Final Year Project Report

Microcontroller based secure GSM communication system (using AES encryption)

Supervised By:
Usman Akram

Project Members:

Mobeen Ahmad (01-113082-017)
Fahad Arif (01-113082-022)
Adil Zaheer (01-113082-002)

BS (ETM)
Graduate Studies and Applied Sciences

Dedication

We dedicate this project to our teachers and supervisor, as we learned a lot from them and they made us capable of achieving this goal. It is also dedicated to all the friends who stood by us and motivated us to keep going and to some senior fellows as well who gave us their precious guideline and helped us whenever we needed.

Acknowledgements

I have taken efforts in this project. However, it was impossible without the support and help of many individuals and my teachers. I would like to pay my warm thanks to all of them. I am greatly obliged to my supervisor for his direction and constant command as well as for providing essential information regarding the project & also for his support in carrying out the project.

I would like to express my gratefulness towards my parents & my group members for their help and encouragement whenever I needed which helped me in achievement of this project.

I would like to express my special appreciation and thanks to engineering persons for giving me such consideration and time.

My credit and thanks also go to my coworker in mounting the project and people who have keenly helped me out with their abilities.

ABSTRACT

This Project focuses on the security of Short Message Service (SMS) and the use of encryption to protect SMS messages. Encryption is an important factor when confidential data is transmitted over the network. The system developed for end to end secure transmission of the SMS. The algorithm used is AES (Advanced Encryption Standards) algorithm. This application is developed on PIC based microcontroller platform. The most widely used algorithm in different application is AES algorithm. We have developed a system using PIC (Peripheral Interface Controller) Microcontroller and GSM Modem platform which allows the user to encrypt the messages before it is transmitted over the network. This system provides a strong, secure, and fast encryption of the data. There is a large amount of confusion and diffusion of the SMS during encryption which makes it very difficult almost impossible for an attacker or hacker to decrypt the encryption pattern.

Table of Contents

List of Figures

Chapter # 01

Introduction

1.1 Introduction

This Project focuses on the security of Short Message Service (SMS) and the use of encryption to protect SMS messages. Encryption is an important factor when confidential data is transmitted over the network. The system developed for end to end secure transmission of the SMS. The algorithm used is AES (Advanced Encryption Standards) algorithm. This application is developed on PIC based microcontroller platform. The most widely used algorithm in different application is AES algorithm. We have developed a system using PIC and GSM Modem platform which allows the user to encrypt the messages before it is transmitted over the network. This system provides a strong, secure, and fast encryption of the data. There is a large amount of confusion and diffusion of the SMS during encryption which makes it very difficult almost impossible for an attacker or hacker to decrypt the encryption pattern. This Project focuses on the use of encryption to only secure SMS messages. The encryption requirements of voice traffic and other data traffic will not be discussed

1.2 Project Motivation

The motivation behind this project is to secure end to end communication for different people who require safe end to end communication and it might be because of their personal needs, business needs or it can be any other according to their specific requirements. So we had in our mind that we have to develop a system for secure communication using the same most common channel i.e. GSM Network which everybody is using today. As our project is GSM based it targets a very large amount of people for example there are people who are running very competitive businesses and they don’t want their rivals to know about their strategic planning and other important information so this system will give them complete safety of their information and communication.

1.3 Need for Secure data Transmission

Information security means that protective info and data systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Maintaining privacy in our personal communication are some things everybody wishes. Coding could be a means that to realize that privacy; it had been fictional for the exact same purpose. As short message service (SMS) is currently wide used as a business tool; its security has become a serious concern for business concern and customers. There’s a requirement for SMS coding so as to produce a secure medium for communication.

1.4 Short Message Service (SMS)

SMS stands for ‘‘short message service’’. Simply put, it's a way of communication that sends text between cell phones, or from a computer or hand-held to a telephone. The "short" half refers to the most size of the text messages: a hundred and sixty characters (letters, numbers or symbols within the Latin alphabet). For different alphabets, like Chinese, the most SMS size is seventy characters.

1.4.1 Working of SMS

It is well-known that SMS service could be a cellular phone feature however so, SMS also can work on different computing devices like computer, Laptop, or pill computer as long as they will settle for SIM Card. SIM Card is required as a result of SMS service wants SMS center shopper that is inbuilt on the SIM Card. As shown in figure

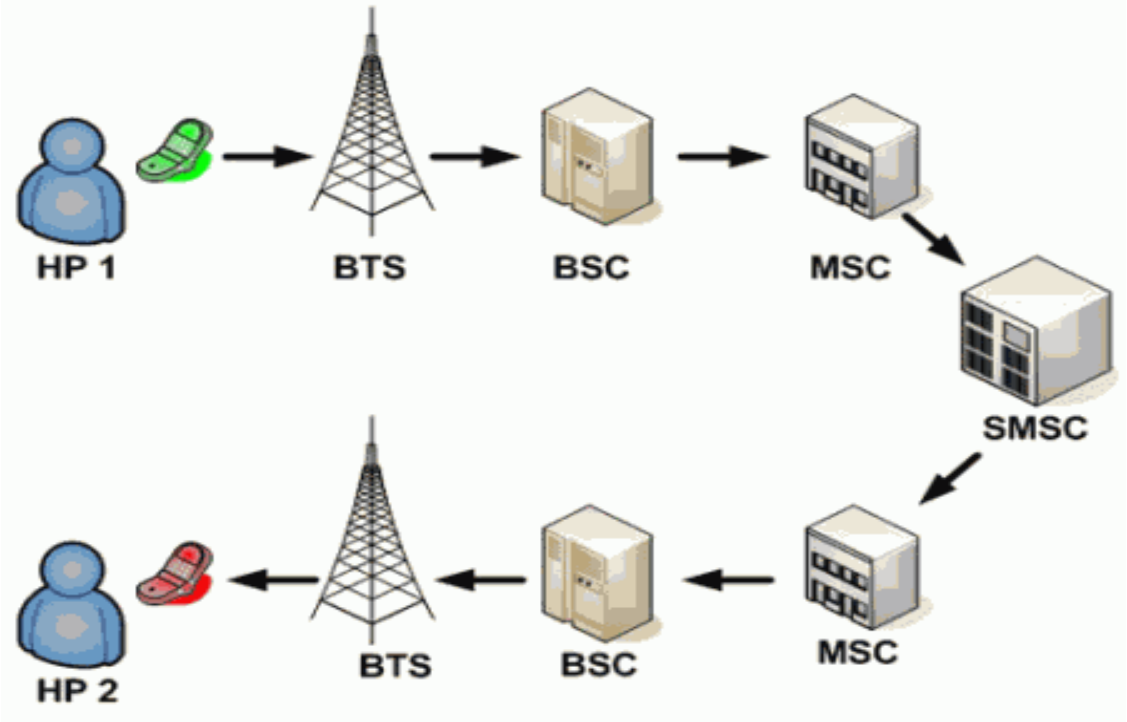


Fig. 1:1 Transmission of SMS

BTS

A base transceiver station (BTS) may be a piece instrumentation that facilitates wireless communication between user equipment (UE) and a network. UEs devices like mobile phones (handsets), WLL phones, computers with wireless net property, wireless fidelity and WiMAX devices.

MSC

The mobile shift center (MSC) is that the primary service delivery node for GSM/CDMA, liable for routing voice calls and SMS likewise as different services (such as conference calls). The Switching center sets up and releases the end-to-end affiliation, handles quality and hand-over necessities throughout the decision and takes care of charging and real time pre-paid account observance.

SMSC

When SMS is transmitted from a cellular phone, the message are going to be received by mobile carrier's SMS Center (SMSC), do destination finding, and so send it to destination devices (cell phone). SMSC is SMS service center that is put in on mobile carrier core networks. Beside as SMS forwarding, SMSC additionally acts as temporary storage for SMS messages. So, if the destination cellular phone isn't active, SMS can store the message and so deliver it once the destination cellular phone is active. As further, SMSC additionally inform the sender whether or not the SMS delivering is success or not. but SMSC cannot store the SMS message forever since the storage capability isn't unlimited. Throughout the SMS delivering, sender cellular phone and SMSC is actively human activity. So, if the non-active destination cell phones become active, SMSC directly notifies the sender cellular phone and tell that the SMS delivering is success. this is often however the SMS works normally.

1.5 GSM Network Vulnerabilities

Several vulnerabilities in the GSM network have been exposed over the past years. Most of them involve the breaking of the encryption algorithms used: A3, A5 and A8. These encryption algorithms were originally developed in secrecy and were not subjected to public review. Subsequently, when the codes for the algorithms were leaked or crypto-analyzed, vulnerabilities were found in these algorithms or in their implementations.

The A3 and A8 algorithms were mainly broken because most GSM providers use the COMP128 algorithm to implement A3 and A8. COMP128 is a hash algorithm that takes a 128-bit key (in this case Key) and a 128-bit input (in this case the random number challenge issued by the HLR) and produces a 96- bit output. The first 32 bits are used as the signed response (SRES) and the remaining 64 bits is used as input for the A5 algorithm. Once the 128-bit key for COMP128 can be derived, the SIM card can be cloned. If the SIM card can be cloned, the entire GSM authentication mechanism falls apart because the GSM network can no longer differentiated between the different users. The most recent attack on COMP128 used a partitioning attack and reduced the attack time to less than a minute. This means that an attacker only needs a minute of physical access time to derive the key and clone the SIM. Over-the-air cloning was accessed to be technically feasible by building a fake base station at a cost of about US$10K.

For the determined attacker, this is certainly achievable.

The A5 encryption algorithm is a stream cipher that protects the over-the air transmission between the ME and the BTS. The A5 algorithms are available in different versions:

- A5/0 uses no encoding.
- A5/1 is that the novel A5 algorithmic program utilized in Europe.
- A5/2 may be a weaker encoding algorithmic program shaped for send overseas and utilized in the countries outside Europe.
- A5/3 may be a well-built encoding algorithmic program that's created as a part of the third Generation Partnership Project (3GPP) for the 3G systems.

Attacks against the A5 algorithm have been published as early as 1997. In 2003, a group of researchers from Israel published practical attacks on the stronger A5/1 algorithm that could be carried out in real-time. This showed that the GSM network can no longer be relied on to provide confidentiality of information even on the radio links. The GSM standards do not impose security requirements for land line connections. Therefore, the implementation of any form of encryption on the land lines is left up to the telecommunications operators.

The GSM network can be subjected to Denial of Service attacks using electronic jammers. Since the GSM operating frequencies are known, generating a stronger radio signal to overwhelm the BTS and MS is trivial. However, a recent paper published by Pennsylvania State University described how a remote Denial of Service attack can be conducted on a GSM network by using SMS.

The idea was to flood the control channel of a particular GSM cell with SMS messages. When the control channel is overwhelmed, call establishments and roaming are severely impacted in the targeted cell.

