International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 507–512

Secured Wireless Communication Using Cryptography

Purva Deshpande[1], Smita Palnitkar[2], Anuja Joshi[3], Rutuja Ghate[4]

[1,2,3,4] *Dept. of E & TC Engg., Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune*

[1]purvadeshpande1999@gmail.com

[2]smitpalnitkar@gmail.com

[3]adjoshi37@gmail.com

[4]rutug5799@gmail.com

Abstract

In prior security frameworks, information transmission between two armed force stations was being hacked by fear mongers, foe countries and even spies. Sub-Sequent, information security is significant particularly from resistance perspective. There are different methods for transmission of information safely. Cryptography is a one of the method which can be utilized for verified transmission of information. There are various calculations accessible for scrambling and decoding information and numerous calculations are being found. Polyalphabetic figure calculation is probably the most grounded calculation utilized for verifying information in armed force stations. In this paper, polyalphabetic figure calculation is talked about for remote information transmission between armed force stations utilizing arm7 processor.

Keywords- *Cryptography, Arm Processor, Security.*

I. INTRODUCTION

Living in an era of information, we need to keep information about every aspect of our lives. Information is an asset and an asset needs to be secured from attacks. Technological advancement are happening day by day which are turning to be negative aspects for very nation and punitive measures need to be taken. Cryptography is one of the methods which would help in curbing such circumstances. In the war time terrorist & spies tries to get the information by leaking the hi-tech security systems with the goal to capture the information useful to win the war. Considering the above scenario cryptography comes out to be one of the good techniques for securing data, by creating a model which would help in maintaining the privacy of confidential information from unauthorized person ultimately providing privacy and integrity to army stations situated over long distance. Polyalphabetic is one of the method of cryptography which would help in implementing the desired purpose to obtain confidential information securely from source to destination using wireless communication.

II. LITERATURE SURVEY

Achieved the main objective stated earlier which is analyzing and implementing the wireless communication: the radio frequency (RF) transmission in the secret message communication for military purpose. The prototype of this project is using the frequency 434 MHz compare to the range about 3 kHz to 300 GHz of the frequency which have been reserved for the RF theoretically. Besides the functionality of this project proved that the other objective have been successfully attained which are design a secrete

ISSN: 2233-7857 IJFGCN

communication. This project have been developed using the programming in the microcontroller PIC 16F877. The "Secure wireless communication for military application" is an effective security and safety system which is made by integrating the advancements in wireless and embedded technology. It helps for a successful secret mission [1].

The design of this application was based on state of the art encryption technologies, namely AES, and exploits this technology within an environment that promotes and facilitates the use of safe practices on the behalf of users. More specifically, the application takes responsibility for the storage, retrieval and management of the secret keys required for the encryption and proposes a protocol for using keys for users that minimizes the risks for the unit if the secrecy of one or more of the keys is breached and the keys are disclosed to unwanted parties [2]

The corresponding attribute group keys are updated and a delivered to valid attribute group members securely. In addition to all of the components which is encrypted with a secret key in a cipher text are re-encrypted by the storage nodes with a random and cipher text components are corresponding to the attributes which are also re- encrypted with the updated attribute group keys. If the user has stored the previous cipher text exchanged before user obtains the attribute keys and holding attributes satisfy the access policy, user cannot decrypt the pervious cipher text. [3].

III. IMPLEMENTATION DETAILS

A. Base Architecture

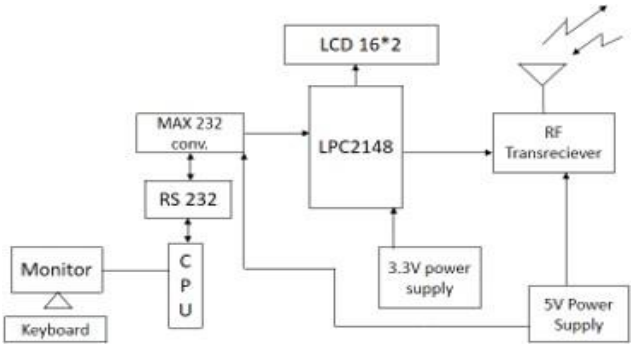
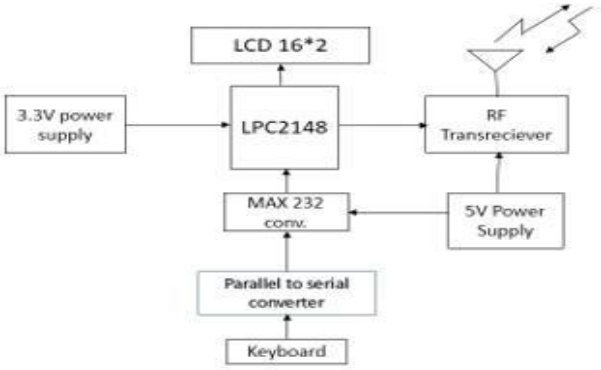


