www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1788-1793

KEYLESS USER DEFINED OPTIMAL SECURITY ENCRYPTION

[1]M. Lakshmi, [2]. S. Kavitha

[1]Asst.professor, Dept.of.Computer science, Meenakshi Chandrasekaran College of Arts & Science Pattukkottai-614 626. Thanjavur..

[2]Research Scholar, Dept.of.Computer Science, Meenakshi Chandrasekaran College of Arts & Science Pattukkottai-614 626. Thanjavur..

Mail Id:vithish88@gmail.com

Abstract— Cryptography and encryptions, these terms are now-a-days have an unseen impact in the merging field of network and its security. In the global communal world, where faster access to precise information is the most basic need; security of confidential data during transfer from one place to another place is a major concern. There are a lot of sheltered approaches that can be applied inside the organizations premises to keep the data safe and sound. The prime goal leading the design of an encryption algorithm must provide security against unauthorized attacks. Key-oriented algorithms are very efficient but they were very bulky to manage as key handling must be done. Due to the great overhead, keyless algorithms seem an attractive option. There can be various techniques that can be used to attain secure transfer of data like firewalls, proxy servers, and steganography, data security plans against worms, viruses or denial-of-service attacks.

Keywords- **Cryptography, Keyless, User defined.**

I. INTRODUCTION

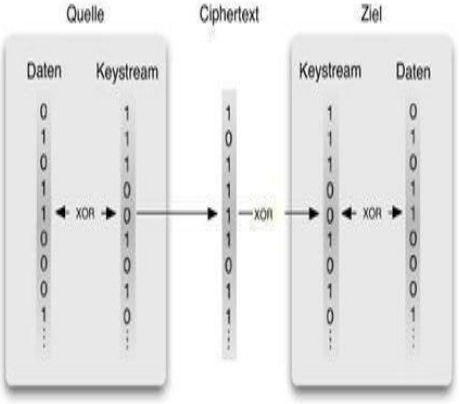
In computer and communication systems security issues play a crucial role and must be addressed before hand to guard against illicit attacks As security of data on any kind of system has became the first priority for the organization, the methods which are used to ensure security not only need to be strong and efficient, but should also be easy to execute and implemented. With progress in technology, encryption came up with a big boom, taken as a weapon of ultimate security. It is an earliest art and it is defined as the science of writing in secret code. Basically, the cryptography algorithms are categorized into two types on the basis of key management, which are key-oriented and keyless encryption algorithms. The prime goal leading the design of an encryption algorithm must provide security against unauthorized attacks. Key-oriented algorithms are very efficient but they were very bulky to manage as key handling must be done.

But cryptography proves itself as a central tool for achieving data and software protection. Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. The strength of this cryptographic technique comes from the fact that no one can read the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. Due to this advantage, quantum cryptography has grasped a great deal of attention and huge amount of research is being carried out on it for safeguarding of business-critical data. During the course of time, various encryption algorithms have been developed to achieve the ultimate aim of safe environment for information transmission. However, the principal objective guiding the design of an encryption algorithm must be security against all possible unauthorized attacks. However for all practical applications, performance and the cost of implementation are also important concerns. The best cryptographic algorithm is the one that strikes a good balance between security and performance.

Working of a stream cipher

PPROPOSED SYMMETRIC KEY ALGORITHM

The KUDOS cryptographic algorithm basically falls under the symmetric encryption i.e. the same key is used at both ends to encrypt and decrypt the data. However, KUDOS actually depends on the sequence counter instead of the encryption key. The major benefit of using KUDOS over other encryption algorithms is its power of customization. The user can manipulate the sequence counter according to his needs;

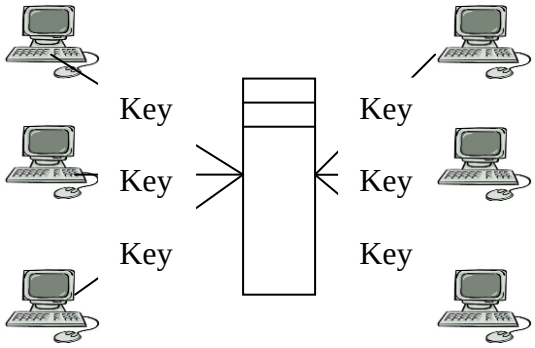


whether he wants it to be simple and faster or hard to crack and secure.

Sequence counter- The first thing which is new in the encryption scheme is sequence counter, which is used to provide the dynamic behaviour while converting the characters from one form to another. Sequence counters are the imposed temporary key to alter the characters and bits in the original data. The sequence is applied to the chosen number of data bits and the sequence number changes according to an algorithm which needs not to be saved or transferred over the network.

Binary level – The binary level is lowermost level. The calculation done here is totally is in form of 0 and 1. Bit level calculation provide more security because its effect are visible to all the level above it include character level.

