International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Smart Communication using RF Technology

[1]Bhavana R. Jamkar Information Technology & MET's Institute of Engineering,

[2]Pooja S. Patil Information Technology & MET's Institute of Engineering,

[3]Shivkanya A. Waman Information Technology & MET's Institute of Engineering,

[4]Yogita D. Kharwade Information Technology & MET's Institute of Engineering

[5]Puneet Patel Information Technology & MET's Institute of Engineering

---***---

Abstract:- Nowadays Security of data transmission is very important issue in Army, stations. Wired and wireless these are two types of communications. RF Technology is used for to transmit the data with wireless communication. There are several techniques for transmit the secured data. In Army station area is required secure communication. At the time information transmission between two army station was being hacked by terrorists, and enemies. we will mainly focus on the maintaining security between two army-station while transmitting data. Cryptography is a one of the techniques which can be used for secured transmission of data. There are A number of theory algorithms available for encrypting and decrypting data and many algorithms are being discovered. Number of theory algorithm is highly secure algorithm used for secured data in Army stations.

Keywords:- RF Trans-receiver, cryptography, Encryption, Decryption, microcontroller.

1. INTRODUCTION

Communication security is the regulation to protect unsanctioned interceptors from accessing secured telecommunication data while still delivering content to the intended recipients. From the introduction of data communication techniques to today, encryption techniques have evolved drastically. Digital technology has effectively replaced old analog methods of voice encryption complex algorithms, data encryption has become much more secure and efficient. But now a day this is done with the help of new technology. In this project, we will mainly focus on the maintaining security between two army-stations while communicating data. To overcome the issues regarding hacking of the transmission code or data between the transmitters and receiver of the army stations, we are going to introduce the new technology, i.e. Secure communication between two army station with cryptography. With the help of this technology using microcontrollers, there will be communication with a secret key that will know to transmitter and receiver only so that the hacker won't be able to get the exact data of communication. No internet connectivity is required for the transmission of data from one station to another as in many places like mountains or forests, there is always a problem of the Internet range or no use of any other devices.

2. ARCHITECTURE

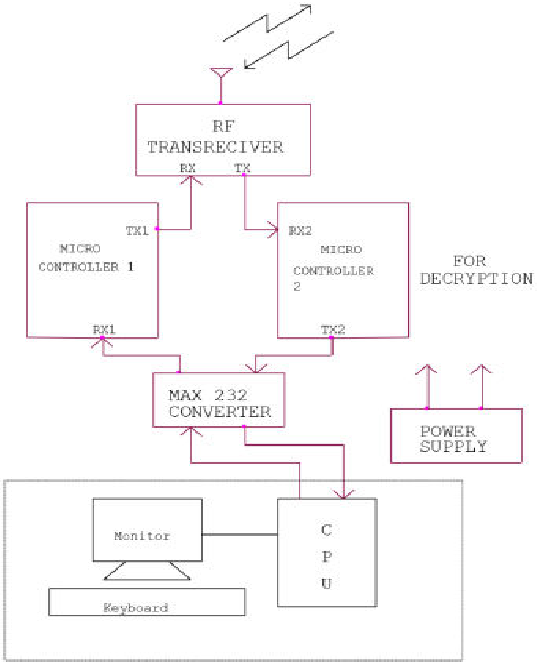


Fig.(a): -PC Side Communication

2.1 Block Diagram Description: - The above figure (a) shows the complete working block diagram of the system. The block diagram of system consists of Power Supply, Microcontroller, Computer, RF Trans-receiver, MAX 232 CONVERTER etc. There modules are used to describe the system properly. Microcontroller 1 and mcrocontroller2 are used for encryption and decryption respectively. RF TRANRECIEVER is used Transferring signals from transmitter to receiver station using RF signals. MAX 232 converter is used for converting the RS232 wave forms to TTL wave forms because computer is work on RS232 and microcontroller work TTL wave forms, it work as mediator between two different devices.

