WIRELESS DATA ENCRYPTION AND DECRYPTION USING OFDM AND PIC

Vivek Raj (vivek.rajon@gmail.com), Tutan Sukla Baidya (baidya.tutan@gmail.com), Vivek Kumar (sinha.vivekon@gmail.com)

ELECTRONIC AND TELECOMMUNICATION
Bharath Institute of Higher Education and Research
BHARATH UNIVERSITY-INDIA

ABSTRACT— **The Data Communication is highly essential in the military field and especially critical during Battles. The project is aimed to protect any confidential data from the enemies. The PC encrypts the given data into pseudo random noise sequence using OFDM and Blowfish Algorithm. The communication takes place through wireless RF transmitter and receiver module operating at a frequency 433.92MHz.**

At the receiving end PIC Microcontroller is used to decrypt the receiver data into original text data. Ones the message is received the alarm indicates, so that one can know that some message is received. Then the password is entered through the keypad. Only if the Password match, the person is allow to view the data through an available LCD display.

This project is tested to operate at a maximum range of 400 feet outdoors and 200 feet indoors and it also penetrates through any obstruction such as tree, wall, etc. This system is also equipped for a secured data transmission. In order to protects the data from unauthorized person, if the four digit password is entered wrongly thrice, on the next entry on the password even through if it is correct, and the particular data received will be erased. Data reception will have to continue afresh for any further data transmission.

Keywords- **Encryption, Decryption, OFDM, PIC Microcontroller, Blowfish Algorithm.**

1. INTRODUCTION

OFDM is the short form for Orthogonal Frequency Division Multiplexing, an FDM modulation technique for transmitting large amount of digital data over a radio wave. OFDM works

By splitting the radio signal into multiple smaller sub-signals they are then transmitted simultaneously at different frequencies to receive. OFDM reduces the amount of crosstalk in signal transmission.

The need for this project arises when we want the data communication to be protected from others. This is highly essential in the military field and critical during Battle. Because during a Battle when a particular army wants to send a message to their remotely located units, which belong to the same army, in between any person can the data when it is transmitted through wireless.

Our aim of the project is to protect the data from the enemies. To accomplish this, we have used a PC as a transmitter and PIC microcontroller as a receiver station. The message to be sent is fed in to the computer for different units. The computer will encrypt the data by generating a duplicate Character with "Blowfish Algorithm" for a real one.

At the receiving end the PIC microcontroller then decrypts the Received data and display the message on the display. The communication takes place through a Wireless RF Transmitter and Receiver operating at 433.92 MHz frequency.

To ensure the security level at the receiving end we have a password protection. Once the message is received the unit will give an alarm so that one can know that the message has arrived. Then the password is entered through the keypad, and if the password matches then one is allowed to view the data.

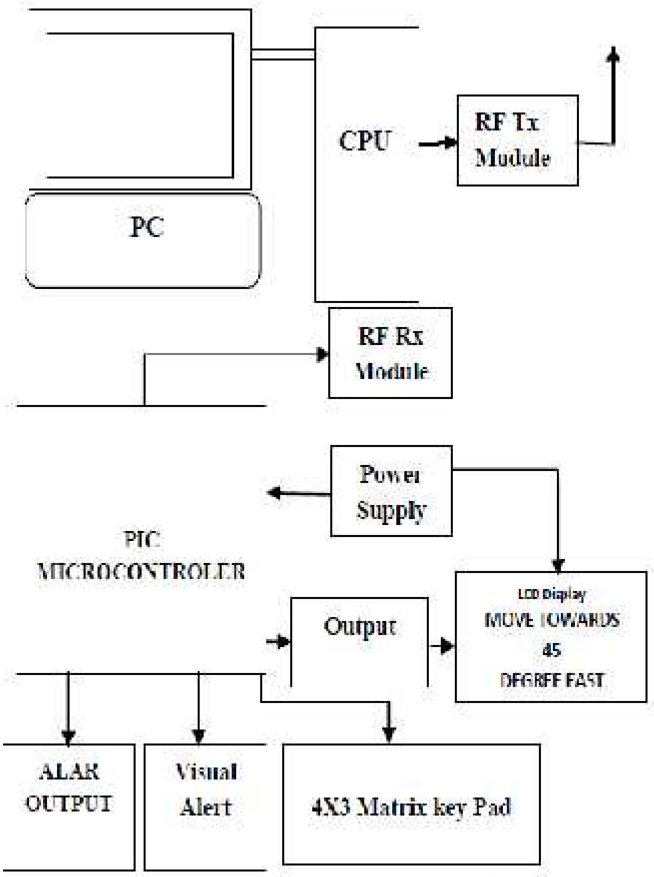

Figure:1.1 Block Diagram of the Proposed Scheme.