In the proposed algorithm we have used both stream cipher and block cipher to enhance the security by using advantages of both i.e. high diffusion and bit level security.



A secret key is established between the KDC and each member of the group. The secret key of Alice with the KDC is referred to as KAlice and similarly the other keys like KBob, KGeorge and so on. Now if Alice wants to send a confidential message to Bob then the process will be

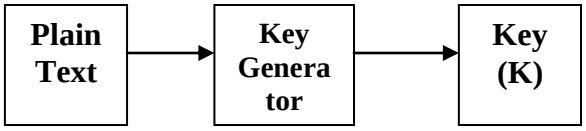
1. Alice sends a request to the KDC stating that she needs to communicate with bob and send some confidential data
2. The KDC informs to Bob about Alice's request
3. If Bob agrees then a *Session Key* is created between Alice and Bob for the purpose of communication.

THE SCHEME

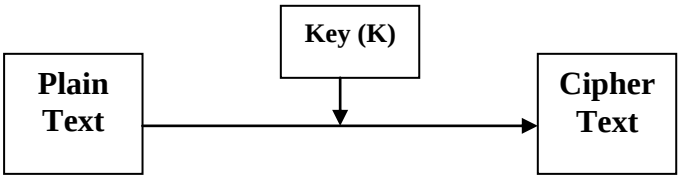
The SBSKCT algorithm consists of three major components:

- Key Generation
- Encryption Mechanism
- Decryption Mechanism

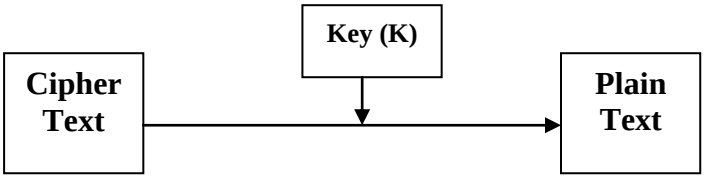
Key Generation:



Encryption Mechanism:



Decryption Mechanism:



PROPOSED ALGORITHM

3.1. Encryption Algorithm:

Step1: The input file i.e the plain text is considered as a binary stream of finite no. of bits.

Step2: This input binary string break in to block with different length like 8/16/32/64/128/256/512….(2k order where k=3,4,5,….) as follows

First n1 no.of bits is consider as X1 no .of block length y1 bits where n1=x1*y1.

Next n2 no .of.bits is consider as X2 no.of block length y2 bits where n2=x2*y2

And so on Finally Nm =Xm with Ym =8.so on padding is required

Step 3: For each block with length n,a unique number (ranging from 1 to 3*n) is generated for

the position of each bit using the following functions F1 (p)=p+n*[{ n+p*(-1)^(n%3)} %3];

Where, n=block length under consideration

P= position of the p th bit (-1)^(n%3) means that (n%3) is the power of (-1) (n%3) returns the remainder when n is divided by 3.

Step 4: The new position of each bit is generated to form the intermediate block using the given function f2(q)=(q+2)/3; where , q= generated unique no. using f1(p) for pth bit.

Step 5: The block of lengeth n(=2k) be regenerated after n/4 (=2k-2). Of iteration. Any of the intermediate blocks generated in this process may be used as encrypted string.

Step 6: The cipher text is formed after converting the encrypted binary string into characters.

Decryption Algorithm:

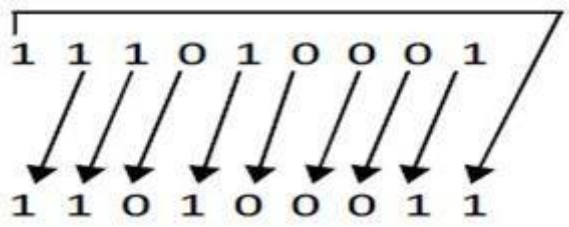
Step 1: For decryption process, the input file i.e. the cipher text is considered as a binary stream.

Step 2: After processing the session key information, this binary string is broken down into blocks of different length as similar as encryption process.

Step 3: Since a block of length n(=2k) is regenerated after n/4(=2k-2) no. of iteration, so the process is symmetric in nature. If n1 no. of iteration is used for encryption then (n/4- n1) no. of iteration is used for decryption.

Step 4: The plain text is reformed after converting the decrypted binary string into characters.

The first stack holds the information about the sequence counter implemented by the user. Whereas the other stack maintains the record for the data on which encryption has to be performed. The encryption process is of five steps; and four out of these five steps can be customized. Only step 2 cannot be altered by the user. The encryption process does a variety of binary operations like Shift Left Operation on the message for protecting it against unauthorized attacks.