1.6 SMS Protocol

The Short Message Service (SMS) was created as a part of the GSM section one normal. every short message is up to a hundred and sixty characters long once Latin alphabets used and

seventy characters long once non-Latin alphabets, like Arabic and Chinese, are used. SMS may be a store and forward service. In different words, SMS messages aren't sent directly from sender to recipient, however via SMS Center (SMSC). Every mobile network that supports SMS has one or a lot of electronic communication centers to handle and manage the short messages. Facts that have led to the popularity of SMS are

- SMS supports authentication of text delivery. The text sender can select to accept a revisit text back to specify whether the SMS has been delivered or not.
- SMS can be sent and acknowledged at the same time with other traffic. SMS uses the control channel as a transport mechanism, unlike voice, data and fax calls which use dedicated radio channels for the duration of the call.
- SMS compression and concatenation have been defined and incorporated into the GSM SMS standards. As such, the original 160 character limitations can be overcome.
- SMS is not bandwidth intensive. This allows telecommunications service providers to offer attractive pricing plans, which includes free SMS messages. Packages with 900 free SMS messages are offered for under USD20 in some service plans in Singapore.

Besides the technological properties, the attractive social aspect of short text messaging has also contributed to the success of SMS. Text messaging is non-intrusive and discreet, and is particularly suitable in certain social settings like meetings or social gatherings. Therefore, SMS has become the primary mode of communications for many. Besides the casual exchange of information among friends, the use of SMS has also expanded to other industries such as gaming, banking, education, remote sensor monitoring, advertising, voting, etc.

Chapter # 2

Literature Review

2.1 Background

Encryption has long been employed by militaries and governments to facilitate secret communication. Encoding is currently usually employed in protective data at intervals several types of civilian systems. as an example, the pc Security Institute reported that in 2007, seventy one of firms surveyed used encoding for a few of their knowledge in transit, and fifty three used encoding for a few of their knowledge in storage. Encoding is used to defend knowledge "at rest", like files on computers and storage devices. In recent years there are varied reports of confidential knowledge like customers' personal records being exposed through loss or stealing of laptops or backup drives. Encrypting such files at rest helps defend them ought to physical security measures fail.

Digital rights management systems that forestall unauthorized use or replica of proprietary material and defend package against reverse engineering (see conjointly copy protection) area unit another somewhat completely different example of victimization encoding on knowledge at rest. In 2010, 6.1 trillion SMS text messages were sent. This interprets into 192,192 SMS per second. SMS has become a huge business, price over $81 billion globally as of 2006. The worldwide average value for SMS message is $0.11, whereas mobile networks charge one another interconnect fees of a minimum of $0.04 once connecting between completely different phone networks. The SMS business being on such an excellent rise is prone to attacks. so it's currently become additional imperative to cipher SMS before causation. Various algorithms for encoding and secret writing are being used and implemented. Out of the whole cluster AES is the most popular.

Short Message Service (SMS) may be a text message service that allows users to send short messages to different users on the world System for Mobile communication (GSM) network. SMS uses a store-and-forward mechanism just like SMTP postal service. Rather than mail servers, SMS Centers (SMSC) store the SMS messages before they're forwarded to the mobile user's service supplier or another SMSC. though the network connections between the SMSC and nodes in a very GSM network ar typically protected by Virtual personal Network (VPN) tunnels, the SMS message hold on unencrypted at the SMSC. This suggests that workers of SMSC operators, or others United Nations agency will hack into the system, will read all the SMS messages passing through the SMSC. Several SMSC conjointly retain a replica of the SMS messages for audit, asking and dispute resolution functions. One amongst the additional

position victims of such attack in recent years was England soccer captain David Beckham, whose SMS exchange together with his personal assistant married woman Loos was intercepted and printed in a very tabloid. A couple of workers from European phone operator mmO2 were unemployed for serving to their friend acquiring copies of his girlfriend’s SMS messages.

Chapter # 03

Modern Cryptography

3.1 Modern Cryptography

In cryptography, secret writing is that the method of encryption messages (or information) in such the simplest way that eavesdroppers or hackers cannot browse it, however that licensed parties will. In secret writing algorithm, the message or info (referred to as plaintext) is encrypted victimization associate degree secret writing algorithmic rule, turning it into associate degree illegible cipher text. This is often typically through with the utilization of associate degree secret writing key that specifies however the message is to be encoded. Any individual who will see the cipher text shouldn't be able to verify something regarding the initial message. a certified party, however, is ready to decrypt the cipher text employing a cryptography algorithmic rule, that typically needs a secret cryptography key, that adversaries don't have access to. For technical reasons, associate degree secret writing theme typically wants a key-generation algorithmic rule, to at randomly manufacture keys.

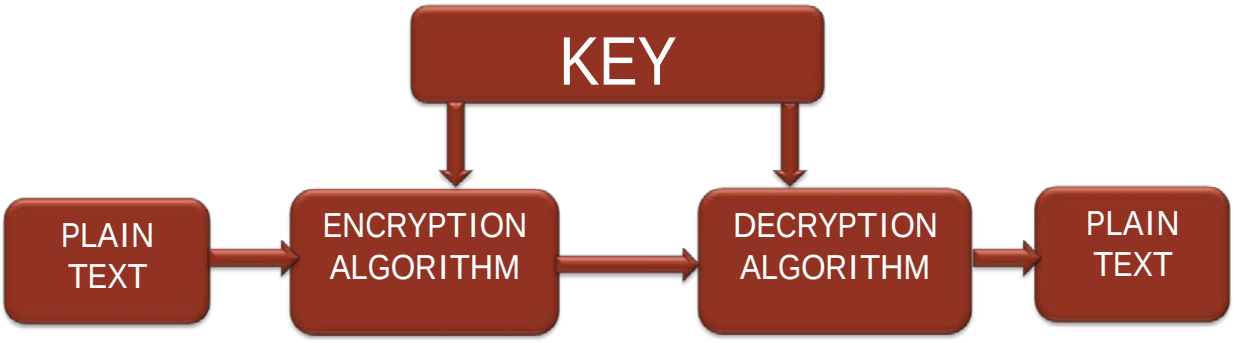


Fig. 3:1 Modern Cryptography

The "Advanced Encryption Standard'' (AES) could be a specification for the coding of electronic knowledge established by the U.S. National Institute of Standards and Technology (NIST) in 2001.Originally known as Rijndael, the cipher was developed by 2 Belgian cryptographers, Joan Daemon and Vincent Rijmen, United Nations agency submitted a proposal that was evaluated by the bureau throughout the AES choice method. AES has been adopted by the U.S. government and is currently used worldwide. It supersedes the information coding normal (DES) that was printed in 1977. The rule delineate by AES could be a symmetric-key rule, which means constant key's used for each encrypting and decrypting the information. In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year

standardization method within which fifteen competitive styles were given and evaluated, before the Rijndael cipher was elite because the best suited (see advanced secret writing commonplace method for additional details). It became effective as a federal commonplace on could twenty six, 2002 when approval by the Secretary of Commerce. AES is enclosed within the ISO/IEC 18033-3 commonplace. AES is out there in many various secret writing packages, associate degree is that the initial publically accessible and open cipher approved by the National Security Agency (NSA) for high secret info once employed in an United States intelligence agency approved science module (see Security of AES, below).

3.2 AES Rijndael Algorithm Working

The Advanced encoding algorithm includes 3 block ciphers, AES-128, AES-192 and AES-256. AES contains a fastened block size of 128 bits and a key size of 128, 192, or 256 bits. The block-size contains a most of 256 bits; however the key-size has no theoretical most. The cipher uses range of encoding rounds that converts plain text to cipher text. The output of every spherical is that the input to following spherical. The output of the ultimate spherical is that the encrypted plain text called cipher text. The input given by the user is entered in an exceedingly matrix called State Matrix.

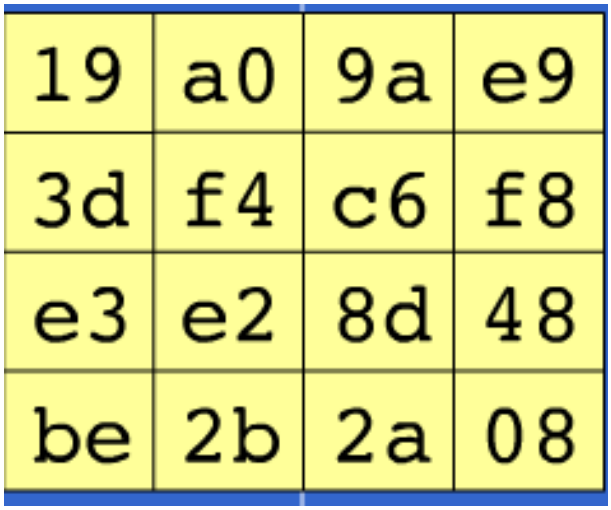


Figure 3.2: 128 Bits data in ASSCII 4x4 Matrix

AES has four types of transformations.

- Substituting the Bytes
- Shifting the Rows
- Mixing Columns
- Adding Round Keys in every round

3.2.1 Sub Bytes Step

This transformation performs Sub Bytes step of AES rule. Within the S-Box Substitution step, every computer memory unit within the matrix is organized victimization of 8-bit substitution box. This substitution box is termed the Rijndael S-box. This operation provides the non-linearity within the cipher. The S-box used comes from the inverse over GF (28), well-known to possess sensible non-linearity properties. To avoid attacks supported easy pure mathematics properties, the S-box is built by combining the mathematical function with invertible transformation. The S-box is additionally chosen to avoid any mounted points (and therefore may be a derangement), and conjointly any opposite mounted points. This step causes confusion of information within the matrix. S-Box Substitution is dispensed one by one for LPT and RPT. this is often the primary step of unvaried spherical transformation. The output of this spherical is given to successive spherical.

Figure 2.3(a): Sub Bytes Step

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Figure 3.3(b): After Sub Bytes Step

3.2.2 Shift Rows Step

Shifting of Rows is implemented on the rows of the template. It shifts the bytes at regular intervals in every row by a particular offset. The primary row remains unchanged. Every computer memory unit of the second line is shifted one position to the left. likewise, the third and fourth rows square measure shifted by 2 positions and 3 positions severally. The shifting pattern for block of size 128 bits and 192 bits is that the same.

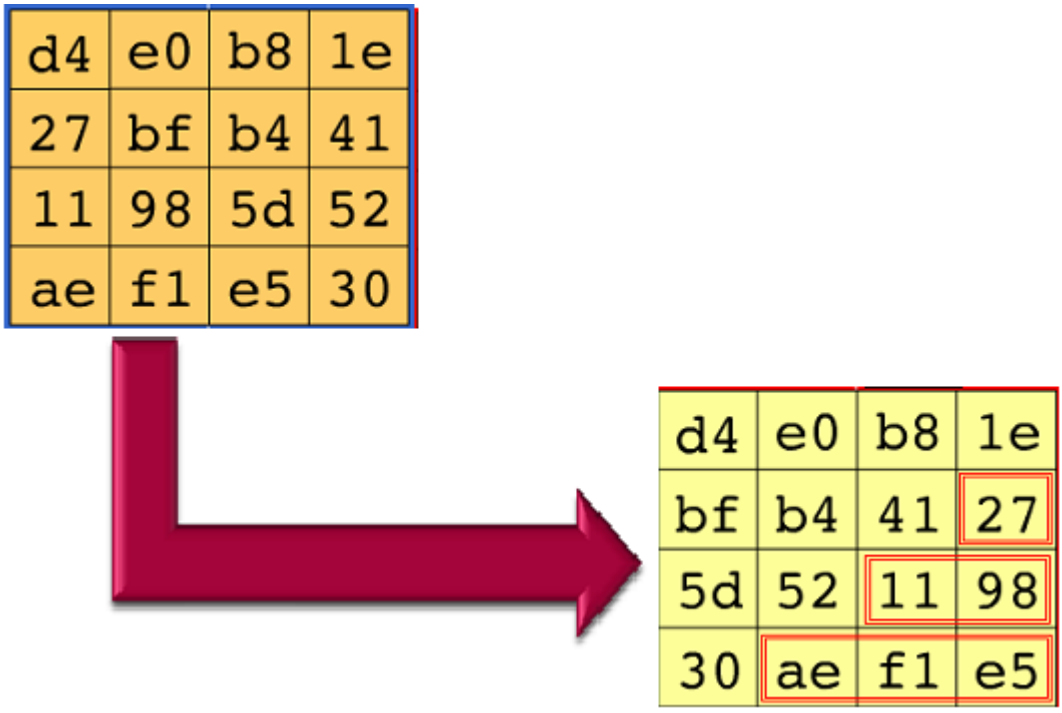


Figure 3.4: Shift Rows Step

3.2.3 Mix Columns Step

In the combine Columns step, the four bytes of every column of the state matrix area unit combined victimization associate invertible linear transformation. A arbitrarily generated polynomial is organized in an exceedingly 4*4 matrix. a similar polynomial is employed throughout secret writing. every column of the state matrix is XOR-ed with the corresponding column of the polynomial matrix. The result's updated within the same column.