1.1 OBJECTIVES

The major objectives of the project work are:
1. To protect the data from unauthorized person
2. Understanding the concept of Encryption/Decryption.
3. To study the PIC microcontroller.
4. Understanding the concept of Interfacing with PC and Microcontroller.
5. Study or Blowfish Algorithm.

2. THE BLOWFISH ALGORITHM

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt the message .Blowfish is also a block cipher, meaning that it divides a message up into fixed length.

Block during encryption and decryption .The block length for Blowfish is 64 bits; message that isn't a multiple of eight bytes in size must be padded.

Blowfish is a public domain, and was designed by Bruce Schneider exclusively for use in performance-constrained environment such as embedded system. It has been extensively analyzed and deemed "reasonably secure" by cryptographic community.

Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 cycles. (Not-so-careful implementation, like Kocher, doesn't increase that time by much.) Longer message increase computation time in a linear fashion; for example, a 128-bit message takes about (2X12) clocks. Blowfish works with keys up to 448 bits in length. A graphical representation of the Blowfish algorithm is in figure 2.1. In this description, a 64-bit plain text message is first divided into 32-bits. The "left" 32-bits are XOR' ed with the first element of a P-array to create a value called P, run through a transformation function called F, then XOR' ed with the "right" 32-bits of the message to produce a new value called F'. F' then replace the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive member of the P-array. The resulting P' and F' are then XOR' ed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bits cipher text.

A graphical representation of F appears in Fig 2.2.The function divides a 32 bits input into 4 bits and uses those into an S-array. The lookup result are and added and XOR 'ed together to proceed the output.

Because Blowfish algorithm is symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plain text; for decryption, the input cipher text.

The P array and S array values used by Blowfish are recomputed based on the user's key. In effect, the uses' key is transformed into the P array and s array; the key itself discarded after the transformation. The P array and S array need not to recomputed (as long as key does not change), but it must remain secret.

