International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Secured Wireless Communication Between Remote Army Stations

Anand Nayan Nagada[1], Pooja Vardhaman Pahade[2], Indrani Jitendra Shah[3]

[1]*UG Student, depart. Of E&TC, SNJB's KBJ COE, nagda.anand@gmail.com*
[2]*UG Student, depart. Of E&TC, SNJB's KBJ COE, pooja.pahade1612@gmail.com*
[3]*UG student, depart. Of E&TC, SNJB's KBJ COE, indranishah777@gmail.com*

Abstract- In earlier security systems, data transmission between two army stations was being hacked by terrorists, enemy nations and even spies. Hence, data security is very important especially from defense point of view. There are various techniques for transmission of data securely. Cryptography is a one of the technique which can be used for secured transmission of data. There are numerous algorithms available for encrypting and decrypting data and many algorithms are being discovered. Poly alphabetic cipher algorithm is one of the strongest algorithms used for securing data in army stations. In this paper, poly alphabetic cipher algorithm is discussed for wireless data transmission between army stations using arm7 processor.

Keywords - Cryptography, security, Decryption, Encryption.

I. INTRODUCTION

We are living in. the information age. We need to keep information about every aspect of our lives. In other words, information is an asset and an asset needs to be secured from attacks.

To be secured, information needs to be hidden from unauthorized access, protected from unauthorized change and availability to an authorized entity when needed. Security is one of the most important factors in our life. We apply password to our PC's, laptops for preventing our private data. It is also a type of security. Technological advancements are happening day-by-day. Hence, there is a possibility of leaking secret information that may seriously damage any organization or a national security. [1]

Especially, at the war time the terrorists and spies tries to get the information by leaking our hi-tech security systems so that they can capture the important information useful to win the war. In the Business field too, security plays an important role. The Present techniques having many drawbacks such as, anyone can receive, transmitted encoded message then these systems never provides the applications such as:

- Privacy & Integrity
- Message Authentication
- Availability
- Confidentiality

Spread spectrum technique, Cryptography technique are some of methods for securing data. Subsequently, we describe these techniques, especially the poly alphabetic substitution cipher in detail, and at last conclusion of paper.

@IJMTER-2015, All rights Reserved

II. SECURITY TECHNIQUES

A. Spread Spectrum Techniques

Dating to World War II innovation, spread spectrum was a military communications application for decades before the technology became advanced. The U.S. Military has used SS signals over satellites for at least 25 years. Military systems have used spectrum widths from 1000 to 1 million times the information rates are used.
The ability to resist interference and interception along with its anti-jamming effects proved beneficial for military purpose. But the biggest disadvantage of this technique that proved to be dangerous to military application was it was easy to hack by spies and enemies.[2]

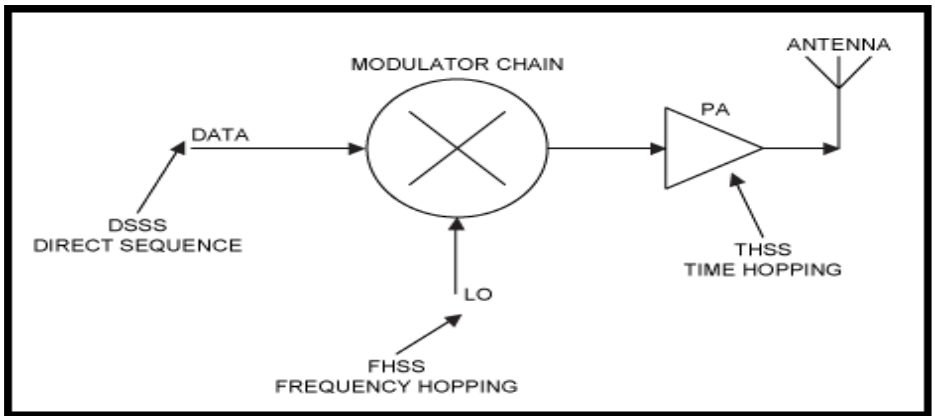

Figure 1. Block diagram of DS-SS Technique

In this technique as shown in fig.1, the serial data input is given to modulo-1 adder, at the same time pseudo-random noise signal (PRN) is applied to modulo-1 from PRN generator. The output of adder is given to the chains of modulator to modulate it with the local oscillator (LO) frequency to generate modulated signal. This modulated signal is applied to power amplifier to amplify the signal and then it is transmitted in air as an electromagnetic wave with the help of transmitting antenna.

B. Cryptography Technique

Due to the drawbacks of DS-SS system, we have to switch to new advanced technique, i.e. cryptography technique to achieve the security.