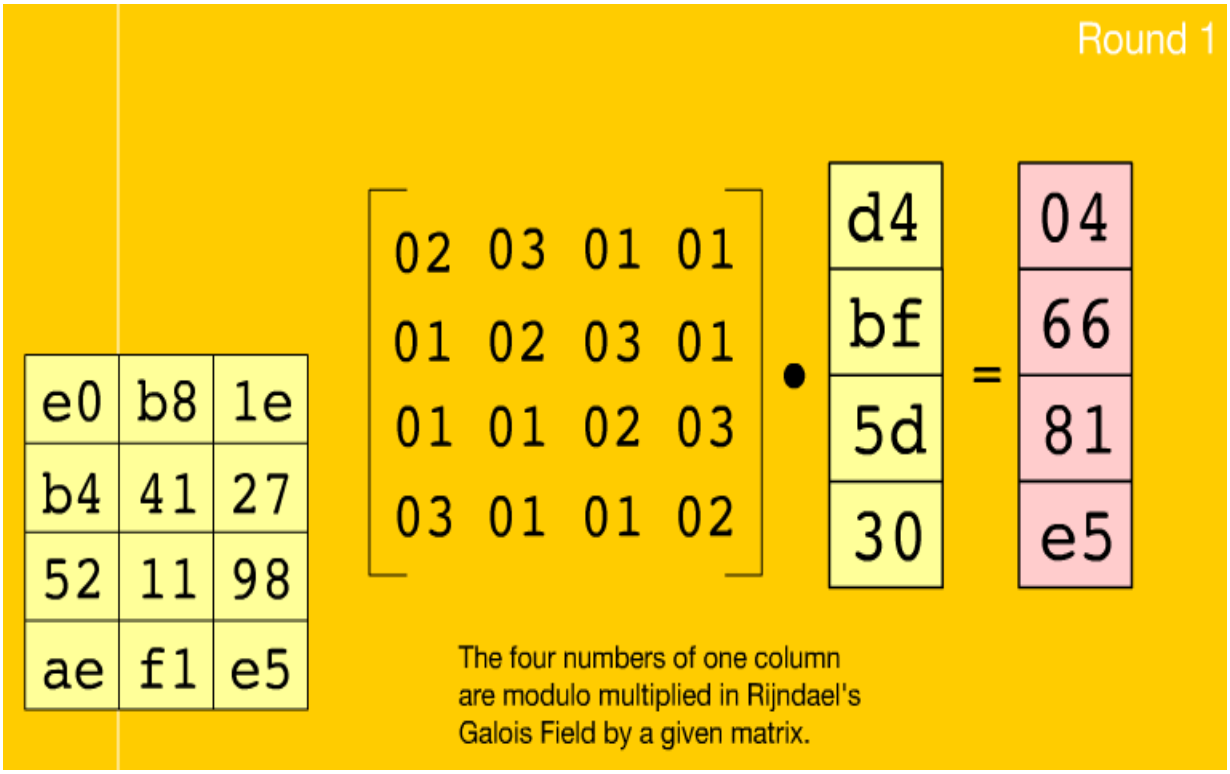


Figure 3.5(a): Mix Columns Step

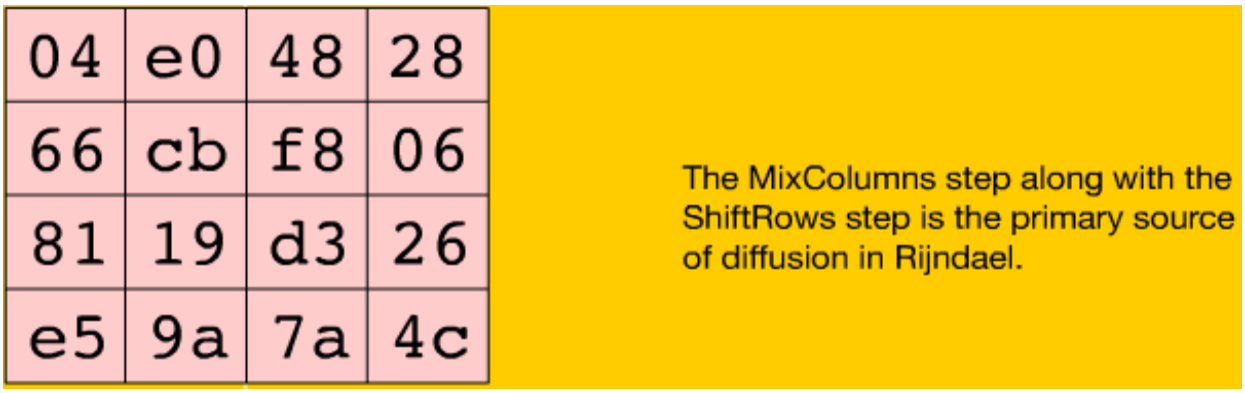


Figure 3.5(b): After Mix Columns Step

3.2.4 Add Round Key

The round key is produced by performing certain operations.

Each memory unit of the matrix is Xor-ed with the key, and a new key is produced for every new round using Rijndael algorithm.