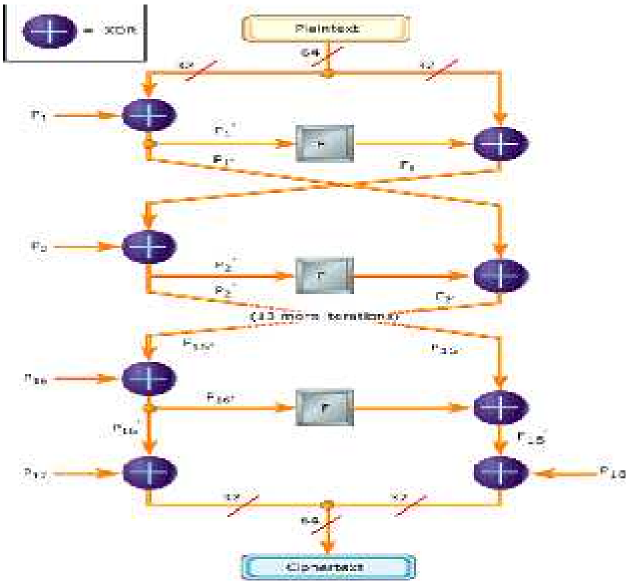

Figure: 2.1: The Blowfish Algorithm

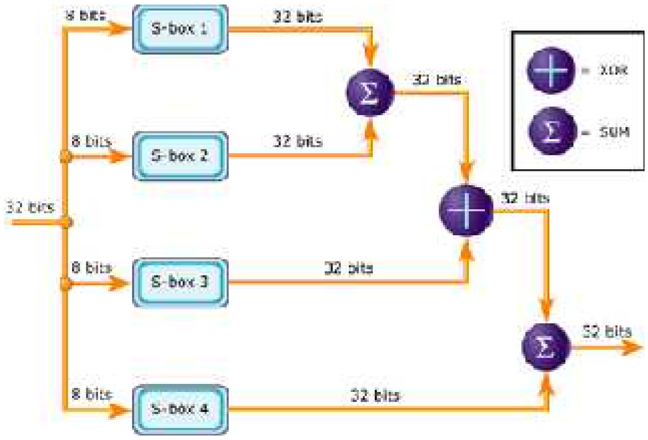

Figure.2.2: Graphic representation

3. RF MODULE

The RF module, as the name suggest, operates at Radio Frequency. The corresponding frequency range varies between 30 kHz & GHz. In this RF system, the digital data is represented as variations in the amplitude of carrier wave.

Transmission through RF is better than IR (infrared0 because of many reasons. Firstly, signals through RF can travel through larger distance making it suitable for long range applications. Also, while IR mostly operates in line-of-sight mode, RF signals can travel even when there is an obstruction. between transmitter & receiver. Next, RF signals can travel is more strong and reliable than IR transmission. RF communication uses a specific frequency unlike IR signals which are affected by other IR emitting sources.

This **RF module** comprises of an **RF Transmitter** and an **RF Receiver**. The transmitter/receiver (Tx/Rx) pair operates at a frequency of **434 MHz** An RF transmitter receives serial data and transmits it wirelessly through RF through its antenna connected at pin4. The transmission occurs at the rate of 1Kbps - 10Kbps.The transmitted data is received by an RF receiver operating at the same frequency as that of the transmitter.

3.1. RF TRANSMITTER

Radio frequency (RF) transmitter widely used in radio frequency communication systems .With the increasing availability of efficient , low cost electronic modules, mobile communication systems are becoming more and more widespread. Wireless communication systems are including cellular phones, paging devices, personal communications system, and wireless data networks, have become ubiquitous in society. A mobile terminal apparatus used in the cellular radio communication system receiver is radio frequency signal transmitted from a base stations , by a antenna , inputs the signal to receiving radio frequency unit via- antenna duplexer , high frequency amplifiers the signal, removes unnecessary waves outside the receiving band from the signal, convert the signal into an intermediate frequency signal ,demodulates the intermediates frequency signal by a demodulator , and converts the signal into a baseband signal. Generally a radio transmitter and receiver is used for performing a radio transmissions and receiving operations, whereby a high frequency signal obtained from a modulator is transmitted to un antenna to for a radio transmitter and is transmitted there from to a radio remote transmitter and receiver of the transmitted signal is receive through another antenna. The transmitting baseband signal is subjected to predetermined signal process into a modulator which modulates the carrier waves signal. The transmitter can be powered by any voltage (Vcc) between 1.5V and 12V. The higher the voltage, the stronger the RF signal becomes. Just make sure not to exceed 12V because if you do the transmitter will break, which is bad. The data that the microcontroller will be sending will go into the pin labelled "Data In" .We also learn in the datasheet that the transmitter needs 20 milliseconds to start up.

Figure: 3.1 A Typical view of RF Transmitter

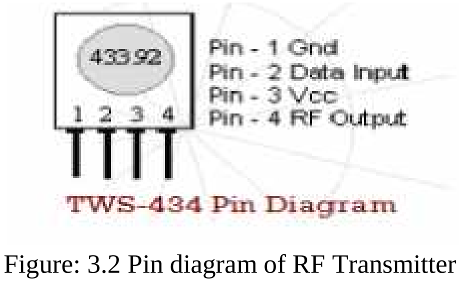

Figure: 3.2 Pin diagram of RF Transmitter

3.2. RF RECEIVER

The receiver needs between 4.5V and 5.5V to power it. This means we will be feeding the Vcc pin of the receiver (the pin that you use to power up the receiver) a regulated 5V supply. The receiver will output any data it receives through Pin 2, which is labelled "Digital Data Output". Pin 3, labelled "Linear Output/Test" is for testing out the receiver, and we will not be using it at all. It takes the receiver around 30 milliseconds to start up.