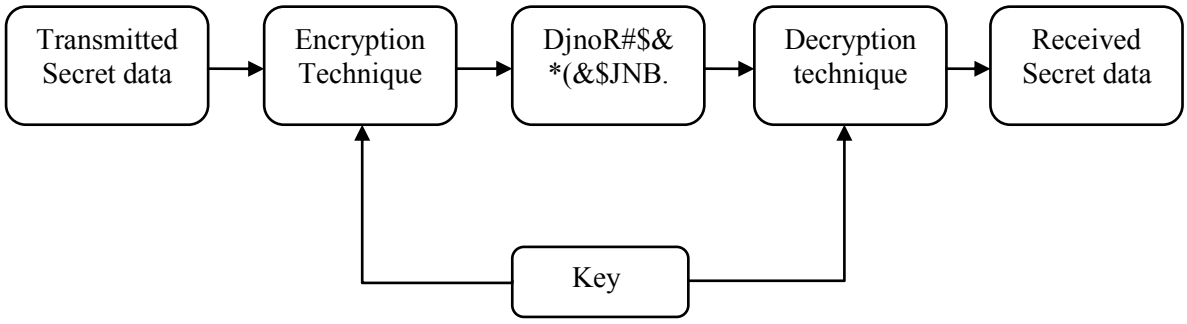

Figure 2. Cryptography Technique

@IJMTER-2015, All rights Reserved

Fig.2 shows cryptographic technique which is used to encrypt the data using encryption algorithm. Symmetric, i.e. same key is used here for encryption & decryption purpose. Cryptography technique is mainly classified into two categories as follows:

Symmetric key algorithm: In symmetric key algorithm, same key is used for encryption and decryption of the same data on both sides.

Asymmetric key algorithm: Asymmetric key algorithm uses different keys for encrypting and decrypting the same data on both transmitter's & receiver's side.

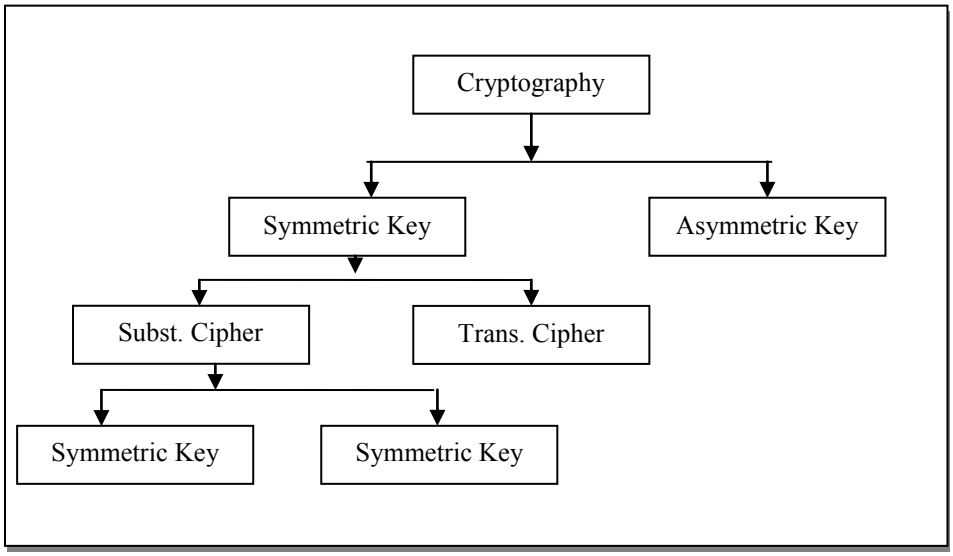

Figure 3. Various types of cryptography techniques

Fig.3 shows various types of cryptography techniques. Symmetric key algorithm is further categorized into two types: Substitution cipher and transposition cipher. Substitution cipher is used mostly for security purpose due to its advantages. Among these two algorithms the polyalphabetic substitution cipher algorithm is more advantageous and used in various applications.[2]

- ***Monoalphabetic substitution cipher***

In this type of substitution, a character in the plaintext is always substituted by some other character in the cipher text regardless of its position in the text. Here each plaintext character is shifted down by 3.[4]

- ***Polyalphabetic substitution cipher***

This algorithm is widely used due to its following advantages:

i. Provides more security than monoalphabetic cipher.
ii. Easy to implement.
iii. Replacement of same characters repeated in algorithm can be done using different characters.

III. POLYALPHABETIC CIPHER ALGORITHM

In this technique, we have simply used the number system to encrypt the data. The flowchart shown explains the detailed process of encrypting and decrypting the information to be transmitted.

@IJMTER-2015, All rights Reserved

- **Algorithm for Encryption:**
  i. START.
  ii. Represent the message to be transmitted in numeric form(i.e. a:'0',b:'1',..,z:'25').
  iii. Add corresponding key to the cipher text.
  iv. Substract 26 from the addition.
  v. Write corresponding letter of above numbers & Repeat the procedure till the end of text.

- **Algorithm for decryption:**
  i. START.
  ii. Represent the message received in numeric form(i.e. a:'0',b:'1',..,z:'25').
  iii. Add 26 to this numeric form.
  iv. Substract corrsponding key from the above addition.
  v. Write corresponding letter of above numbers & Repeat the procedure till the end of text.

IV. DESIGNED SYSTEM FOR SECURED WIRELESS COMMUNICATION

In our project, we have designed a system for secured wireless communication between two army stations. These type of system can be designed for PC's used at both the stations or one PC at main base station and a wireless device at remote base station.