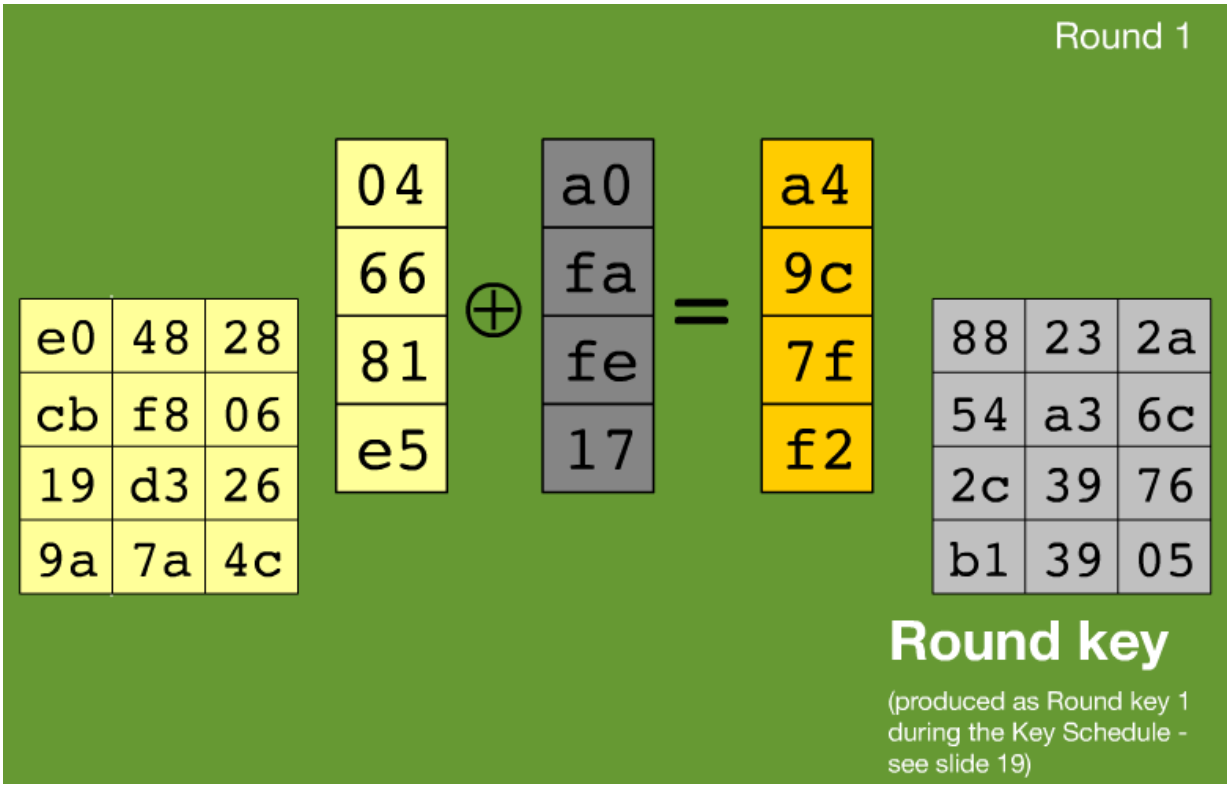


Figure 3.6(b): Add Round Key

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

Figure 3.6(b): Add Round Key

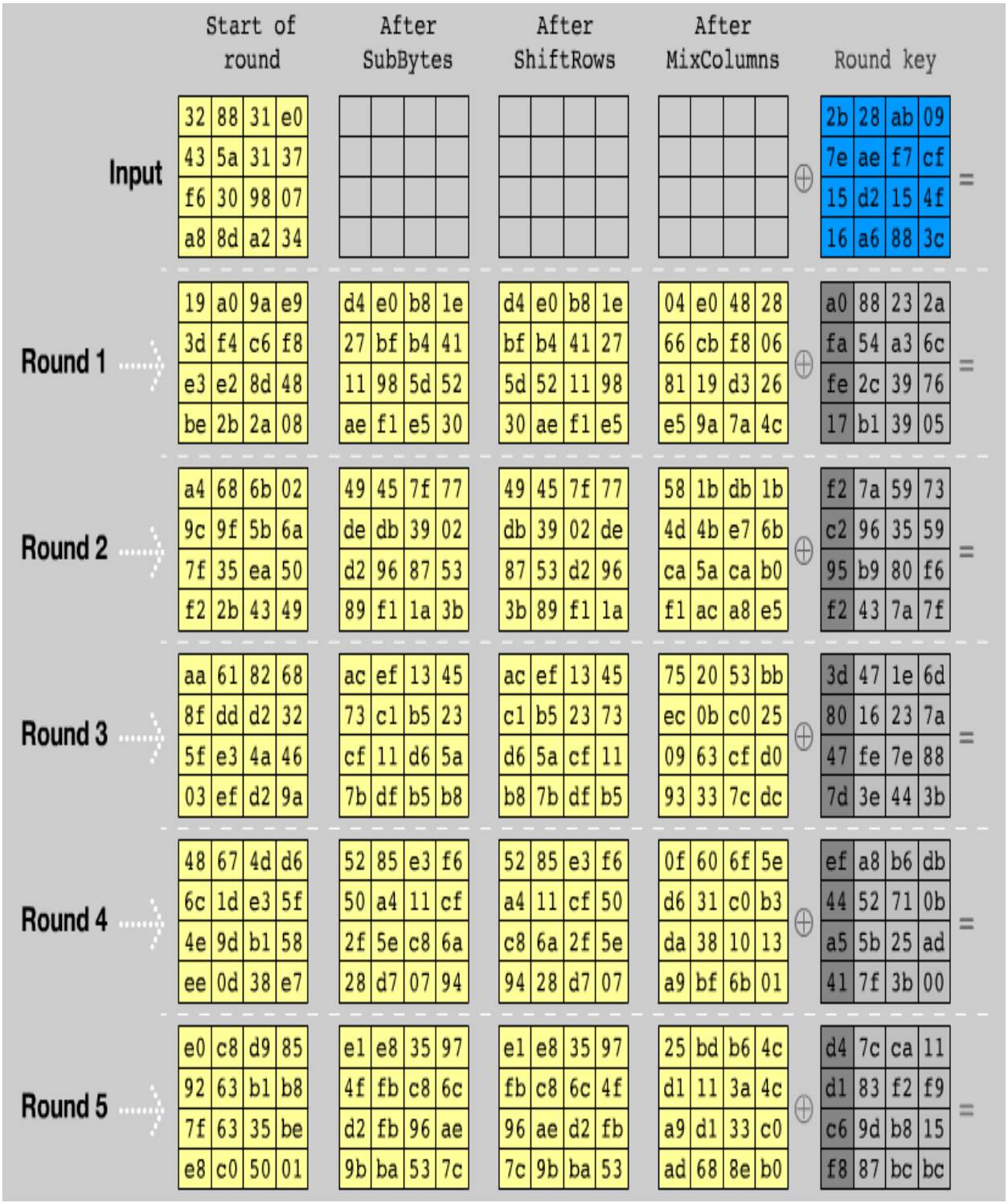


Figure 3.7(a): First 5 Rounds

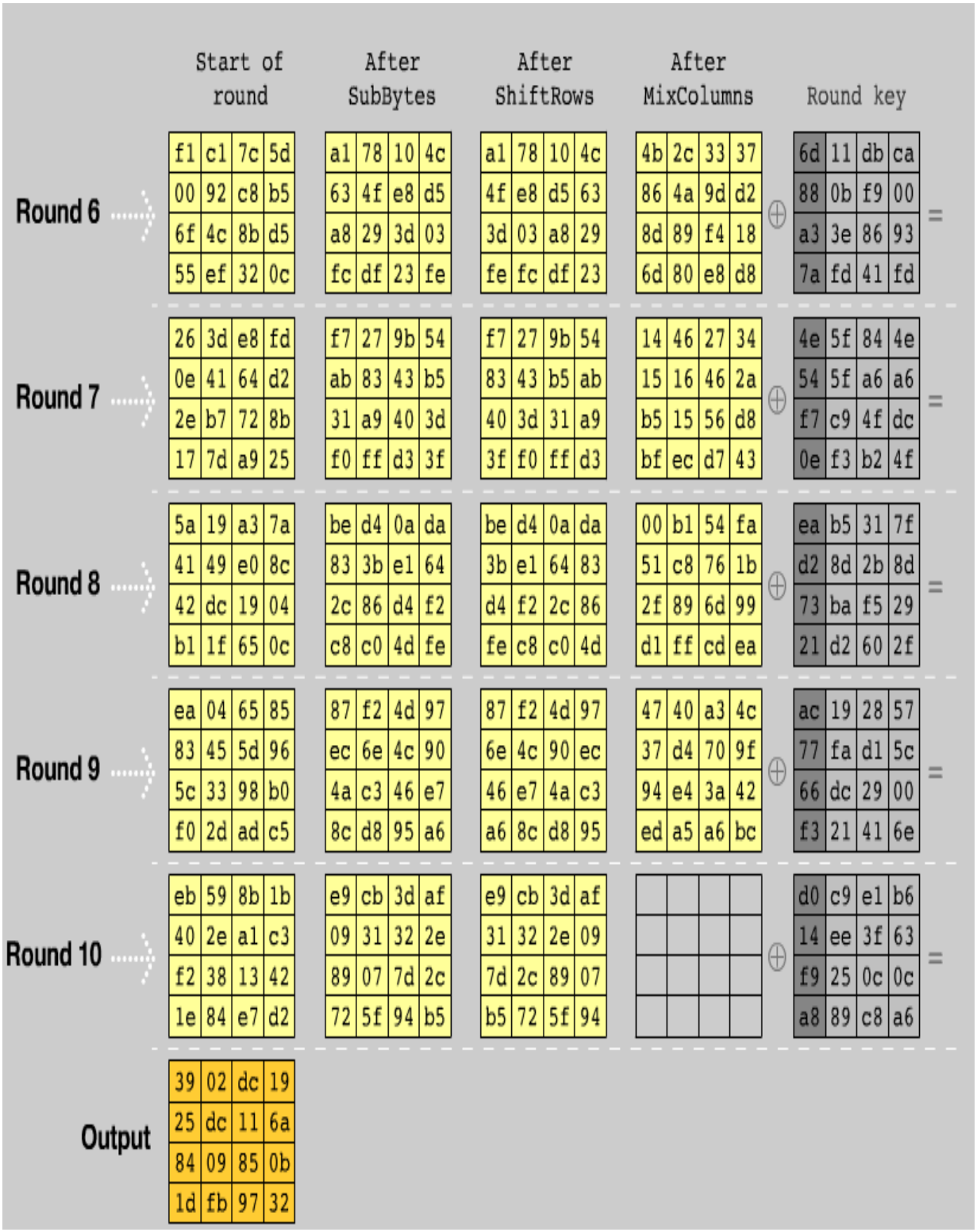


Figure 3.7(a): After all Rounds

3.3 Decrypting the Algorithm

The cryptography formula is noted because the cipher and also the cryptography formula is used as the inverse cipher. Additionally, the cipher and also the inverse cipher operations should be dead in such the simplest way that they cancel one another. The rounds keys should even be utilized in reverse order. The Cipher Text that is created of 128-bit 4*4 Matrix is that the input for the cryptography method.

Chapter # 04

Project Requirements & Specification

Project Requirements & Specification

4.1 Hardware Project Requirements

PIC16F877A Microcontroller

GSM Modem

LCD Alphanumerical 16x2

Keypad

Serial Cable

4.1.1 Microcontroller PIC16F877A

The microcontrollers which are very extensively used particularly in industries, automotive, consumer and appliances applications are PIC microcontrollers. The obstruct figure of PIC16F877a is given below:

Reason of using PIC

There are numerous reasons meant for which we favor PIC microcontroller more than ATMEL. A number of the reasons are underneath.

• PIC has incorporate ADC's that prevents the hardware complexness

• its design is far stronger then ATMEL that's why it doesn't burn thus typically.

• It is wide utilized in industries.

• It has incorporate watch dog timer, EEPROM and PWM etc. that makes it additional competent then ATMEL.

• PIC design relies on RISC (reduced instruction set computer) structural design, whereas 8051 have CISC (complex instruction set computer) design.

• If we have a tendency to mention instruction set of micros then 8051 has 250 directions that take one to four machine cycles to execute, whereas PIC has nearly forty directions that's nearly four cycle instruction.

• In ATMEL one clock cycle divide the clock frequency by twelve, whereas in PIC one clock cycle divide the clock frequency by four, thus on this base we are able to safely say that PIC is

far quicker then ATMEL.

• If we have a tendency to use twelve megacycle per second crystal in ATMEL 8051 and PIC then the speed of execution are going to be.

8051= 12MHz/12 = I megacycle per second, that is adequate to one million directions per second.

PIC = 12MHz/4 = three megacycle per second, that is three million directions per second.

• 8051 consumes additional power then PIC.

• 8051 has the commands that will additional complicated calculations, whereas in PIC there's straightforward single direction and technologist should tell each step to urge the result.

Kinds of PIC

Usually PIC microcontrollers are divided into major groups:

1. 8 bit microcontrollers

2. 16 bit microcontrollers

Each kind is additional divided into a lot of product, as shown within the higher table. Now the microcontrollers from PIC10 to PIC fourteen known as low level microcontrollers. And PIC16 and PIC18 had known as middle level microcontrollers. Whereas sixteen bit microcontroller family is known as high finish microcontrollers.

Most of scholars and works use the middle level microcontrollers and even among them the foremost standard and often used microcontroller is PIC16F877A (we conjointly used this microcontroller thanks to its wide features).

The way of selecting a suitable microcontroller

Each and every microcontroller has its distinctive variations and separate options. However selecting applicable microcontroller wants a large call. For that you simply ought to raise some inquiries to yourself i.e.

• Does the project wants analog input or digital?

• How several I/O pins square measure required?

• Does your project have the necessity of precise timing?

• How abundant the memories will your project requires?

• Does your work want a serial I/O?

• Does your work require digital input or output?

Observing all the above questions we are determined to choose PIC16F877A microcontroller. Underneath is the detail of PIC16F877A microcontroller:

Features of PIC16F877A Microcontroller

It has too several options that it's wide used a number of the options square measure below:

It has solely thirty five words instruction to find out

• 8 rank profound hardware heap.

• extremely far above the ground performance computer architecture CPU

• straight, circuitous and additionally virtual addressing modes

• disrupt ability

• Power on retune (POR)

• Power awake regulator

• Oscillator pop out clock

• supervisory body instance having its individual on chip generator

• Power reduction the inactive mode

• Selectable the generator choices

• Pin out well-matched to the 16C73B/74B/76/77

• completely static style

• In circuit sequential programming (ICP)

• Single 5 five potential unit in circuit sequential programming potential

• High supply current twenty five ma

• Low power utilization

• Programmable set of laws shield.

• suspend capacity

• working pace DC twenty megacycle timer input

• In route debugging via 2 pins

• mainframe scan write admission to plan memory.