MO-RX3400-A is an ASK receiver module. The MO-RX3400-Ais based on a single-conversion, super-heterodyne receiver architecture and incorporates an entire Phase-Locked Loop (PLL) for precise local oscillator generation. It can use in OOK / HCS / PWM modulation signal and demodulate to digital signal. MO-RX3400-A had a high performance and easily to design your product.

It can be used on wireless security system or specific remote-control function and others wireless system.

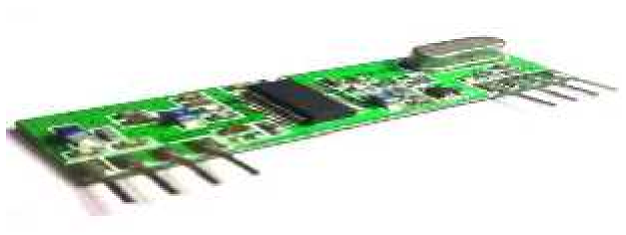

Figure: 3.3 Typical view of RF receiver

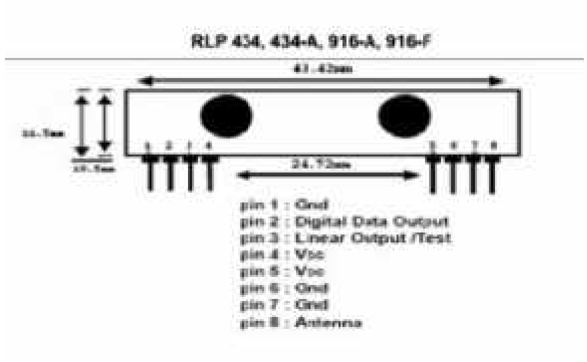

Figure: 3.4 Pin Diagram of RF Receiver

4. ENCRYPTION AND DECRYPTION PROCESS

The Encryption Technique is done by Transferring PSEDUO NOISE signal instead of Actual data.

4.1. PN SEQUENCE GENERATORS

A Pseudo-random Noise (PN) sequence is a sequence of binary numbers , eg.-+1, Which appears to be random; but is in fact perfectly deterministic, The sequence appears to be random in the sense that the binary values and groups or runs of the same binary values occurs in the sequence. A software or hardware device designed to produce a PN sequence is called a PN generator.

A PN generator is typically made of N cascaded flip-flop circuits and specially selected feedback arrangement as shown below.

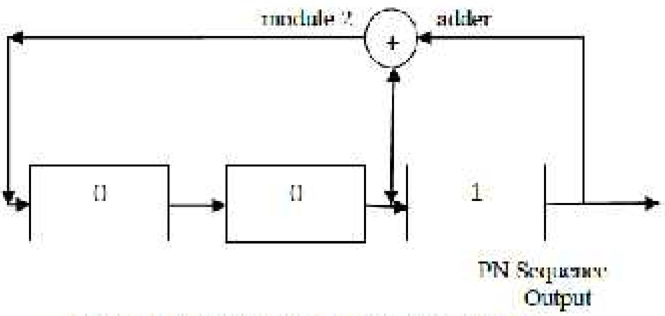

Figure.4.1: Pseudo Random Noise Generator

The flip-flop circuit when used in this way is called a shift register since each clock pulse is applied to the flip-flop cause the contents the contents of the each flip-flop to be shifted to the right. The feedback connection provides the input to the left most flip-flops.

With N binary stages, the largest number of different patterns the shift register can have is 2N. However the all binary zero state is not allowed because it would cause all remaining state of the shift register and its output to be binary zero. The all-binary-zero state doesn't cause a similar problem of a repeated binary ones provided the number of flip-flop into the module 2 adder is even. The order of the PN sequence is therefore [2N-1]

Starting with the register in state 001 as shown in 4.2, the text 7 states are 100, 00, 101, 110, 111, 011, and then 001 again and the states continue to repeats. The output taken from the right-most flip-flop is 1001011 and then repeats. With the three stage shift register shown, the period is 7. The PN sequence in general has 2N/2 binary ones and [2N/2]-1 binary zeros.

