International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 6, November-December 2014 **ISSN 2278-6856**

Design of a New Cryptographic Algorithm for Development of secure real-time password enabled exchange communication for Indian Armed Forces

Arun Singh Chouhan[1] and Bipin Pandey[2]

[1]Associate Professor, Department of Computer Science & Engineering
Vyas Institute of Engineering & Technology,
Jodhpur Rajasthan), India

[2]Assistant Professor , Department of Computer Science & Engineering
Vyas Institute of Engineering & Technology, Jodhpur Rajasthan), India

Abstract

In this research paper ,we proposed a study that aims at the design a new cryptographic algorithm for secure password communication for purpose of exchanging messages between army officers and central workstation connected to same type of computer networks. For this we used here a key management scheme algorithm and symmetric encryption cryptographic algorithm we used here a very lightweight block cipher based algorithm. The scope of this algorithm is military units and is intended to become the basis for the designed development of an integrated framework for the exchange of secure messages between different sites of military or other organizations that are concerned about information security.

Keywords:-Secure messaging, Key Management, Symmetric Encryption

1. INTRODUCTION

There are some of challenges faced by Indian Armed forces during information exchanges between officers and armed office workstation to ensure the data security principles like data integrity, confidentiality and Authenticity. Indian Armed Forces, similarly to other organizations that are concerned about the security of information exchanges, have always heavily relied on secure exchanges of messages. A reliable system for such message exchanges is considered to be a particular strength for such organization, so a symmetric encryption algorithm is used for particular real-time messages communication The problems and overheads related to the management of the secret keys are considered. The application of an advanced scheme for the automation of the key management is proposed.

2. FUNCTIONS OF THE SYMMETRIC ENCRYPTED COMMUNICATION SCHEME

The basic functional principle for a system of symmetric cryptographic communication is the use of a shared secret key that is used for both encryption and decryption. The secret key is the most important element of the encryption system, as it is the principle means that transforms clear messages to cipher-texts. The disclosure of the key to malicious users or hackers exposes the essence of communication. For a group of users of a symmetric cryptography system, the method of a shared secret key is widely used. With this method, if a malicious user were to join forces with enemy cryptanalysts, they would only be capable of disclosing their own secret keys and hence disclose all communication in which they took part. This way, in a group of authenticated users such as the users in a military environment, the use of a shared key for all users entails problems since any disclosure of the key would annihilate security for all communications. For this reason, instead of using a single key for everyone, a protocol can be designed for which every user is issued a secret key which they distribute via safe communications channels or via personal contact to all the users with whom they are interested of securely communicating.

3. PROPOSED METHODOLOGY & ALGORITHM

We propose a computationally lightweight block cipher based algorithm allows secure password communication for purpose of exchanging messages between army officers and central workstation connected to same type of computer networks. In this algorithm uses a matrix key which on multiplication with a ternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate a perfect model of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The type of operations used for transforming plain text to cipher text. All encryption algorithms are based on two general principles. Substitution in which each element in the plain text is mapped to another element and transposition in which the elements in the plain text are re-arranged. Most systems involve multiple stages of substitution and transpositions. The number of keys used. If the sender and receiver use the same key, the system is referred as symmetric, single key, secret key or conventional

encryption. If the sender and the receiver each uses a different key, the system is referred to as asymmetric, two key or public key encryption. The way in which plain text is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. The application presented in this article is developed based on the above protocol. More specifically, a user of the application is assigned a personal key (of their own choice or automatically generated) that they disclose to certified users of the same application that have access to the common network. On the other side, the same user receives the corresponding secret keys from all these users. The above protocol gives the possibility for duplex encrypted communication between use. A stream cipher processes the input element continuously, producing output one element at a time, as it goes along. In this cryptographic algorithm for keys generating we used a very strong and lightweight block cipher algorithm that given as:

3.1Algorithm for generation of Keys

The steps that are involved in the proposed block cipher algorithm is as follows.

Step #1. The decimal values and letters of the plain text are given numerical values starting from 0.

Step #2. A random matrix is used as a key. Let it be X.

Step #3. A "Ternary Vector" for 3^3 values i.e. from 0 to 26 is generated.

Step #4. Let this be "Y".

Step #5. 1 is subtracted from all the values of ternary vector.

Step #6. The modified ternary vector is multiplied with the matrix key.

Step #7. A sign function is applied on the product of ternary vector & matrix key.

Step #8. 1 is added to all values of Step #7.

Step #9. A sequence is generated which is used as sub key

Step #10. The sub key is added to the individual numerical values of the message to generate cipher text.