• Industrial, business and extensive high temperature ranges

• extremely wide in operation power vary a pair of.0 potential unit to five.5 volt

Diagram showing Pin Configuration

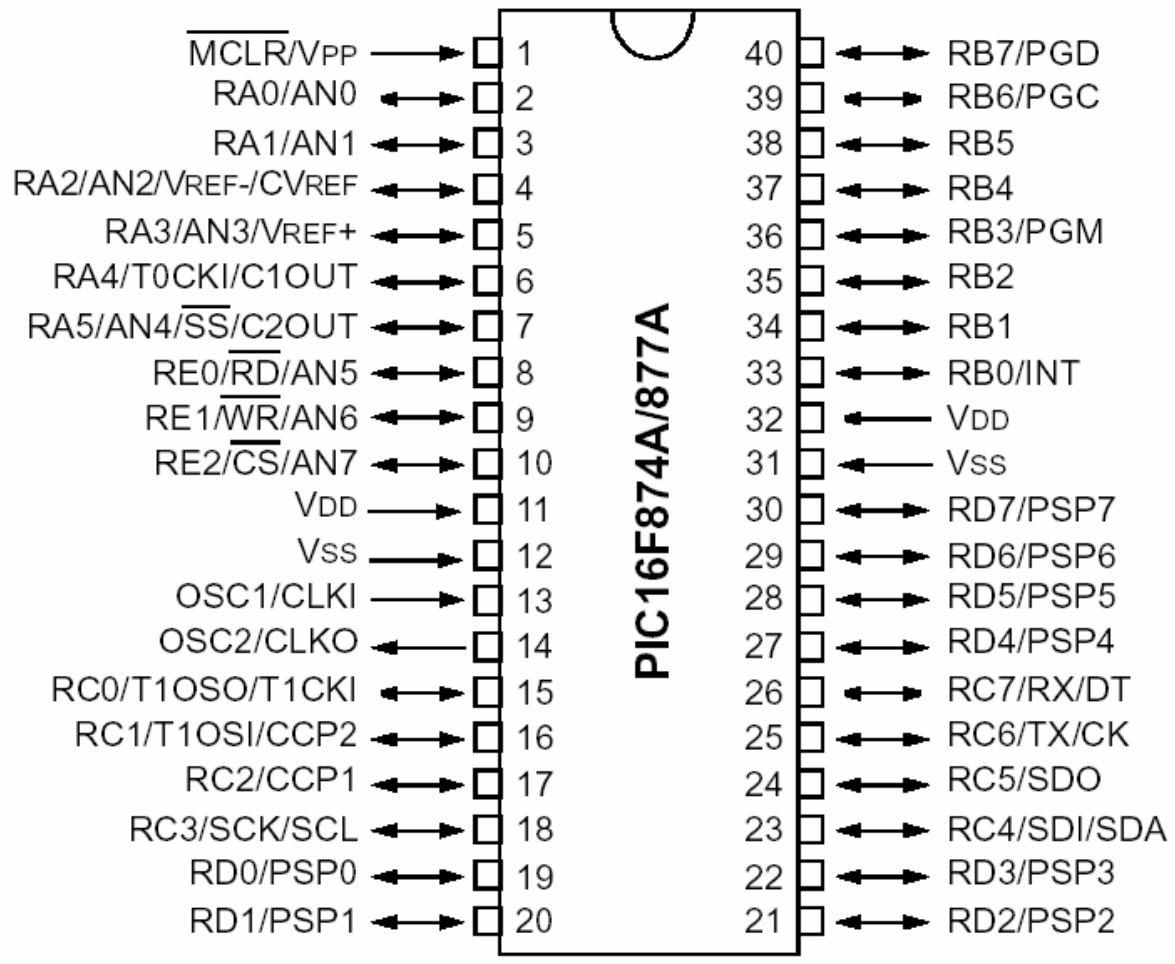


Fig 4.1 pin diagram of PIC16F877A microcontroller

Peripheral functions

Peripheral feature of this controller is numerous that's why it is widely well-liked in the midst of students and additional departments such as industries and further applications. A number of the functions are below,

• Timer zero eight bit clock and counter through eight bit pre scalar.

• Regulator one sixteen bit clock, counter having pre scalar, it may be added throughout sleep by means of additional timer.

• 10 bit multi control analog to digital convertor

• synchronized port

• “USART” (universal synchronous asynchronous receiver transmitter) with nine bit address recognition.

• PSP(parallel slave port) eight bit extensive with outside RD,WR and cesium controls (40/44 pins solitary)

• Brown out uncovering trail for brown out reset (BOR)

• Capture is sixteen bit and most resolution is twelve.5 ns

• Compare is additionally sixteen bit and most resolution is two hundred ns

• PWM most resolution is ten bit

There is a distinction of box up designator of PIC16F877A in terms of total miss (g) and range of pins.

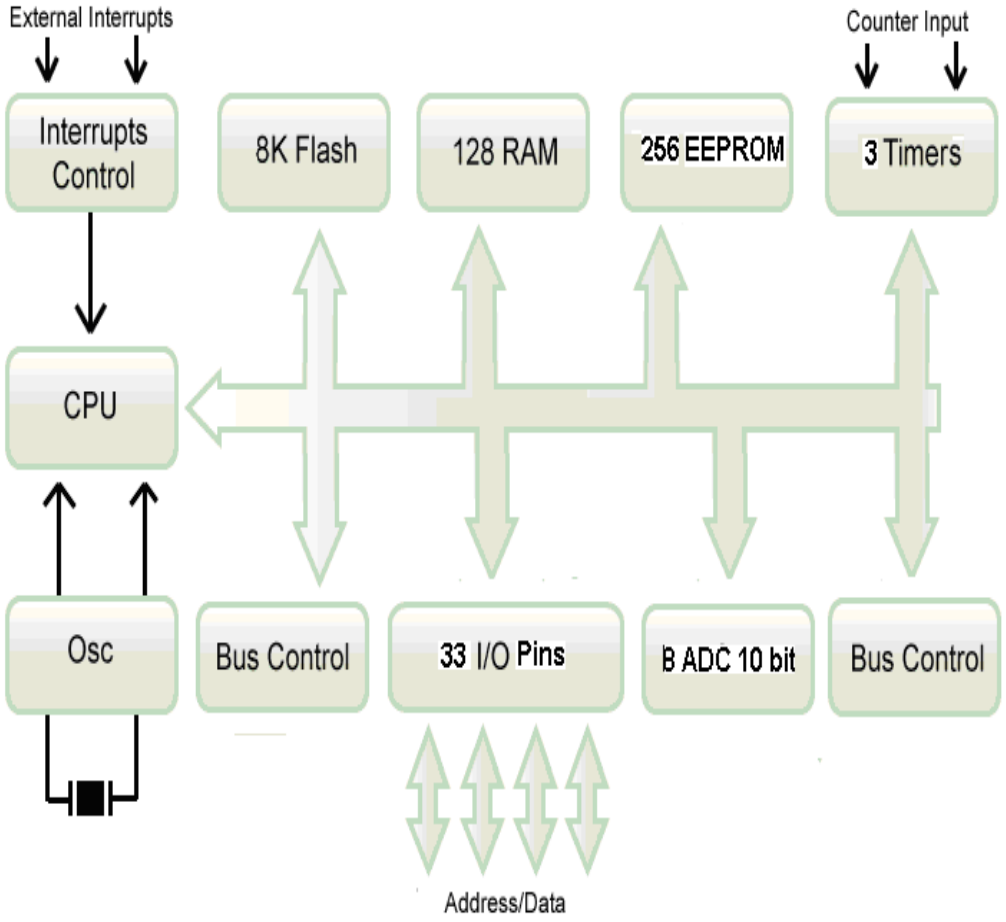


Figure 4.2: Block Diagram of PIC 16F877A

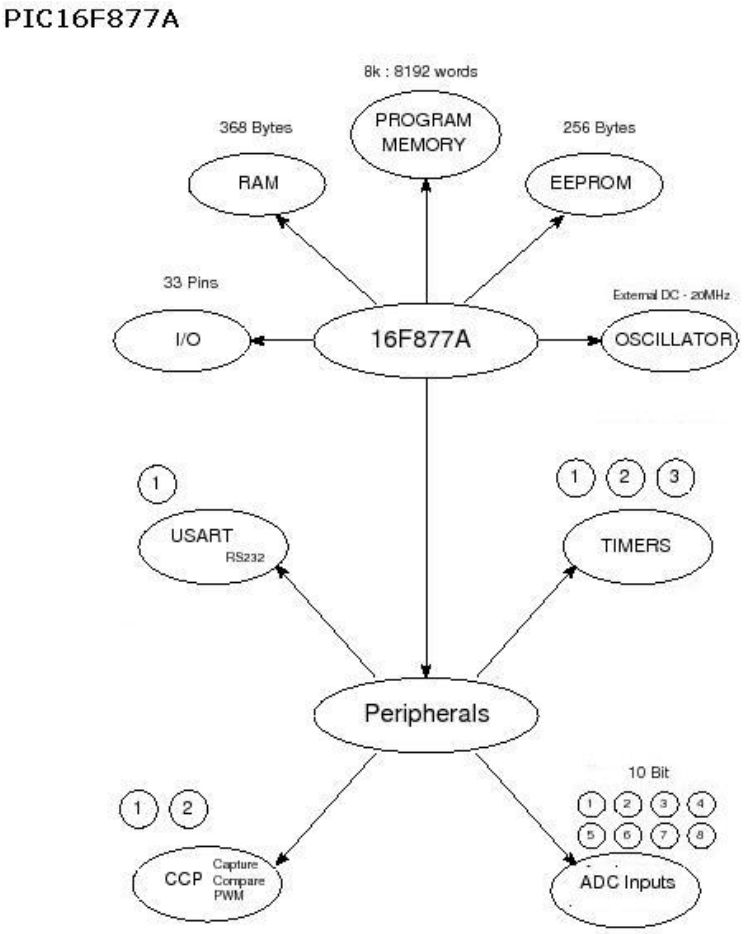


Figure 4.2: Block Diagram of PIC 16F877A

4.1.2 GSM Modem Sim300

Considered for international market, SIM300 may be a Tri-band GSM/GPRS engine with the aim of working on frequencies EGSM 900 megacycle, DCS 1800 megacycle and PCS1900 megacycle. SIM300 provides GPRS multi-slot category ten capabilities and support the GPRS writing schemes CS-1, CS-2, CS-3 and CS-4.
With a small configuration of 40mm x 33mm x a pair of.85 mm, SIM300 will match most the house demand in your application, like good phone, PDA phone and alternative mobile device. The physical interface to the mobile application is formed through a sixty pins board-to-board instrumentality that gives all hardware interfaces amongst the unit and customers' boards apart from the RF transmitter interface.

- The keyboard and SPI liquid crystal display interface can offer you the pliability to develop made-to-order applications.
- Two serial ports will assist you simply develop your applications.
- Two audio channels embrace 2 microphones inputs and 2 speaker outputs. This could be simply designed by AT command.

SIM300 give RF aerial interface with 2 alternatives: aerial connective and antenna pad. The aerial connective is MURATA MM9329-2700. And customer's aerial may be soldered to the aerial pad. The SIM300 is intended with power economy method, this utilization to as low as twenty mA in SLEEP mode. The SIM300 is integrated with the TCP/IP protocol Extended TCP/IP AT commands area unit developed for purchasers to use the TCP/IP protocol simply that is extremely helpful for those information transport applications.

Principle ofAT Command:

The ''AT '' or ''at '' prefix should be set at the start of every line. To finish an instruction, a character should be inserted. Instructions are typically followed by a reply that features ''. In most a part of this document, solely the responses is indicated, the characters are omitted by choice.

Four sorts of extended AT commands implemented:

Test Command	AT+CXXX=?	The equipment returns the list of parameters and values ranges set with the with the corresponding Write command or by internal processes.
Read Command	AT+CXXX?	This command returns the currently set value of parameters.
Write Command	AT+CXXX=<…>	This command sets user-related parameter values.
Execution command	AT+CXXX	The execution command reads non-variable parameters affected by internal processes in the equipment.

Table 4.1 At Commands format

As soon as you provide a series of AT instructions on detached lines, it's powerfully suggested to depart a disruption among the prior and also the subsequent instruction till the ultimate reply (OK or Error message) seems.

