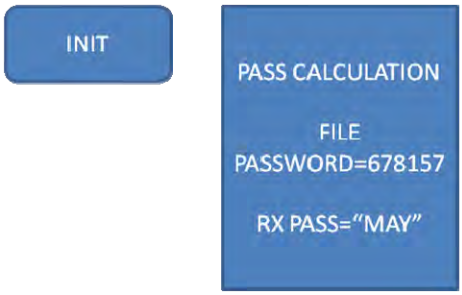


Fig. 8. Sample encoding of the password.

The obtained code after circular shift is placed in matrix along the row and the password for the file set by the initiator is placed along the column. Then multiplication operation is performed. We extract the elements (number) along the diagonal of the matrix shown below. The calculated code is appended with the reply.

Here the password for the file is 678157 and the calculated code for reply is 156.21.144.3.130.21.



X	26	3	18	Encrpted Key (TX)
6	156			156
7		21		21
8			144	144
1		3		3
5	130			130
7		21		21

Fig. 9. Password calculation sword.

The reply will be in the format shown below. The First 2 dotted decimal location carry (2.12) which represent the starting pointer. The third dotted decimal represent the no. of address location to be read for getting the 1st 10 %(i.e. 93 +10). The rest of the numbers in dotted decimal is used for calculating the password for decrypting the file.

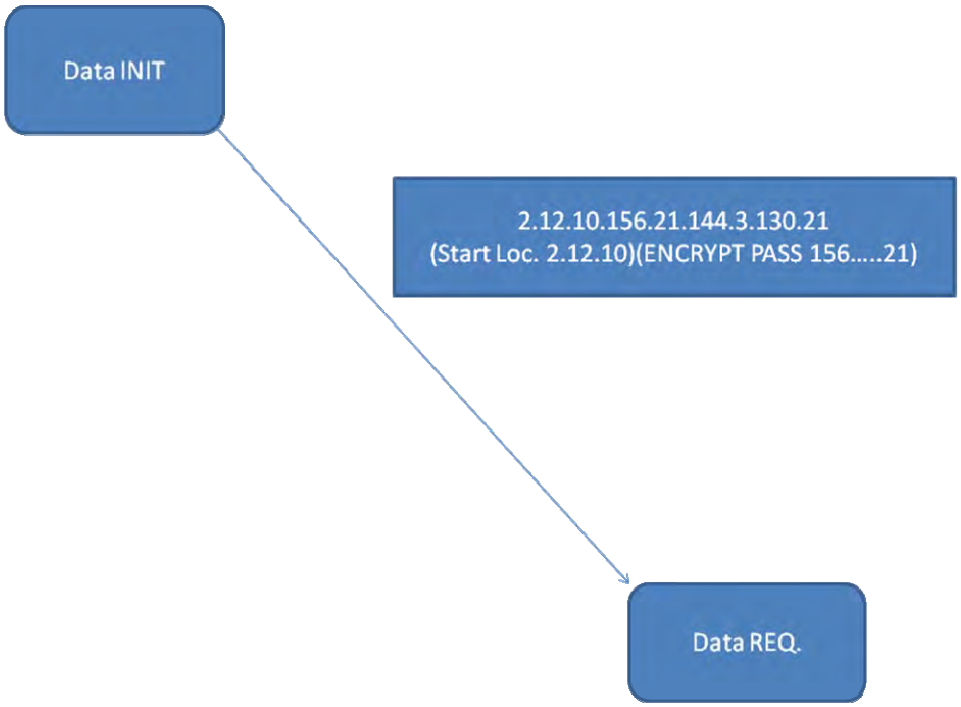


Fig. 10. Initial reply from the data owner to receiver.

The 1st step on the receiver is to extract and calculate the address for 1st 10% of the data. Also find the number of sectors to be read.