PN SEQUENCE 1

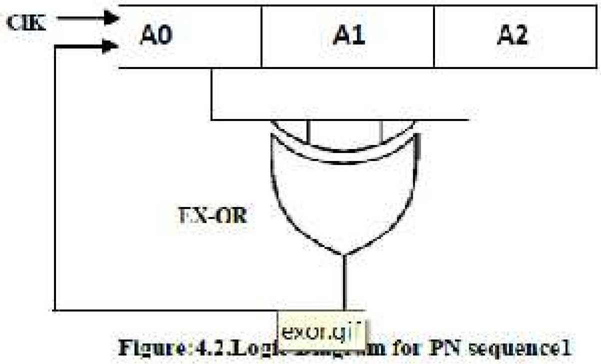

Figure:4.2.Logi[c Diagr]am for PN sequence1

PN SEQUENCE 2

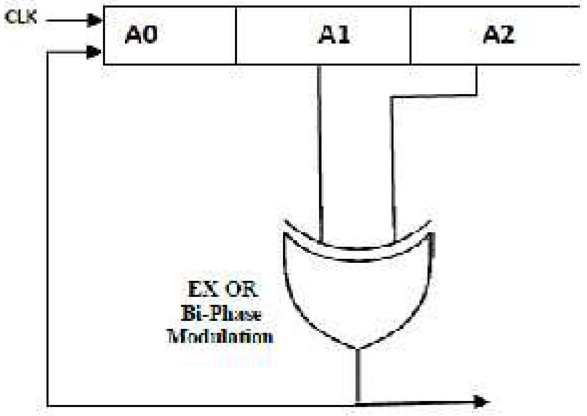

Figure4.3.Logic Diagram for PN sequence 2

5. INTERFACING

5.1 MAX 232

In RS232 there are two data lines RX and TX. TX is the wire in which data is sent out to other device. RX is the line in which other device put the data it needs to send to the device.

RS232 is a asynchronous serial communication protocol widely used in computers and digital systems. It is called asynchronous because there is no separate synchronizing clock signal as there are in other serial protocols like SPI and I2C. The protocol is such that it automatically synchronizes itself. We can use RS232 to easily create a data link between our MCU based projects and standard PC. Excellent example is a commercial Serial PC mouse (not popular these days, I had got one with my old PC which I bought in year 2000 in those days these were famous). You can make a data loggers that reads analog value(such as temperatures or light using proper sensors) using the ADC and send them to PC where a special program written by you shows the data using nice graphs and charts etc.. Actually your imagination is the limit.

One more thing about RS232. We know that a HIGH =+5v and LOW=0v in TTL / MCU circuits but in RS232 a **HIGH=-12V and LOW=+12V**. Ya this is bit weird but it increase the range and reliability of data transfer. Now you must be wondering how to interface this to MCUs who understand only 0 and 5v? But you will be very happy to know that there is a very popular IC which can do this for you! It is MAX232 from Maxim Semiconductors.