Fig. 1 Base Architecture

B. Remote Architecture



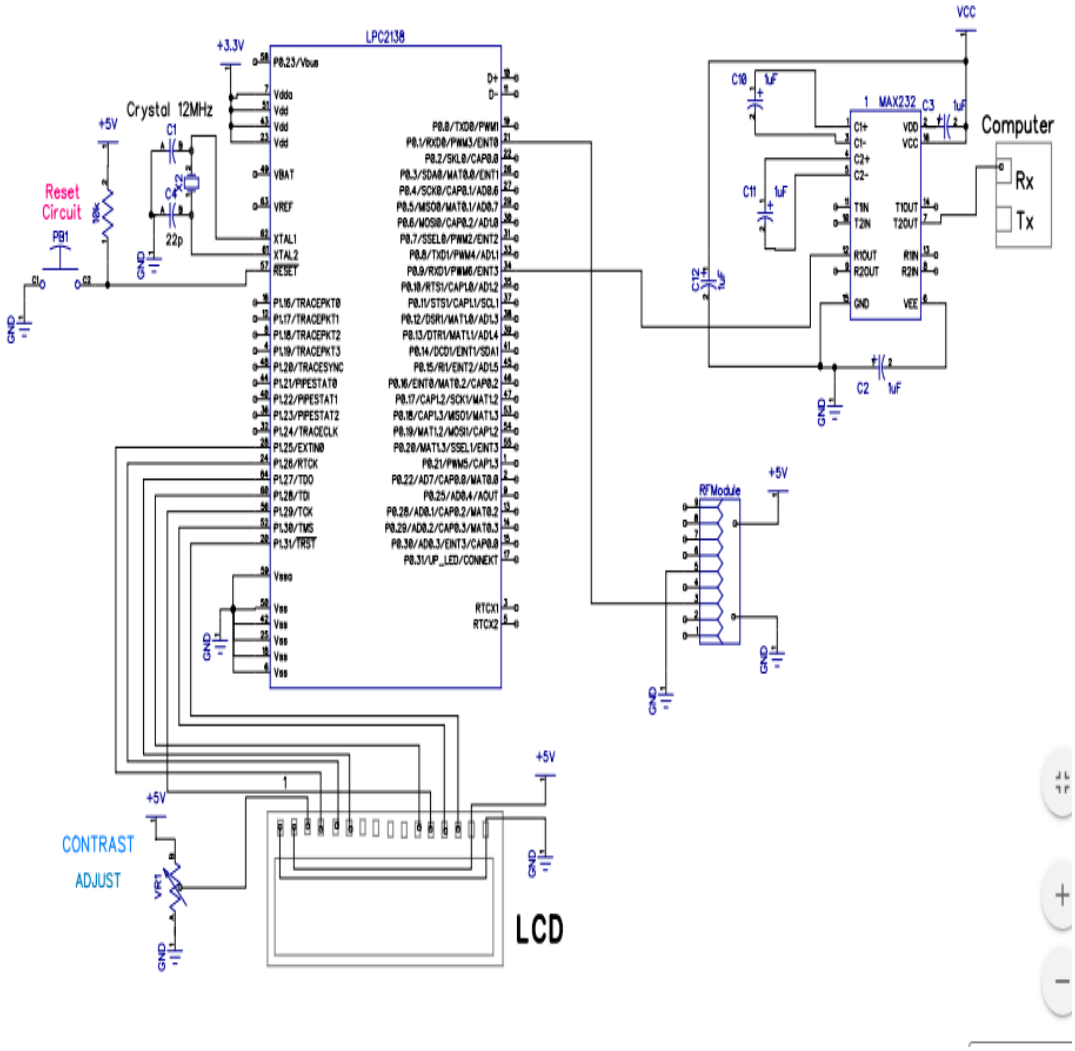
ISSN: 2233-7857 IJFGCN

Fig. 2 Remote Architectu

ISSN: 2233-7857 IJFGCN

The system proposed here is designed for secure wireless communication using encryption and decryption methods. Microcontroller used here is ARM7 LPC2148 at base station and remote station. RF module is used for wireless communication between remote station and base station. RF module works on 2.4GHZ frequency. RF module covers distance up to 30meters. Arm7 works on 3.3v power supply and all other peripheral like RF module. Lcd works on 5v power supply .We are designing 5v power supply using 7805 regulator and from that we will design 3.3v supply using LM317 adjustable regulator. Keypad used at remote station is 4*4 keypad, so that 16 keys are used for transmission of data. ARM7 has two serial port i.e. UART0 and UART1 out of which one is used for communication with PC and other for communication with RF module. RF module is interfaced to controller through serial port. At remote station encryption is done in which a fix number is subtracted from ever character of word and is sent to base station. At base Station that fix number is added to every char of that word and original message is retrieved. LCD indicates encrypted and decrypted message at transmitter and receiver end. Crystal of 12MHz is used to generate frequency for the operation of controller.