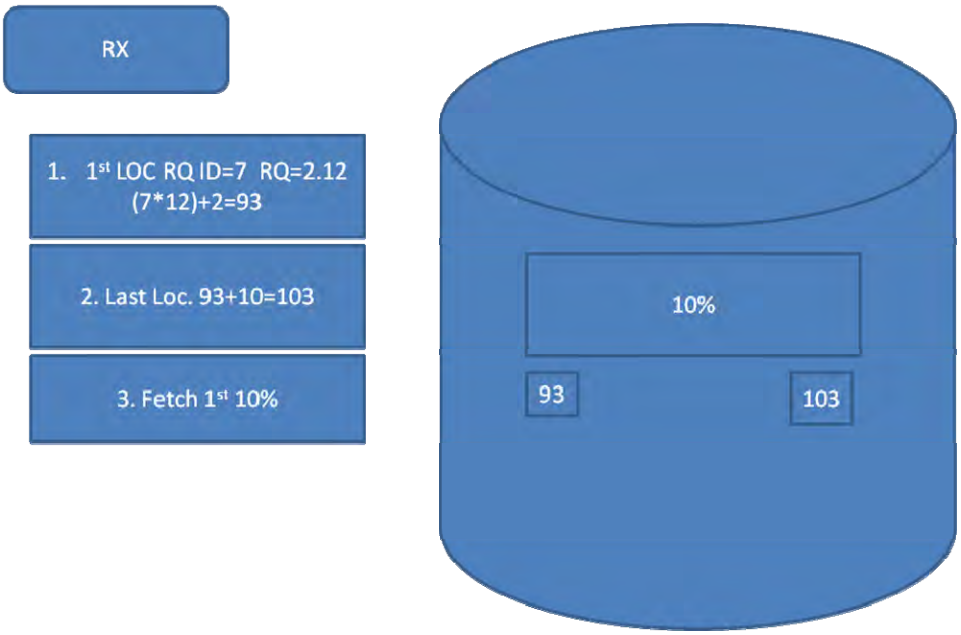


Fig. 11. Receiver side communication with the data center.

Next step is to access the memory location where pointer for the rest of the data is stored. The initiator places the pointer in the location allocated for him/her are the receiver. The length is calculated by comparing, the length of 1st 10% of the data. It 10%=10 then 90%=90. This way the entire data is fetched.

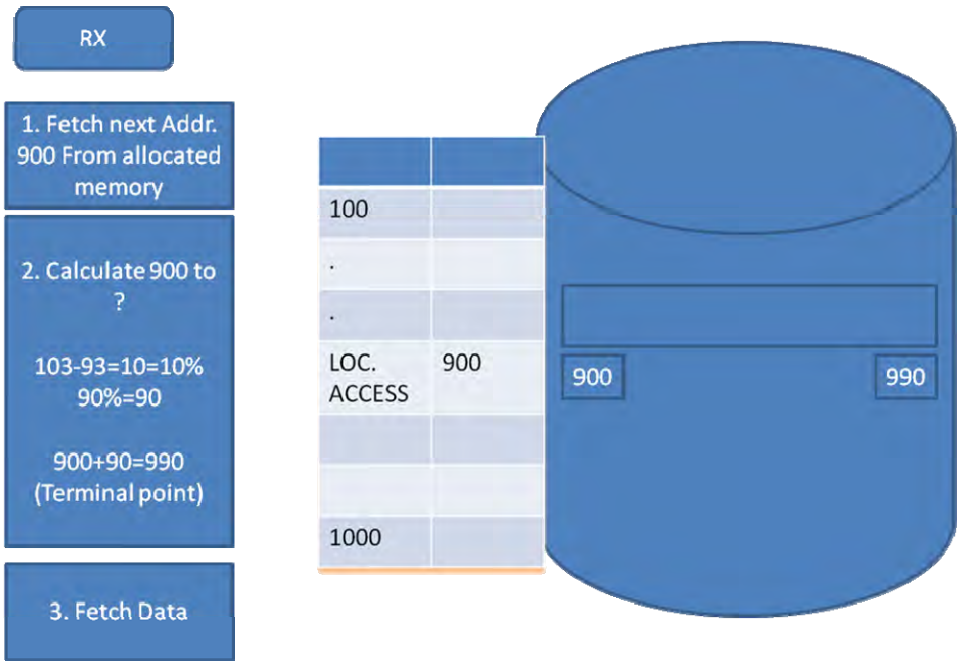


Fig. 12. Receiver side communication with the data center.

Once the data is fetched, the receiver will merge the data. Next step is to decrypt the fetched data once the password for decryption is calculated. This is done by performing the reverse operation to that used while encryption. We perform division operation here and extract the diagonal elements to obtain the password.

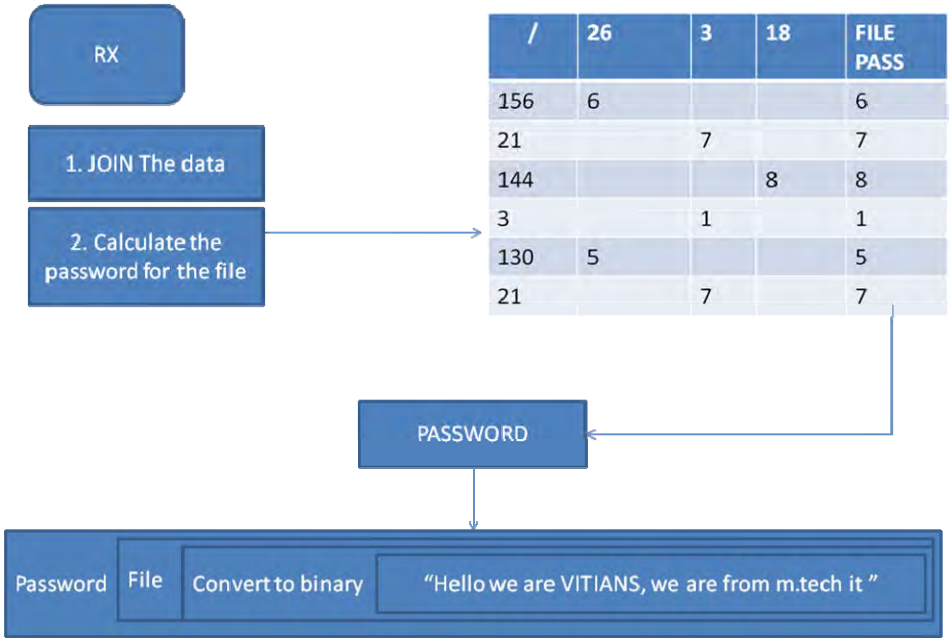


Fig. 13. Decoding the received data .