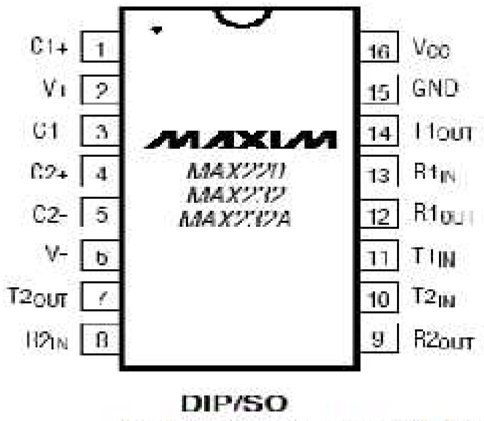

Figure:5.PIN Diagram of MAX 232

5.2 BUZZER

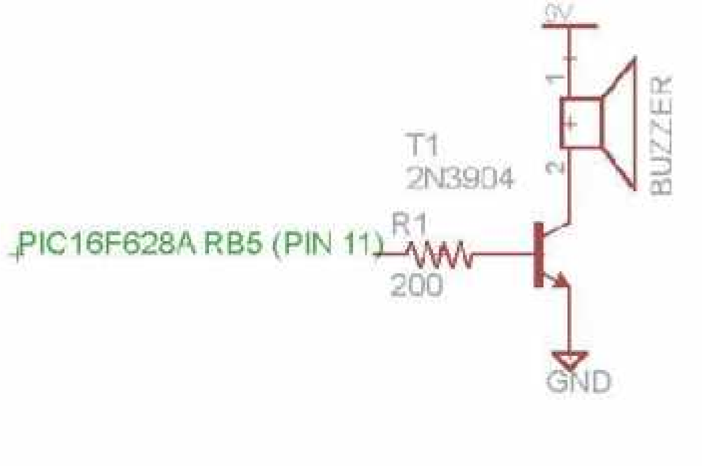

Figure: 5.1. Circuit Diagram of Buzzer

This novel buzzer circuit uses a relay in series with a small audio transformer and speaker. When the switch is pressed, the relay will operate via the transformer primary and closed relay contact. As soon as the relay operates the normally closed contact will open, removing power from the relay, the contacts close and the sequence repeats, all very quickly...so fast that the pulse of current causes fluctuations in the transformer primary, and hence secondary. The speakers tone is thus proportional to relay operating frequency. The capacitor C can be used to "tune" the note. The nominal value is 0.001uF; increasing capacitance lowers the buzzers tone.

5.3. KEYPAD

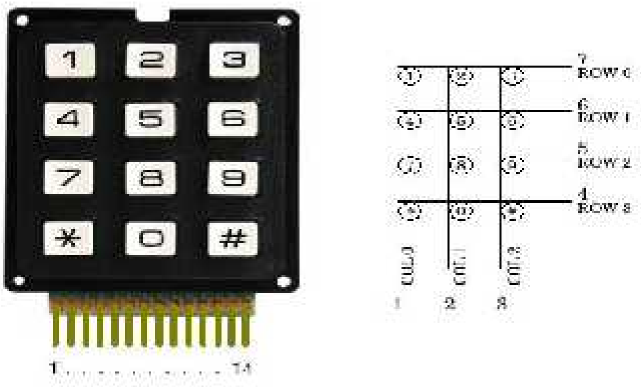

Figure: 5.3.A Typical View of 4x3 Matrixes

The Keypad library allows your Adriano to read a matrix type keypad. You can scavenge these keypads from old telephones or you can get them from almost any electronics parts store for less than $5 USD. They come in 3x4, 4x4 and various other configurations with words, letters and numbers written on the keys. This library is capable of supporting all of those.

6. PIC MICROCONTROLER

The basic building block of PIC 16F877A is based on Harvard architecture.PIC 16F877 is one of the most advanced microcontrollers from Microchip. This controller is widely used for experimental and modern applications because of its low price, wide range of applications, high quality, and ease of availability. It is ideal for applications such as machine control applications, measurement devices, study purpose, and so on.

The PIC 16F877 features all the components which modern microcontrollers normally have. The PIC16FXX series has more advanced and developed features when compared to its previous series. It has a few important features such as:

- High performance
- Only 35 simple word instructions
- fully static design
- wide operating voltage range (2.0-5.56) volts
- High sink or source current (25mA)
- Commercial, industrial and extended temperature range
- Low power consumption

Device	Program FLASH	Data Memory	Data EEPROM
PIC16F874	4K	192 Bytes	128 Bytes
PIC16F877	8K	368 Bytes	256 Bytes