It avoids causing too several AT instructions at an instance while not anticipating a reply for every.

Check the Availability of a Modem:

Now that we have connected G1000 with our Computer and started a terminal application and learnt the principle of AT Command, its time to verify our connection

To check the availability of a modem we just have to enter “AT” command in HyperTerminal And the modem will reply “OK”, if the modem is connected

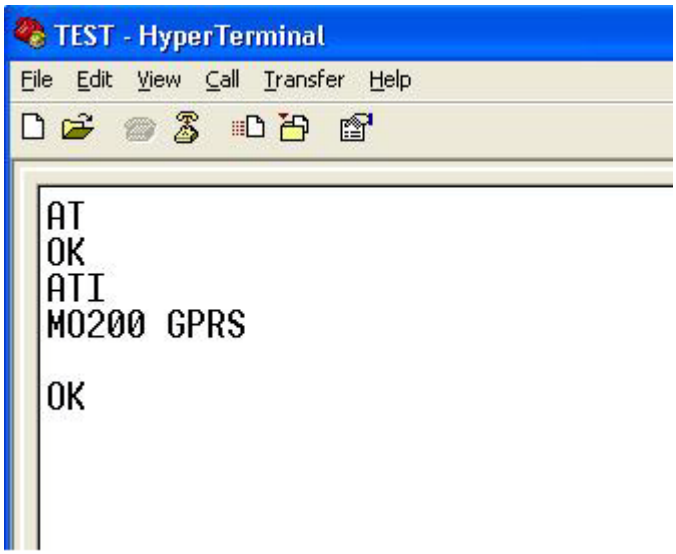


Fig 4.3 At Command

Go to HyperTerminal and type **AT** and press **ENTER.**
SM Modem will respond with **OK**

It will verify that some modem is connected with our COM port, now we will enter the “ATI” command to check the identification of the Modem and verify that its G1000’s GSM modem

Now in HyperTerminal type
ATI and press **ENTER.**
GSM Modem will respond **MO200 GPRS** and **OK**

Now it’s verified that the modem is connected and the modem is G1000’s GSM Modem.

It is advised that before starting any experiment the availability of the modem should be checked with this method.

In case if the modem does not respond, verify the following steps

- Check if the G1000 is switched ON
- RS-232 Cable is connected with G1000 and Computer
- Verify that the COM port with which the Serial Cable is connected is the same used in the HyperTerminal “Connect To” step.
- If the power adaptor is not connected it is possible that the battery is weak, please attach the power adaptor to make sure that the battery power is enough to operate the G1000.

4.1.3 LCD 16×2

LCD sixteen*2 may be a usually used LCD apparatus and it consists of sixteen pins two rows and 16 columns (16 characters per row). These pins are available put together split in 2 sides with both sides having sixteen pins.

It operates on a four bit function mode. Four pins are utilized to carry information with every pin carrying one bit at a time. For this purpose we've got elect the PIN eleven, 12, 13,14of LCD connected to the PIN thirty one, 32, 33, and 34 of PIC controller. The pin configuration of pins that we tend to utilize is delineated below.

- **Pins eleven, twelve, thirteen, fourteen (Data Lines).**

Four bit data bus is linked to these pins. Each of them take 1 bit of data from least important bit to mainly important bit departing from first to last pin.

- **Pins four, five, six (Control Lines).**

The above mentioned lines are control lines, they inform about control sense on LCD. We are going to utilize pin four and five and attach it to PIC controller’s pin number nineteen and twenty correspondingly. These are the pins who inform LCD about the action to be taken. Pin six is grounded.

- **PIN two Vdd.**

We use Pin number two to apply voltage to the device.

- **Pin one (Vss) and Pin three (VD).**

A resistor of 1.2k is attached to pin three in the figure below.

- **Pin seven, eight, nine and ten.**

Generally the above mentioned pins are grounded and we also attached them to ground in our project as it is shown below in the figure.

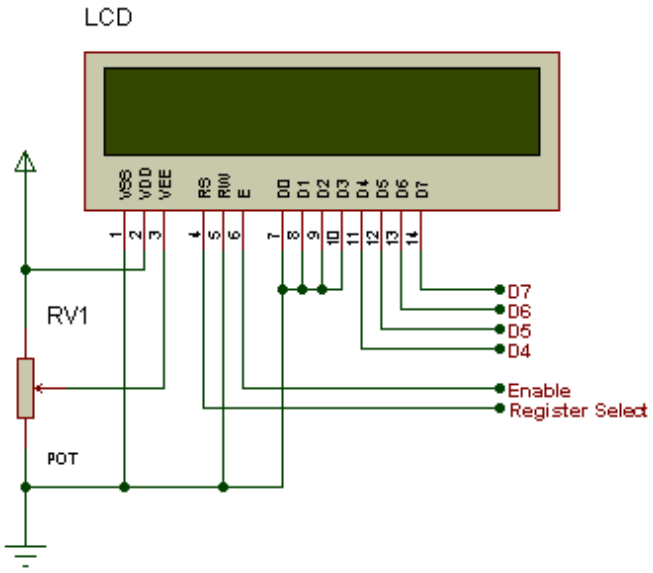
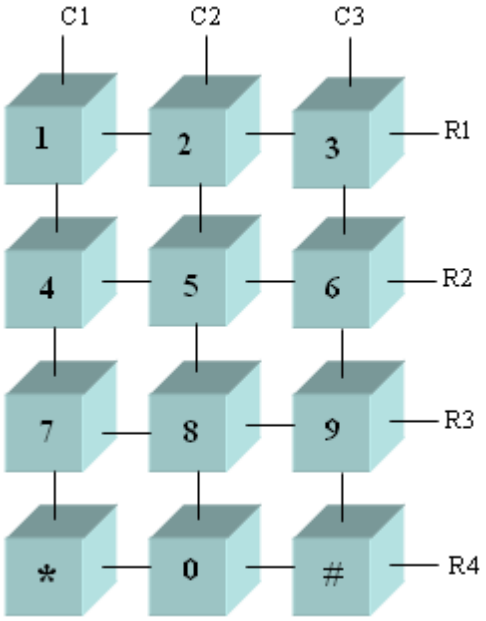


Fig 4.3 LCD 16×2

4.1.4 Keypad 4x3

Keypad is an array of switch. There will be 2 wires connected each time a button is pressed. For example; when button '1' is pressed, pin1 and pin5 is connected. There is no connection between rows and also columns. The button makes it connect. They are many types of keypad. Different types of keypad sometimes come from different manufactures. And it maybe has different pin connection. User is advised to check pin connections before use.

The keypad's pins need to be pulled up or pulled down to avoid floating case. Pull up normally connect to 5V and pull down is connect to ground. Pins of the keypad can straightforwardly be attached to the controller.



Pin	1	2	3	4	5	6	7	8
Column/row	C1	C2	C3	R1	R2	R3	R4	NC

*NC is not connected

Fig 4.4 Keypad 4x3

4.1.5 Serial Cable

What Serial Communication is?

Serial communication is methodology of transmission knowledge between a laptop and another laptop or any tangential devices like a programmable computer, a modem, a copier, or the other instrument. Serial communication uses a transceiver, source sends knowledge one bit at an instance to a recipient over one communication line. Once the speed or speed of transferring knowledge is slower than this methodology is getting used .And additionally after we wish to transfer knowledge during a longer distance. In serial communication solely a cable is needed to attach 2 Pc's along and it needs no further hardware. This is often additionally a reason why it's

unremarkably used method. Most of the computers have either one or might have over one interface.

When a bit is sent serially, it is placed into a bit frame. This frame consist of a begin bit that is backed up by real message bits. Then next involves the parity that can or can't be included and then it is backed up by a finish bit.

The following figure 4.2 is showing a letter m encoded in a character frame.

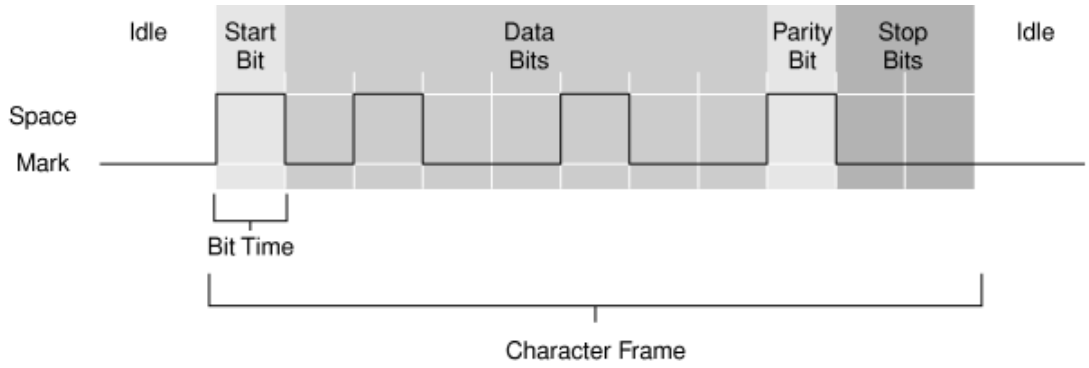


Fig 4.5: Encoding of a letter in character frame.

Standard of the Serial interface

Numerous dissimilar standards of port communication are obtainable .Discussing the foremost common, TIA/EIA-232C commonplace specifies the port interface revealed by Telecommunications business Association. RS-232 is that the abbreviation for suggested commonplace range 232. It describes the initial commonplace for port interface. The RS-232 commonplace consists of distinctiveness of electrical signal like voltage levels. Conjointly consists of interface mechanical characteristics like connectors. Practical description of interchange circuits like every electrical signal functions, and a few techniques for common sorts of terminal to electronic equipment connections. There are other EIA serial communications standards obtainable like RS 423, RS 449 and RS 442 that relates to RS 232.

Serial communication parameters

The parameters which must be kept in mind are following.

- Transmission Baud rate.
- Quantity of data bits encoding.

- How the parity bit can be used.
- How many stop bits will be required?

Baud Rate

Baud rate could be a parameter for measurement how briskly the information is moving between devices that use serial communication. 2 voltage states utilized by RS-232 interface are known as MARK and house. During this style of committal to writing theme, the information measure is same as most range of bits of knowledge additionally together with management bits that are transmitted per second.

Figure 4.2 shows the perfect signal. MARK depicts negative voltage, and house depicts positive. Following is that the truth table for RS-232

Signal>3V=0

Signal>-3V=1

The resultant signal level is sometimes between the vary of +12 V and -12 V and also the dead space between +3 V and -3 V is assigned to soak up line noise.

Start Bits

A beginning bit indicated the start of every frame. It's a relocate from negative to positive voltage (Mark and Space). Its period is in seconds and therefore the reciprocal of information measure. If the speed of transmission of instrument is nine, 600 baud rate then period of begin bit and every bit coming back when is regarding zero.104ms. The entire character frame of eleven bits would be transmitted in regarding one.146 ms.

Data Bit

Data bits area unit transmitted during the reversed logic. The memory blocks containing data bits are sent from least important bit to most important bit. Arrangement of transmission of bits in reversed logic is from the wrong way up and backwards. Bits containing data interpret in character frame from right to left. Consider one for negative and zero for positive voltage levels.