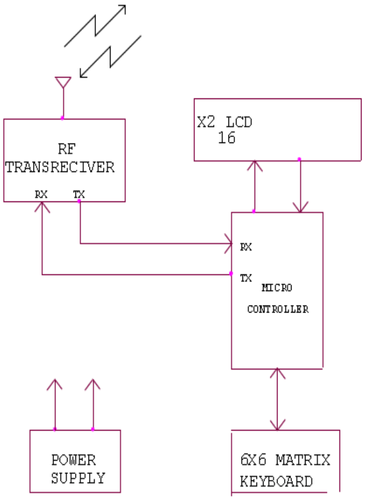


Fig.(b):-Diagram For Slave Station With OUT PC

2.2 Block Diagram Description: - In above fig(b) shows the working of receiver station. The block diagram consists RF Trans-receiver, LCD display, Microcontroller, Keyboard, Power Suplay. LCD display is used for displaying the messages which is typed by receiver or received messages from sender. Keyboard is used for typing the messages. RF Trans-receiver is used for transferring the messages using RF sign

CC2500 RF Trans-Receiver Module

CC2500 RF Modem is a transceiver module which provides easy to use RF communication at 2.4 GHz. It can be used to transmit and receive data at multiple baud rates from any standard CMOS/TTL source. CC2500 Wireless Trans-receiver module is a direct line in replacement for your serial communication it requires no extra hardware and no extra coding to turn your wired communication into wireless one. It works in Half Duplex mode i.e., it provides communication in both directions, but only one direction at same time (not simultaneously). This switching from receiver to transmitter mode is done automatically. We have Various sizes of Communication Modules.

3. ALGORITHM

In Polyalphabetic Cipher Algoritham, 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.

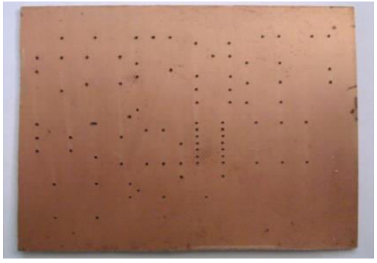
Encipher the following message using the key 19, 15, 22: there is a secret passage behind the picture frame
Answer:
To do this, start by Describing each letter of your plaintext by a number from 0 to 25 ('a' = 0, 'b' = 1, ..., 'y' = 24, 'z' = 25).
Do the identical for your key (unless, as in this case, it is already given by numbers). Then, write out the key over your plaintext like as you did for the letter-key. Finally, add the two numbers in each column. Is in the middle of 0 and 25, write down the similar letter.
If it is bigger than 25, simply subtract 26 from that and write down the letter that corresponds to the number you get.
Here's the first part of the example worked out:
"**there is a secret passage**" becomes:
19 07 04 17 04 08 18 00 18 04 02 17 04 19 15 00 18 18 00 06 04
We then write out the key repeatedly and put the message underneath:

KEY:	19 15 22 19 15 22 19 15 22 19 15 22 19 15 22 19 15 22 19 15 22
MES:	19 07 04 17 04 08 18 00 18 04 02 17 04 19 15 00 18 18 00 06 04
	--
SUM:	38 22 26 36 19 30 37 15 40 23 17 39 23 34 37 19 33 40 19 21 26
-26:	12 22 00 10 19 04 11 15 14 23 17 13 23 08 11 19 07 14 19 21 00
LET:	_M _W _A _K _T _E _L _P _O _X _R _N _X _I _L _T _H _O _T _V _A

Decryption is reverse process of encryption:

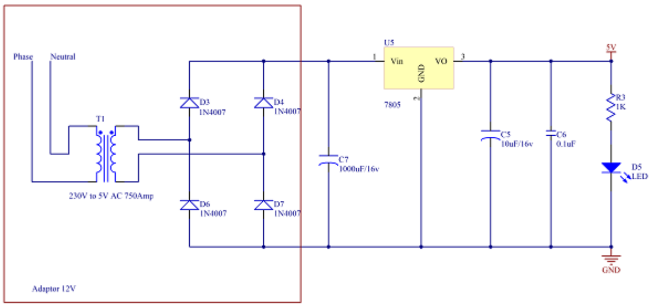
ENCRYPTED MES:	M W A K T E L P O X R N X I L T H O T V A
MES:	12 22 0 10 19 04 11 15 14 23 17 13 23 08 11 19 07 14 19 21 0
+ 26:	38 48 26 36 45 30 37 41 40 49 43 39 49 34 37 39 33 14 45 47 26
	-- ------
SUM:	38 48 26 36 45 30 37 41 40 49 43 39 49 34 37 39 33 14 45 47 26
- SECRETE KEYS:	19 15 22 19 15 22 19 15 22 19 15 22 19 15 22 19 15 22 19 15 22
SUB:	19 33 04 17 30 08 18 26 18 30 28 17 30 19 15 26 18 18 26 32 04
- 26:	19 07 04 17 04 08 18 00 18 04 02 17 04 19 15 00 18 18 00 06 04
RESULT:	T H E R E I S A S E C R E T P A S S A G E

4. IMPLEMENTATION



Designing Of PCB

It is the use of printed circuit board. The actual electronic circuit is limited to the imagination of the person designing the board. The name printed circuit board arises because the electronic circuit appears to be printed on the base material. A printed circuit actually consists of this layer of copper foil. The final circuit is shaped by etching the copper in FeCl3. The copper foil acts as a wire or conductor in the circuit. Component parts like resistor, transistor, capacitor and IC are soldered to the conductive foil to complete the electric path and circuit.

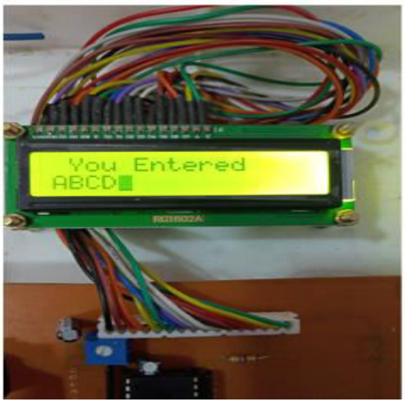


Designing Of Power Supply

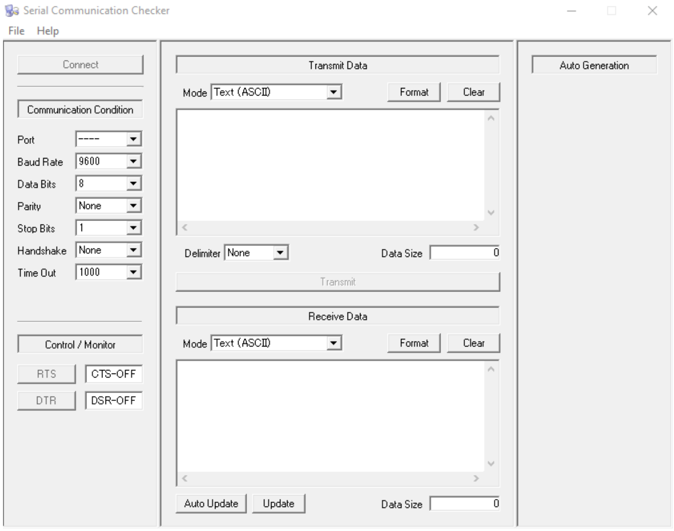
This is high priority feature. It uses 5V DC supply to work. Microcontroller, converter as well as Rf transceiver. For this, we have to use transformer to convert 230 V AC to 5 V AC. Rectifier is used to convert this 5V AC supply to 5V DC. Further, LM7805 will provide pure 5V DC supply for overall system. Capacitors are used at input and output side for filtration of ripples. 1. Transformer- converts 230 V AC supply to 5 V AC supply. The following information must be available to the designer of the transformer.

5. RESULT

It can be configured to drive a dot-matrix liquid crystal display under the control of a 4 or 8 bit microprocessor. Since all the functions such as display RAM, character generator, and liquid crystal driver, required for driving a dot-matrix liquid crystal display are internally provided on one chip, a minimal system can be interfaced with this controller/driver.