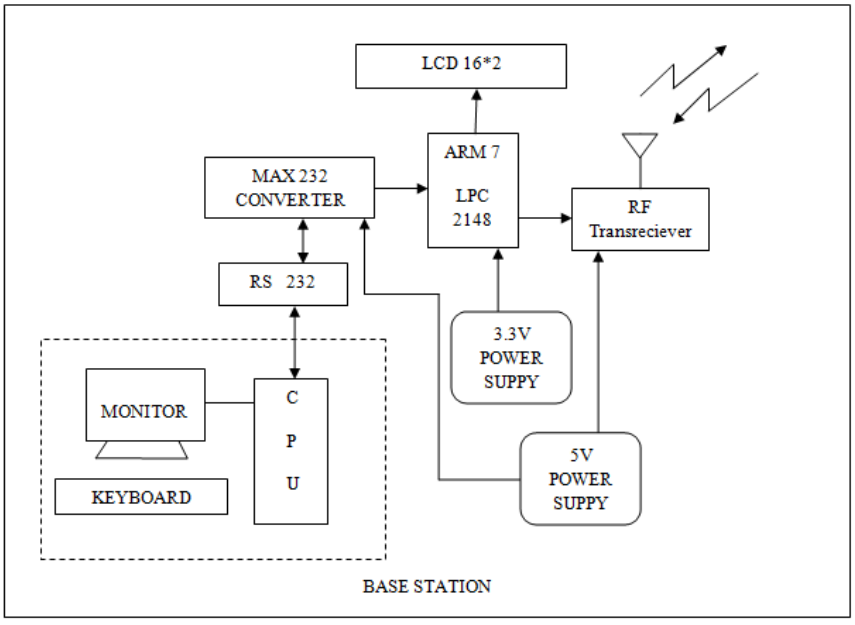

Figure 4. Block diagram at Base Station

At the transmitter's side, two arm7 microcontrollers are used for encryption and decryption purpose. One RS232 converter is also required for conversion of message transmitted from PC to microcontroller. a transreciever is also used for wireless commmunication between two stations. *Comcheck* is an application software used to observe the transmitted and Received data in frame structure.

@IJMTER-2015, All rights Reserved

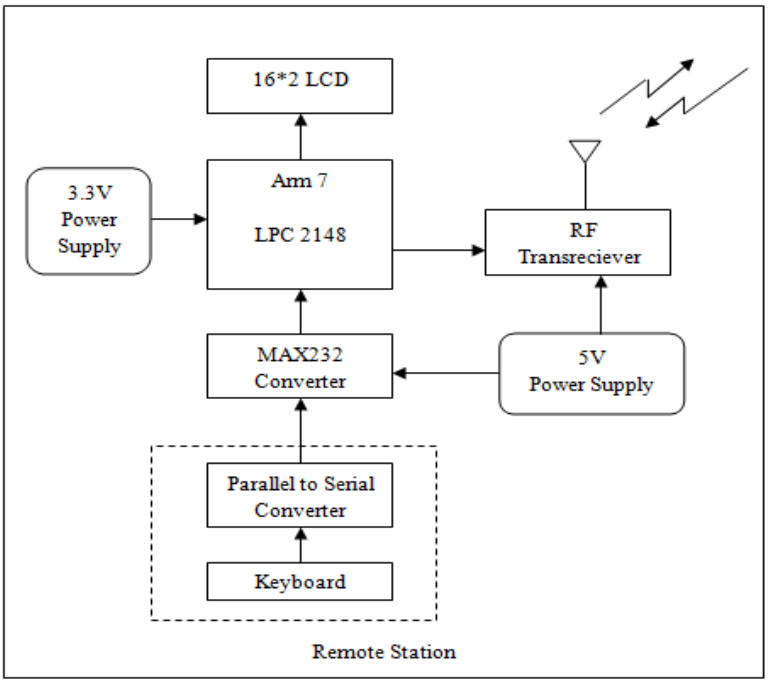

Figure 5. Remote Station

At remote station's side, we have designed a wireless device for transmitting and receiving message to and from main base station. A 16*2 LCD is used for displaying message. We have designed a 6*6 matrix keyboard consisting of almost 36 keys for typing message. Here also we have used one arm7 microcontroller and a transreciever for communication purpose.

V. CONCLUSION

Cryptography is indeed, the best method for data security. Among the various types of cryptographic techniques, Polyalphabetic Substitution cipher is the best method. This paper will help to maintain the privacy and to prevent any unauthorized person from extracting the information from the communication channel. So using this small concept, we will try to implement the algorithm for secured wireless communication over a long distance. This algorithm will help in obtaining the higher degree of security from terrorists, spies or any other harmful person. So this system can be practically used to obtain important information from source to destination using wireless communication.

REFERENCES

[1] Behrouz A. Forouzan, ed. SIE Cryptography And Network Security
[2] Dnyanda Namdeo Ahire 'Secured Wireless Communication' International Journal of Computer Applications, Volume 54-NO.1, September 2012.
[3] Http://www.cryptojinas.com -information of cryptography.
[4] Http://www.truecryt.org.

@IJMTER-2015, All rights Reserved