V. SIMULATION RESULTS



ISSN: 2233-7857 IJFGCN

Fig. 3 Simulation result of secure wireless ARM7 base

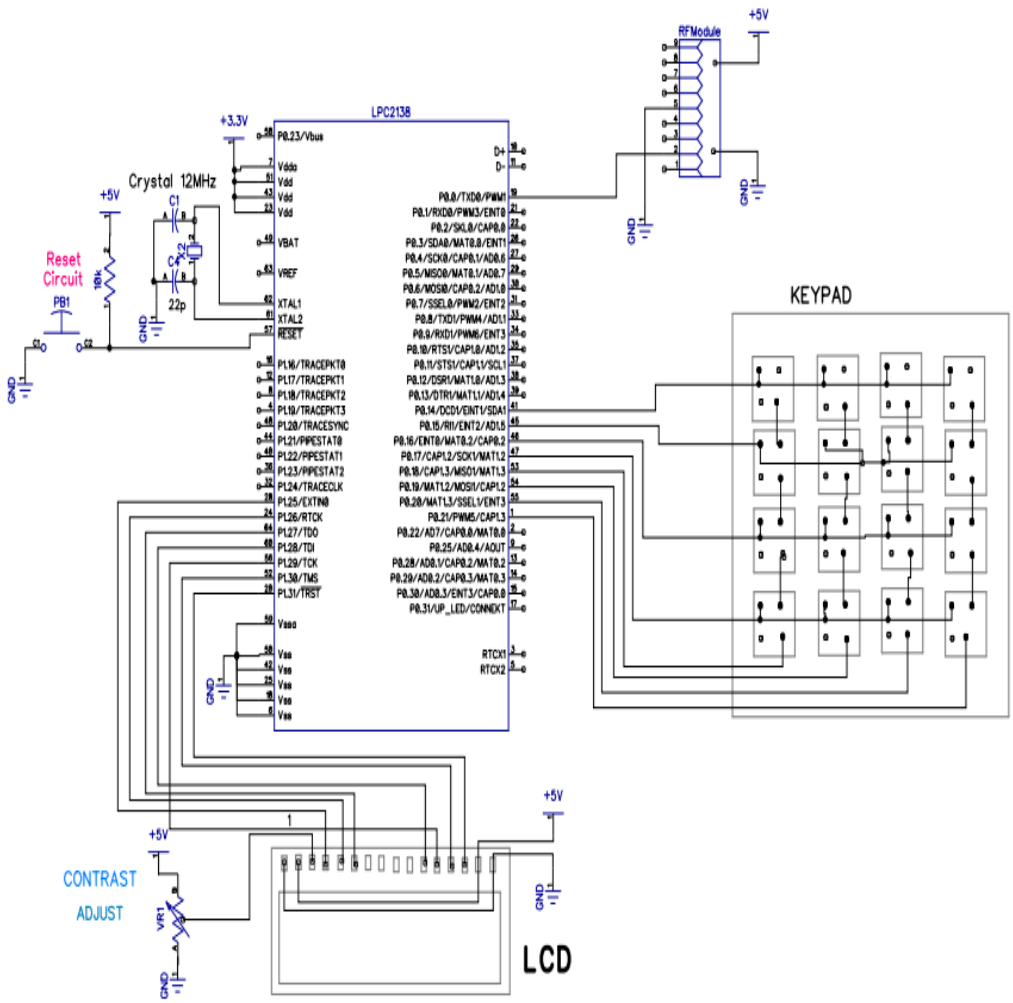


Fig. 4 Simulation result of secure wireless ARM7 remote

VI. 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.

ISSN: 2233-7857 IJFGCN

REFERENCE

[1] Sana Y. Sayyed, Sayali N. Gurap, Jyoti . Devadhe, Kajal R. Gat, "A review on: secure wireless communication for military application", International Journal Of Electrical, Electronics And Data Communication,2017
[2] Nikolaos G. Bardis , Nikolaos Doukas and Konstantinos Ntaikos "Design and Development of a Secure Military Communication based on AES Prototype Crypto Algorithm and Advanced Key Management Scheme",
[3] WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS
[4] Rasika S. Rangari , Prof. Anil N. Jaiswal ,"Review Paper on Highly Secure Data Communication Between Two Decentralized Army Stations", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),2015.
[5] S. Roy and. Chuah, "Secure data retrieval based on cipher text policy attribute based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[6] Anwar Saipulla Benyuan Liu Jie Wang,"Barrier Coverage with Airdropped Wireless Sensors Department of Computer Science, University of Massachusetts Lowell, MA 01854 USA IEEE 2008.
[7] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in Proc.IEEE INFOCOM, 2006, pp. 1–11.

ISSN: 2233-7857 IJFGCN