Parity Bits

An elective bit named as bit follows knowledge bits within the character frame. If present, the bit additionally follows inverted logic methodology that's one for voltage at negative side and zero for voltage at the positive side. Bit is enclosed for merely error handling. This should be set earlier that parity of the transmission should be even or odd. If the bit is chosen odd then the transmitter sets

bit so as to makes associate degree odd range of one's between the information bits and also the bit. Odd parity is employed in transmission. The bit is about zero, as a result of their five ones gift in knowledge bits associate degreed an already placed odd range. The table 4.1 shows the kinds of parity checking.

Parity Type	**Description**
ODD	Parity bit set so that there is an odd number of 1 bits
EVEN	Parity bit set so that there is an even number of 1 bits
MARK	Parity bit is ALWAYS set to 1
SPACE	Parity bit is ALWAYS set to 0

Table-4.1: Parity bits configuration.

Stop Bits.

The last portion of a character frame consists of stop bits. Negative voltage levels are always used to represent the stop bits.

Serial Data Format

As mentioned earlier the information format of serial communication consists of 1 begin bit, between 5 to eight knowledge bits, and one stop bit. Parity and a further stop bit are additionally enclosed within the serial info. Following figure helps well to explain the initial info for serial communication.

Fig-4.6: Showing in order arrangement of serial data

In view of an example that might properly portray eight-N-1 is understood as 8 information bits however no bit, and one stop bit, whereas seven-E-2 is understood as 7 information bits, even parity, and a pair of stop bits, as a result of information bits typically represent associate degree grapheme they're additionally spoken as character. As a result of the remaining bits frame the information bits they're known as framing bits.

How to connect two devices using serial cable?

The RS-232 normally defines a tool that uses serial cables for communication. Dividing them into 2 classes because the knowledge Terminal instrumentation DTE and knowledge Circuit-Terminating instrumentation DCE, these are the terms used for locating the direction of the signals on the pins and conjointly for the pin out for the connectors on device. It conjointly reflects RS-232 as customary for communication between laptop terminal and electronic equipment. DCE devices like electronic equipment, plotter, and metallic element adapter and DTE devices sort of a laptop or terminal.

Talking concerning speed first of all, pertaining to the terminal speed. It's the speed between electronic equipment and laptop that's (DTE to DCE). This speed is quicker than the DCE to DCE speed. Known as line speed, DCE to DCE is that the link between modems. Usually used modems in today's time are twenty eight K or 33.6K modems that the DCE to DCE speed predicted to be either twenty eight K or 33.6K. Keeping an equivalent thought in mind for the high speeds of the electronic equipment the DTE to DCE speed is predicted to be concerning a hundred and fifteen, 200 BPS. But communication programs that we have a tendency to exploitation have DCE to DTE speeds settings, and also the speed is nine.6 KBPS, one hundred forty four KBPS etc and conjointly the electronic equipment speed.

Suppose for the transferring of a document in DCE to DCE at the speed twenty eight K the electronic equipment compresses it and also the actual transfer is at a hundred and fifteen.2 KBPS between computers and so have a DCE- DTE speed of a hundred and fifteen.2 KBPS.

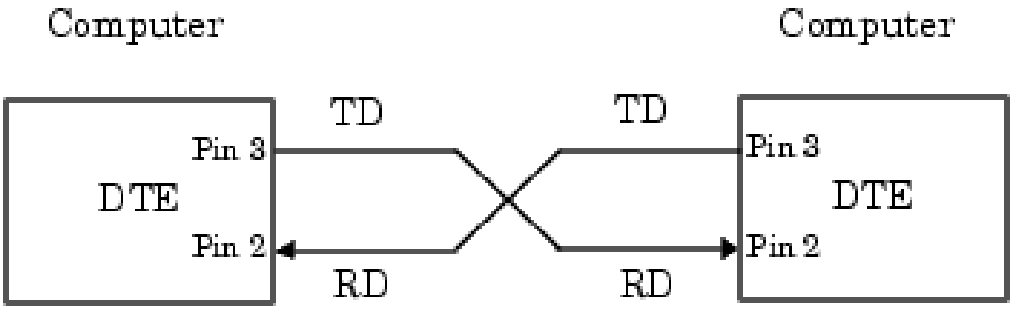


Fig-4.7: two devices showing DTE –DTE connection.

Serial Port Signals and Pin Assignments

Serial ports include solely 2 signal varieties that square measure knowledge signals and management signals. Interface communication wants three pins solely .One is for receiving knowledge whereas one is for transmission knowledge, and one is for signal ground. RS-232 serial ports is out there in 2 sizes ,one is that the D kind twenty 5 pin instrumentation and therefore the different is D kind 9 pin instrumentation .A feminine instrumentation is needed on the device as each of those connectors named on top of square measure male on the rear of the laptop. Pin connections, name and practicality for the 9-pin and 25-pin D-Type connectors' given below.

9 Pin Connector on a DTE device (PC connection)	
Pin Number	**Direction of signal**
1	Carrier Detect (CD) (from DCE) Incoming signal from a modem
2	Received Data (RD) Incoming Data from a DCE
3	Transmitted Data (TD) Outgoing Data to a DCE
4	Data Terminal Ready (DTR) Outgoing handshaking signal
5	Signal Ground Common reference voltage
6	Data Set Ready (DSR) Incoming handshaking signal
7	Request To Send (RTS) Outgoing flow control signal
8	Clear To Send (CTS) Incoming flow control signal
9	Ring Indicator (RI) (from DCE) Incoming signal from a modem."

Table-4.2: Pin configuration of a 9 Pin DB connector.

The Data Pins

Most of the interface devices support full duplex communication. That means they'll send and receive information at the exact same time, for this reason separate pins is employed for transmission and receiving information. To meet the preceding purpose these devices, use TD, RD, and GND pins. There also are some sorts of interface devices that solely support a method communication referred to as one half duplex communications. These specific devices use solely the TD and GND pins. The transmit information wire TD is employed once information from DTE

device is transmitted to DCE device. It will be terribly confusing as a result of this wire is employed by, a DCE device to receive information. DTE device keeps the TD line in mark condition once it's not getting used or idle. The receive information wire named RD receives the info by DTE devices, and it's unbroken in mark condition by DCE devices once it's not getting used.

Serial communication with PIC

PIC microcontroller could be a very hip microcontroller and is offered in a very package of forty pin PDIP pin out with several internal peripherals. The Forty pin layout of this kind of microcontroller makes it easier to use peripherals as a result of the functions area unit opened up over the pins, therefore creating it a lot of easier to pick out what external devices to connect or not without concern an excessive amount of if there enough pins to try to the work.

Illustration of Transmission of 8 Bit and 9 Bit Data

To send out any eight bit information the worth are hold on in register TXREG. This register stores the worth as transitory buffer before the information is sent. As a result of the transmission is eight bits, TX9 bit is adequate to zero. This bit stores the data for any ninth bit if out there. Inspection on the receiver's aspect, to receive the eight bit information the worth is hold on in register RSR. This register stores the worth as momentary buffer before the information is received. As a result of the information is eight bit therefore the price of register RX9 is adequate to zero. Equally if the information is nine bits the TX9 and RX9 register are crammed consequently.

MAX 232 (Voltage Level Converter)

USART solely utilized for transferring bits from PIC to PIC microcontroller only, but to transfer it from PIC to computer addition of another part is needed. Max 232 is employed to transmission whereas staying in RS 232 protocol and is additionally used for conversion of voltage level from USART to RS232. As a result of RS232 uses totally different voltage levels than USART that operates in 0-5 volts vary, easy lay 232 is employed. RS232 is totally different because it uses voltages below -5 volts for the logic level "l". And for logic level "0" it uses higher than five volts. This conversion is finished by easy lay 232 as easy lay 232 itself care for five volts.

Transmission from USART to Computer

When bits are being sent from USART to pc then pins used are:-

Pin ten or pin eleven connected to the output of USART.

Pin fourteen or pin seven transmits info to the pc.

Pin number ten of MAX 232 is connected with the controller's pin number twenty six.

This will carry the data that is transmitted to the pc connected to the output of USART. Pin seven can transmit this info to the computer by changing the voltage level that's appropriate to RS 232. This Pin is connected to the computer finish with Pin three of DB9 connecter.

4.2 Software Project Requirements

- **Proton IDE PIC Compiler**
- **Visual basic 6.0**

4.2.1 Proton IDE PIC Compiler

We have used Proton IDE compiler for programming the PIC16F877A microcontroller.

Proton IDE could be a strong and great visual Integrated Development setting (IDE) designed specifically for the compiler.

• This is easy

• Write down your code in it and easily assemble it with a single click.

• Your code can be checked with virtual simulator.

• Its updates are available easily and its can be updated without any fee.

• It is friendly with Windows, suggests that its programming setting is windows.

• It has third party computer programmer combination.

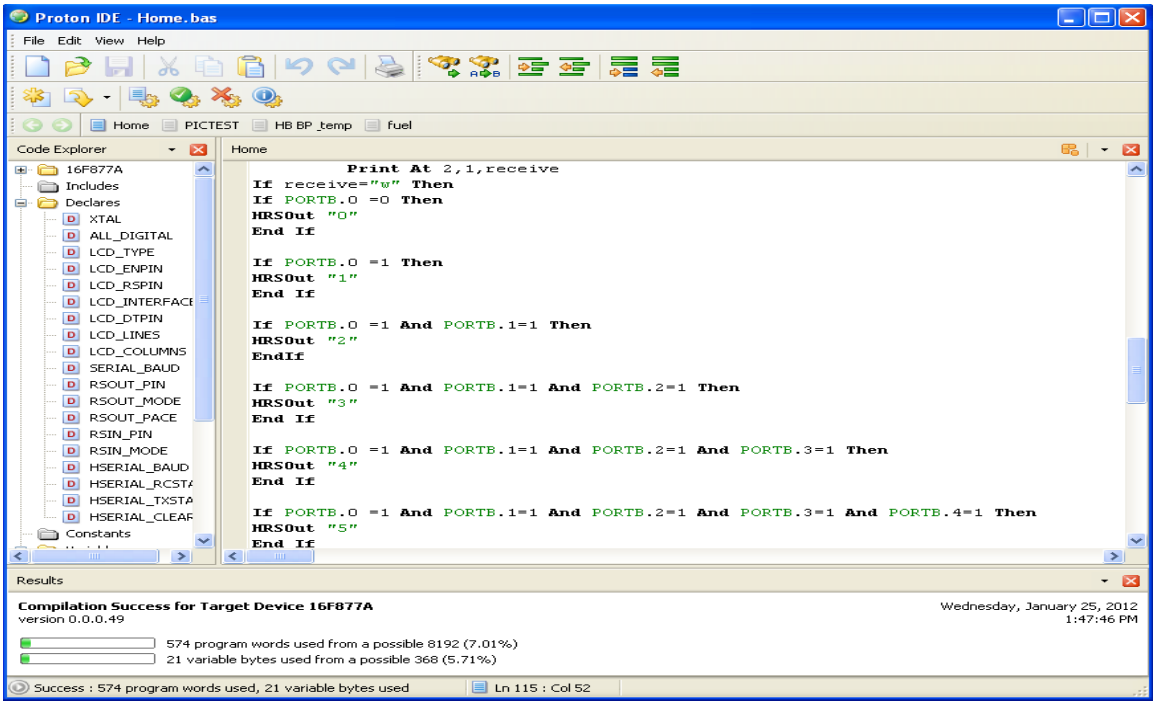


Fig 4.8 Proton compiler

• It contains incorporated boot loader for not solely 16fxxx however additionally for 18fxxx.