Display of Entered Data by User



Serial Communication Checker

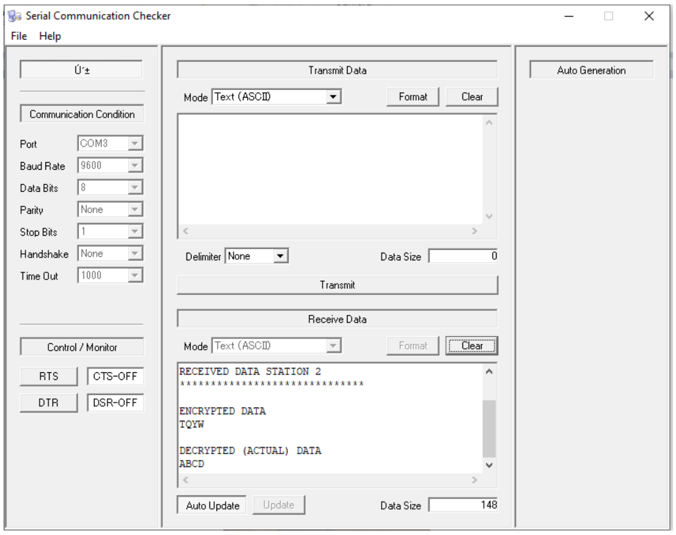
Port ----
Baud Rate 9600
Data Bits 8
Parity None
Stop Bits 1
Handshake None
Time Out 1000

Transmit Data: Mode Text (ASCII), Delimiter None, Data Size 0

Receive Data: Mode Text (ASCII), Data Size 0

RTS CTS-OFF
DTR DSR-OFF

Serial Communication Checker Window



Serial Communication Checker

Port COM3
Baud Rate 9600
Data Bits 8
Parity None
Stop Bits 1
Handshake None
Time Out 1000

Transmit Data: Mode Text (ASCII), Delimiter None, Data Size 0

Receive Data: Mode Text (ASCII), Data Size 148

```
RECEIVED DATA STATION 2
******************************

ENCRYPTED DATA
TQYW

DECRYPTED (ACTUAL) DATA
ABCD
```

RTS CTS-OFF
DTR DSR-OFF

Display Encrypted and Decrypted Data from Receiver Side

6. CONCLUSION

Cryptography is that the best method for data security Among the varied kinds of cryptographic techniques, Number of theory algorithm is that the best method. This paper will help to keep up the privacy and to stop any unauthorized person from extracting the data from the communicating. So, using this small concept, we will try to implement the algorithm for secured wireless communication over a long-distance using RF technology. This algorithm will help in obtaining the upper degree of security from terrorists, spies or the other harmful person. So, this method may be practically used to obtain important information from source to destination using RF signals.

REFERENCES

[1] Kulkarni Laxmi G, Dawande Nitin A, "Secured Communication for Missile Navigation", International Journal of Engineering Research and General Science, Volume 2, Issue 4, June-July, 2014 ISSN 2091-2730

[2] Dnyanda Namdeo Hire," Secured Wireless Data Communication", International Journal of Computer Applications (0975 – 8887) Volume 54– No.1, September 2012

[3] Anand Nayan Nagada, Pooja Vardhaman Pahade, "Secured Wireless Communication Between Remote Army Stations" IJMTER Volume 2, Issue 7, [July-2015] Special Issue of ICRTET'2015.

[4] T.Sivasakthi, S.Priyanka,V.Swathi Priya, P. Mathuvanthi," Cryptographic Based Secured Communication between Army Stations", IJERCSE ISSN (Online) 2394-2320 Vol 6, Issue 7, July 2019

[5] Juraj Dudak, Gabriel Gaspar, and Pavol Tanuska, "Implementation of Secure Communication via the RF Module for Data Acquisition", Received 28 January 2019; Revised 3 May 2019; Accepted 20 May 2019; Published 11 June 2019.

[6] 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), Volume4, Issue 1, April 2015

[7] Sana Y. Sayyed, Sayali N. Gurap, Jyoti L. Devadhe, Kajal R. Gat, "A Review On: Secure Wireless Communication For Military Application", International Journal Of Electrical, Electronics And Data Communication Issn(P): 2320-2084, Issn(E): 2321-2950 Volume-5, Issue-11, Nov.-2017