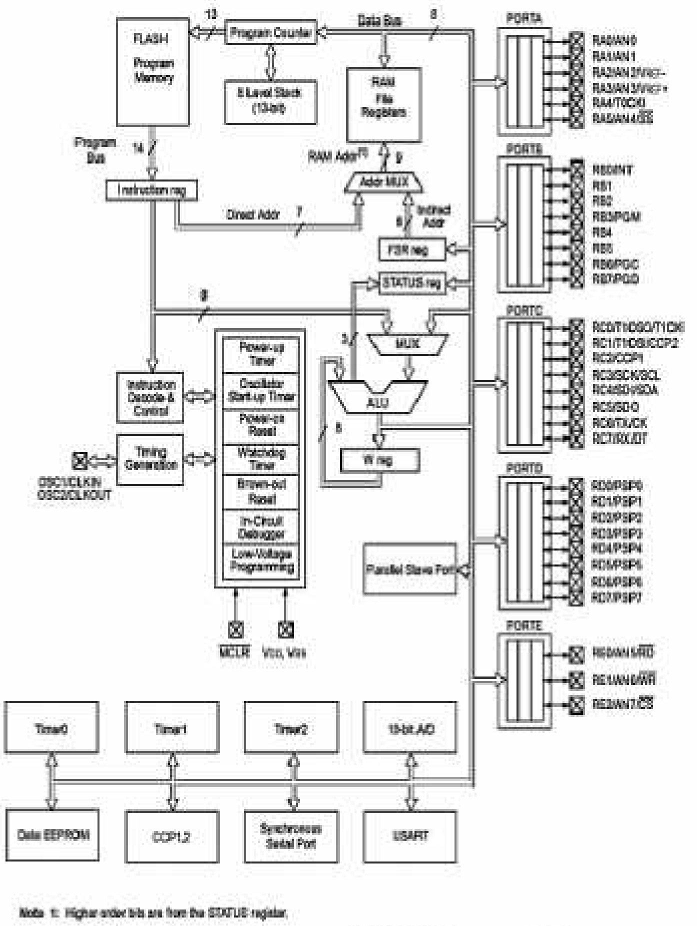

Figure: 6.Architecture of PIC Microcontroller

In order to write a program, we need a memory to run some system before interface on the IC. Program memory contains the programs that are written by the user. The program counter (PC) executes these store commands one by one. Usually PIC16F877A devices have a 13 bits wide program counter that is capable of addressing 8K*14 bit program memory space. This memory is primarily used for storing the program that are written (burned) to be used by the PIC. These devices also have 8K*14 bits of flash memory that can be electrically erasable or reprogrammed. Each time we write a new program to the controller, we must delete the old one at that time. The figure above shows the program memory and stack.

6.1. Memory Layout

The PIC16F877 has 8K £ 14-bit words of Flash program memory, 368 bytes of data RAM, 256 bytes of data EEPROM and an 8-level x 13 bit wide hardware stack. The Program Counter (PC) is 13 bits wide, thus making it possible to access all 8K x 14 addresses. The low byte is the PCL (Program Counter Low byte) register which is a readable and writableregister. The high byte of the PC (PC<12:8>) is not directly readable or writable and comes from the PCLATH (Program Counter Latch High) register. The PCLATH register is a holding register for the PC<12:8>. The contents of the PCLATH are transferred to the upper byte of the program counter when the PC is loaded with a new value. Although the PC is capable of addressing the entire program memory space, conceptually the program memory is represented by four banks of 2K £ 14-bit words. Banking is necessary since there are only 11 bits for the address in the instruction word for a call or go to. The other two bits are obtained from the top two bits of PCLATH (i.e. PCLATH<4:3>). This means that the user must set those extra bits in PCLATH before branching out of the 2K bank that contains the current instruction. Within the program memory space, the reset vector (location to go to on reset) is at 0000h and the interrupt vector (location to go to on interrupt) is at 0004h.

6.2. TXD AND RXD

Usually, a microcontroller by itself is not sufficient to perform the intended tasks. For instance, an oscillator chip is necessary to time the programmed instructions. In order to investigate the capabilities or to test a given microcontroller, obviously it is vital to build the proper circuitry. Example: potentiometer and a power supply to simulate analog inputs or LEDs to simulate the digital outputs. Hence, some hardware and software vendors provide the microcontroller with the supplementary circuit elements on the same breadboard. These boards are called Development Boards. One can also build a development board himself/herself if he/she is willing to go through the painstaking process of building the circuit.

The development board used in the series of experiments is Flash PIC development board. (Figure6.1)

It has the following features:

- RS232 through a 9-Pin D-Shell as well as screw terminals and a jumper header.
- Up to 32K words of In-System Programmable FLASH memory with up to 256 bytes of EEPROM and up to 1.5K of Internal RAM (depending on processor selection).
- Up to 8, 10 bit, Analog Inputs, using either internal or user supplied reference.
- 9 I/O controlled LEDs, 8 of which are jumper selectable.
- 32 KHz “watch” crystal for on-board Real-Time operations.
- A universal clock socket allows for “canned oscillators”, as well as a variety of crystals, ceramic resonators, and passive terminations.
- 0.1” cantered headers provide for simple connection to the processor special function pins and I/O.
- A 6-pin, ICD connection is provided for in-system programming and debugging.
- This connection is directly compatible with the Microchip ICD, ICD2 and CCS ICD-S programming hardware. Flash PICs can also be programmed through RS232 using an appropriate boot loader application.
- On-board regulation allows for power inputs from 8-38VDC with an LED power indicator.
- Termination is provided for 5VDC output at 250ma.