It can be seen that to extract the original information from the coded text is highly impossible for the third person who is not aware of encryption keys and the method of coding. Even if the algorithm is known it is very difficult to break the code and generate key, given the strength of the algorithm .Thus given a short response time through Wireless Sensor Network and broadcasting communication, the algorithm is supposed to be safe.

3.2 Algorithm for generation of key holders

Step #1. Consider the sequence of values starting from 0 to n where n be an integer.

Step #2. Read the sequence generated from algorithm 3.1.

Step #3. Read the starting element of step 1 and store the first element of step 1 and the corresponding first element of step 2 in a separate Key holders.

Step #4.1 Compare the element of step 3 with the elements of step 2. If there is a match, store the corresponding elements of step 1 in the key holders specified in step 3. Neglect already visited elements.

Step #4.2 Repeat step 4.1 with the remaining elements of the key holders of step 3 and store them in the same key holder. This will form one key holder.

Step #5. Go to next element of step 1 which is not visited earlier.

4. SECURITY ANALYSIS

The model uses a sign function on the product of ternary vector and a matrix key to generate the sequence. The sign function converts all positive values to 1, negative values to -1, and zero with 0.This sequence is substituted for plain text to generate cipher text. Thus it is impossible to generate the matrix key from the known plain text and cipher texts. Thus this model is free from differential crypto analysis. Since variable length keys are used it is also free from linear crypto analysis. This algorithm is completely free from cipher text only and known plain text attacks but may not be completely free from chosen plain text and cipher text attacks where a part of information may be leaked out by cryptanalysis.

This algorithm is completely free from cipher text only, type of attack. By the other attacks, the key may not be retrieved but a part of plain text may be retrieved.

5. ADVANTAGES

1. It is almost impossible to extract the original information.
2. Even if the algorithm is known, it is difficult to extract the matrix key.
3. Versatile to users. Different users of internet can use different modified versions of the new algorithm.
4. As per basin values, the same character is substituted by different alpha numerical value which provides more security for the message.

6. CONCLUSION

We conclude our cryptographic Algorithm for Wireless Sensor network and in this work a ternary system with a 3 digit number is used. So the sub key generated is a 3^3 i.e. a 27 digit number. By considering a ternary vector with a four digit number or five digit number, the length of the sub key can be increased by 3^4, 3^5 which increase the length of sub key generated. Similarly by considering n –array vector the length of the sub-key generated can still be increased. Thus by increasing the length of sub-key, security of cipher system can be increased still further. This Algorithm is very useful for providing security in broadcasting in battleground and short distance message communication. In the given work, a ternary vector with a 3 digit number is used. By using a n-ary vector the length of the vector can be increased. By increasing the length of the vector, the number of basins may not be increased. But the number of values in each basin will be increased which provides more strength to the developed model. It is also observed that by slight variations in the key values and plain text, the number of basins formed and number of values of each basin are varying in nature, which provides a better avalanche effect. This provides more security and strength to the algorithm.

References

[1] D.w. davies and w.l. price, Security for Computer Networks, John Wiley & Sons, New York, 2nd edition, 1989.

[2] Criticism of ISO CD 11166 banking key-management by means of asymmetric algorithms", W. Wolfowicz, editor, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 191–198, 1993.

[3] Arun Singh, Bipin Pandey, "Design and Performance Analysis of new Cryptographic Algorithm for Wireless Sensor Networks & Broadcasting Applications Security" ,IJAIEM vol 3,issue 11,Nov. 2014 pg 299-301.

[4] W.Fumy,P.landrock, "Principles of key anagement", IEEE Journal on Selected Areas in Communications, 11(1993), 785–793.

AUTHORS

Arun Singh Chouhan received the B.E in Computer Science & Engineering from University of Rajasthan Jaipur(Rajasthan) and M.Tech from Devi Ahilya University ,Indore(MP) and currently pursuing PhD in Computer Science and Engineering from Jodhpur National University, Jodhpur(Rajasthan).He is more interested in Cloud Computing, Computer Networks and Distributed system with challenges and application in computer science. He is member of various international bodies like IAENG, Hong-Kong, CSTA, New-York, USA, UACEE, USA and ISTQB, Germany.

Bipin Pandey received the B.Tech in Computer Science & Engineering from Gautam Budha Techincal University, Lucknow (UP) and currently pursuing M.Tech in Computer Science and Engineering from Jodhpur National University, Jodhpur(Rajasthan).He have wide knowledge of Java Programming and Database Management Systems and Internet Programming. He is also Oracle Certified Java Professional(OCJP) Certified professional.