Once the password is calculated, the user decrypts to obtain the original data.

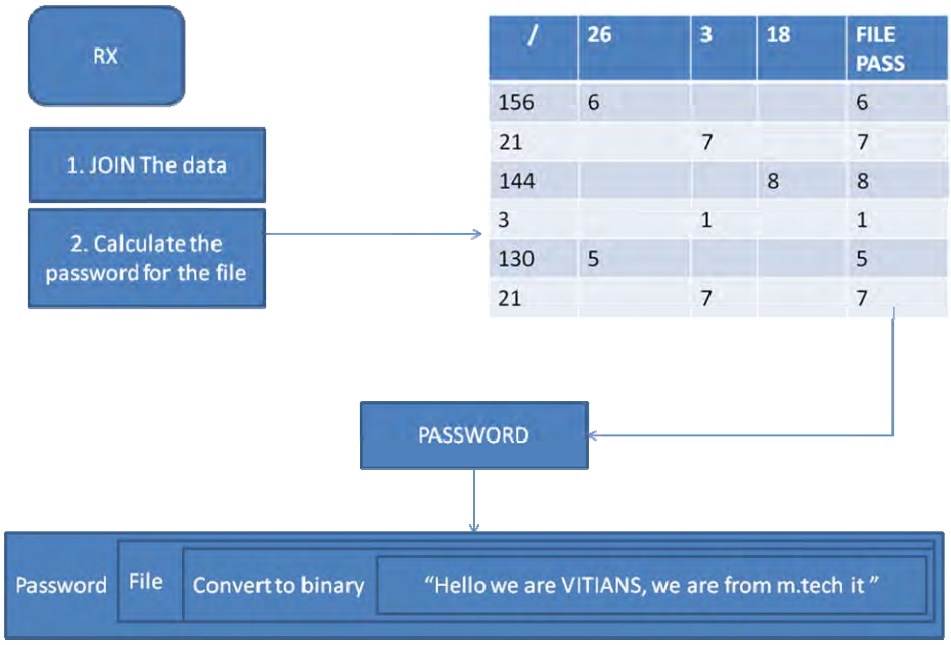


Fig. 14. Retrival of data.

This way, it gives the flexibility to store data in global storage and in a secured way, since intruder may be able to access only one part of data, but will take forever to find out the other part of data. Moreover, calculating address for the 1st 10% of the data will be very difficult. And randomly picking up data from central storage will not evolve any information. Lot of effort has been put in this field, for generating algorithms. The main class of cryptography is classified as public key cryptography and private key cryptography. Public key or asymmetric key cryptography, as the name implies, the key is known to everyone in the environment, Private key or symmetric key cryptography, deals with encrypting and decrypting using a cipher key that cannot be disclosed to outside the communication group.

4. Conclusion And Future Work

Cryptography is used to achieve few goals like confidentiality, data integrity and authentication of the data which has been exchanged between the sender and receiver. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. It has been found that the algorithms which are available at this moment are more or less difficult or complex in nature, and of course it is quite obvious, because those algorithms are used to maintain high level of security against any kind of forgeries.

The aim of this work was to design and implement a new model to centralize data storage for easy exchange of data for an organization with secured exchange. We plan to implement this using the emerging technology Swarm Intelligence. Swarm Intelligence is the popular technique used now days to solve all the kind of engineering, science and biological problems where the nature-inspired computing technique is employed for obtaining the optimum result. In this environment, we have planned to create the self-organized, distributed agents for various purposes like key generation, distribution etc. which may help us in reducing the key storage and distributing the keys in the secured manner.

References

[1] Canim, M.; Kantarcioglu, M.; Malin, B., (2011) Secure Management of Biomedical Data With Cryptographic Hardware, Information Technology in Biomedicine, IEEE Transactions.
[2] Viehmann, J. Secure communication with secret sharing in static computer networks with partition in mistrust parties, Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference.
[3] Gary C. Kessler : Block Encryption Standard for Transfer of Data an article available at www.garykessler.net/library/crypto.html.
[4] Gary C. Kessler : A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data an article available at www.garykessler.net/library/crypto.html.
[5] Pfleeger : Security in Computing 4th Ed, pp 194 - 230.
[6] S. William, Cryptography and Network Security: Principles and Practice, pp 69 - 236.
[7] S. Hebert: A Brief History of Cryptography, an article, pp 54 - 179