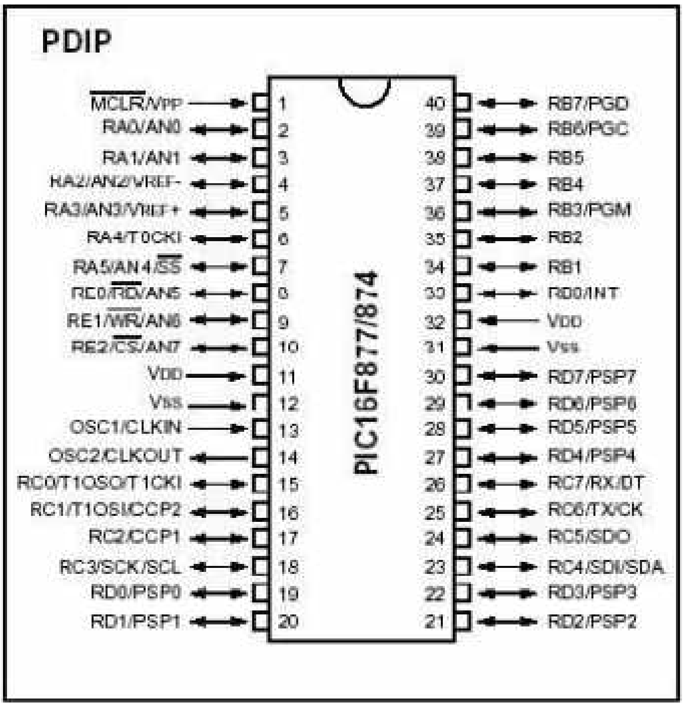

Figure: 6.2 Pin Diagram of PIC Microcontroller

7. CONCLUSION

In military applications, the secret message and information between the higher officials and governments as well as any confidential instructions to be carried out by the army battle is through secret code or highly secured communications systems. For this applications in this project, the advance multiplexing technique known as OFDM is used to protect the confidential data. This provides the desired security in data communication. Here proper authentications are needed by means if entering a 4 digit password to receive the confidential data. If not provision is also implemented in which the transmitted data is erased after several wrong tries.

The devices used are wireless and the handset are to carry to any remote locations. The radio signals are clear and the signals are received at all places even passing through any abstractions in-between. Keeping in mind the great security threat and the important of good and secured communications system, this proposed work can be utilized for the military.

8. ACKNOWLEDGEMENT

I take this opportunity to express my sincere gratitude to Principal of **Bharath Institute of Higher Education and Research** who have contributed in making the work a great success. I express gratitude to my guide. Prof. **Ralph Thangaraj** who constant help & encouragement support me to complete my work.

9. REFERENCES

[1] L. Xiao and L. Cuthbert "Improving Fairness in Relay-Based Access Network" International Symposium on Modelling, Analysis Simulation wireless Mobile System, October 2008.

[2] L. Huang, M. Rong, L. Wang, Y. Xue and E. Schulz " Recourse Scheduling for OFDM/TDD based relay enhance Cellular Network " IEEE Journal on Wireless Communication Networks, Vol. 27, PP 1544-1548, June 2009.

[3] Balraj B and Thamaraiselvi D "OFDM Based Reduction in High- Speed Wireless Communication " International Journal on Technology Today, Vol.02, PP 119-122,July 2010.

[4] Z.Han and K.J Liu "Resource Allocation for wireless Network : Basics , Techniques and Application , Published by Cambridge University Press, September 2008."

[5] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25 2008, http://www.schneier.com/blowfish.html

[6] Diaa Salama Abdul. Elminaam, Hatem Mohamad Abdul Kader and Mohie Mohamad Hadhoud3, "Performance Evaluation of Symmetric Encryption Algorithm," in IJCSNS International Journal of computer Science and Network Security, Vol.8 No.12 December 2008, PP. 280-286.

[7] www.microchip.com

[8] www.tinsharp.com

[9] www.linuxtechnology.com