Shift-left operation

The plain text is read from input file line by line i.e. separated by a full stop. The user has the option of choosing the sequence counter for transposition of characters. This sequence number must be a positive whole number. The shift-right operation is used here for transposing the characters. The first line characters are transposed using the sequence counter and the next line characters are transposed by incrementing the sequence counter by one. If the user opts not to choose the sequence number, the default sequence number 1 is selected. Suppose the value for first line is 1, for second line will be 2, and so on. If

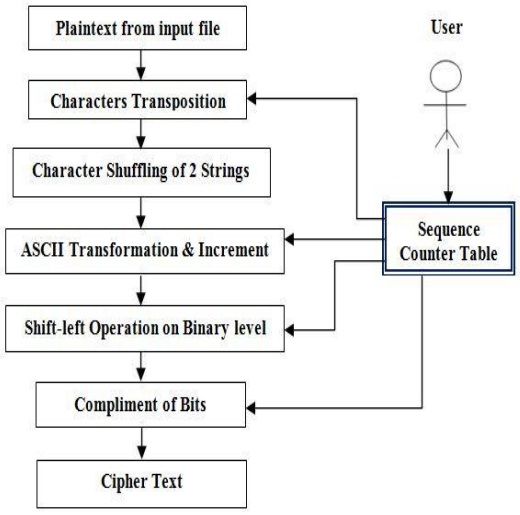
user specifies it as 5, value for first line will be 5, for second line it will be 6, for third line 7 etc. This step is categorized under block level encryption.

This part of encryption is user independent and is a block level encoding. Here, two strings of equal length are chosen from the text file and are shuffled. The shuffling takes place by placing one character of first string followed with one character from second string; and so on. For example: Following are the strings of length 20 characters selected:

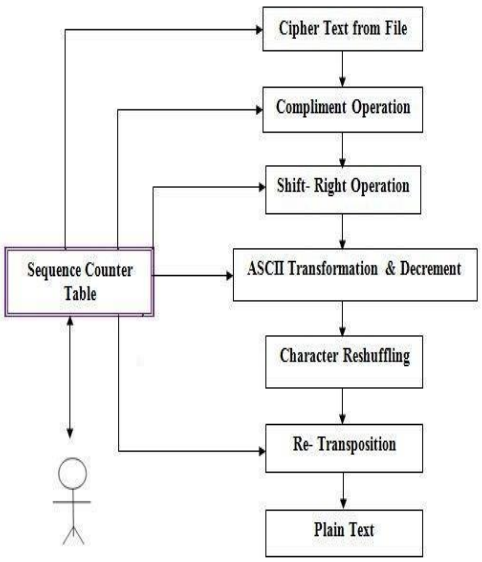
Q W E R T Y U I O P A S D F G H J K L Z and q w e r t y u i o p a s d f g h j k l z;

Then the output of this phase is:

Q w E r T y U i O p A s D f G h J k L z and q W e R t Y u I o P a S d F g H j K l Z.



KUDOS encryption process



KUDOS decryption process

CONCLUSION

The algorithm proposed in this paper is Keyless User Defined Optimal Security Encryption (KUDOS) is based on the concept of user customization. The algorithm doesn‟t use the traditional approach of using an encryption key; but defines a series of sequence-counters for encoding. The cryptosystem gives extra power to the user i.e. to choose the sequence-counters. Thus it is up to the user to maintain a balance between speed and security provided by the algorithm. The user can increase or decrease security and speed depending upon his/ her needs. The cryptographic algorithm is based partially on both stream and block encryption, hence the output of same input block over same input sequence-counter is dissimilar and provides enhanced security. Moreover, for security enhancement, the encryption is done at three levels: block level, character level and bit level. It makes it more

complicated and harder to break even with default values of sequence counters. Error control mechanisms can be used to safeguard the data against The KUDOS encryption algorithm is successfully tested on text data. KUDOS efficacy in text data encryption along with its supreme security; seems like an answer to the future encryption issues.

REFERENCES

[1] K. Gary, an Overview of Cryptography, an online article. Available: www.garykessler.net/library/crypto.html.[2] Y. Hao, E. Osterweil, D. Massey, L. Songwu, and Z. Lixia, "Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 656-669, Sept 2011.

[3] C. Bissell and A.K.Vladimir, "Pioneer of the sampling theorem, cryptography, optimal detection, planetary mapping" [History of Communications],*IEEE ommunications Magazine*, vol. 47, no.10, pp. 24 - 32, Oct 2009.

[4] J. Katz and Y. Lindell, *Introduction to Modern Cryptography:* Principles *and Protocols*, 1st ed. USA: Chapman and Hall/ CRC, 2007.

[5] R. S. Vignesh, S. Sudharssun, and K. J .J. Kumar, : A Comparative Study," *2nd International Conference on Environmental and Computer Science ICECS '09*, 2009, pp. 333 – 337.