• It includes a plug in design.

• It includes a device support of twelve, 14, sixteen bit core devices.

• It includes a true compiler that produces legible and alterable ASM code.

• It has the power of floating purpose variables.

• It has additionally string variables.

• It has thirty two bit variables.

• It includes a support for bit, computer memory unit and word variables.

• It has giant arrays up to 256 parts.

• Data table support is superb

• It includes a nice graphics liquid crystal display support.

Proton IDE is designed to speed up creation progress in a calm consumer development atmosphere without compromising performance, suppleness or control.

Code Explorer

Perhaps the most superior code explorer for PIC based development on the marketplace. Swiftly steer your line up code and device Special Function Registers (SFRs).

Compiler Results

Provides data regarding the device used variety of code and information used the account number of the project and additionally date and time. You'll be able to additionally use the results window to leap to compilation errors.

Programmer Integration

It allows you to begin your most popular programming software system from at intervals the event atmosphere. This allows you to compile and so program your controller with simply many mouse clicks (or keyboard strokes, if you favor).

Incorporated Boot loader

Quickly transfer a code into your controller while not the necessity of a hardware computer user. Boot loading will be done in-circuit via a serial cable linked to your computer.

Actual Time Simulation Support

Proteus implicit System Modeling (VSM) combines diverse mode SPICE circuit imitation, animated elements and chip models to make possible co-simulation of whole microcontroller primarily based styles. For the primary time ever, it's potential to develop and check such styles before a physical paradigm is built.

Serial Communicator

An easy to employ service that allows you to broadcast and obtain information via a serial cable linked to your computer and development board. The straightforward to use configuration window permits you to pick port range, baud rate, parity, computer memory unit size and range of stop bits.

Online Updating

Keeping your software up to date via internet enables you to stay right up to date with the newest IDE features and fixes.

Plug-in structural design

The Proton IDE is been intended by means of flexibility in mind with sustain for IDE plug-in.

Operating Systems that are supported

Windows 98, 98SE, ME, NT 4.0 with SP 6, 2000, XP (recommended)

Hardware Requirements

400 MHz Processor (500 MHz or higher recommended)

128 MB RAM (128 MB or higher recommended)

50 MB hard drive space

16 bit graphics card.

4.2.2 Visual basic 6.0

Visual Basic six could be a high level and event-driven programing language and have a integrated development atmosphere (IDE) from Microsoft. Visual Basic (VB) is a perfect programing language for developing subtle skilled applications for Microsoft Windows. It makes use of Graphical computer program for making sturdy and powerful applications. The Graphical computer program because the name suggests, uses illustrations for text that alter users to act with associate degree application. This feature makes it easier to grasp things in a very faster and easier manner.

Coding in GUI atmosphere is sort of a transition to ancient, applied mathematics strategies wherever the user is guided through a linear path of execution and is proscribed to little set of operations. In GUI atmosphere, the quantity of choices hospitable the user is far larger, permitting a lot of freedom to the user and developer. Options like easier comprehension, user-friendliness, quicker application development and plenty of alternative aspects like introduction to ActiveX technology and net options build Visual Basic a stimulating tool to figure with. Visual Basic (VB) was developed from the fundamental programing language. Within the Seventies, Microsoft started developing ROM-based understood BASIC for the first microprocessor-based computers. In 1982, Microsoft QuickBasic revolutionized Basic and was legitimized as a significant development language for DOS atmosphere. Later on, Microsoft Corporation created the improved version of BASIC known as Visual Basic for Windows. Visual Basic (VB) is associate degree event-driven programing language. This is often known as result of programming is finished in a very graphical atmosphere not like the previous version BASIC wherever programming is finished in a very text solely atmosphere and dead consecutive so as to manage the computer program. Visual Basic allows the user to style the computer program quickly by drawing and transcription the user components. Because of this frolicked is saved for the repetitive task.

Important Features of Visual Basic (VB)

• Entire set of objects - you 'draw' the app.
• Numerous icons and images for your simple use
• answer back to mouse and keypad strokes
• Whole array of mathematical, string managing, and graphical functions
• Can handle fastened and dynamic variable and management arrays
• Serial and random access file support
• Useful program and error-managing functions
• Strong info access tools
• ActiveX support
• Package & implementation Wizard makes distributing your software apps straightforward.

Visual Basic 6 vs. previous versions of Visual Basic

The innovative Visual Basic for DOS and Visual Basic for Windows were manufactured in 1991. Visual Basic three (a large upgrading above preceding versions) was out in 1993. Visual Basic four was introduced in late 1995 (added thirty two bit function support). Visual Basic five was introduced in late 1996. New surroundings, supported formation of ActiveX controls, removed sixteen bit application support. Visual Basic six - out in middle 1998s - some known new options of Visual Basic six are:

- Quicker compiler
- Object for scheming the data with New ActiveX
- Allows info integration with wide selection of applications
- New information statement organizer
- New Package & preparation Wizard
- Added web capabilities.

Visual Basic 6.0 IDE

Visual Basic IDE consists of numerous components

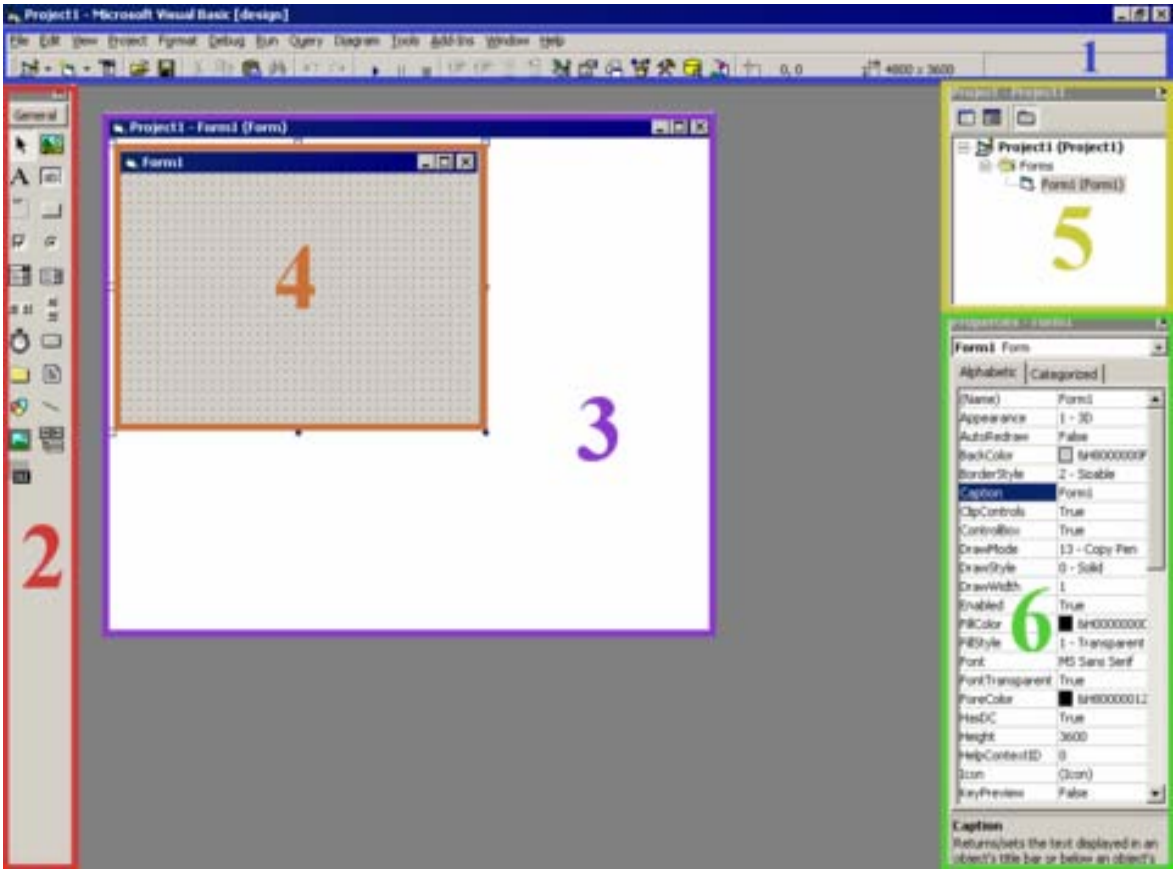


Fig-4.9 Visual Basic 6.0 IDE

- Menu and gear bars: Different options and tools are available for organizing and editing the programs.
- Toolbox: It contains totally different objects like textbox, buttons, labels etc.
- Object Window: It contains kind or User management.
- Graphical object: This show however your application can seem like. In figure there's a kind named Form1
- Project Explorer: this can be the place from wherever you explore totally different go into the project.
- Properties window: Here, you choose the various properties of objects and alter the properties.

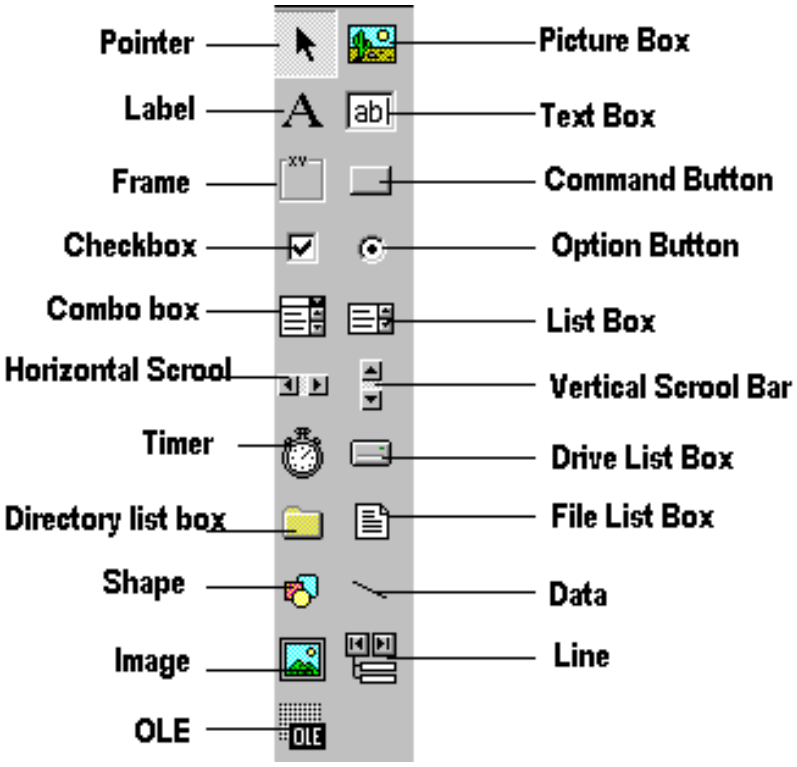


Fig- 4.10 VB Tool box

Chapter # 05

Project Design & Implementation

Project Design & Implementation

5.1 Block Diagram

5.1.1 Transmitter Side

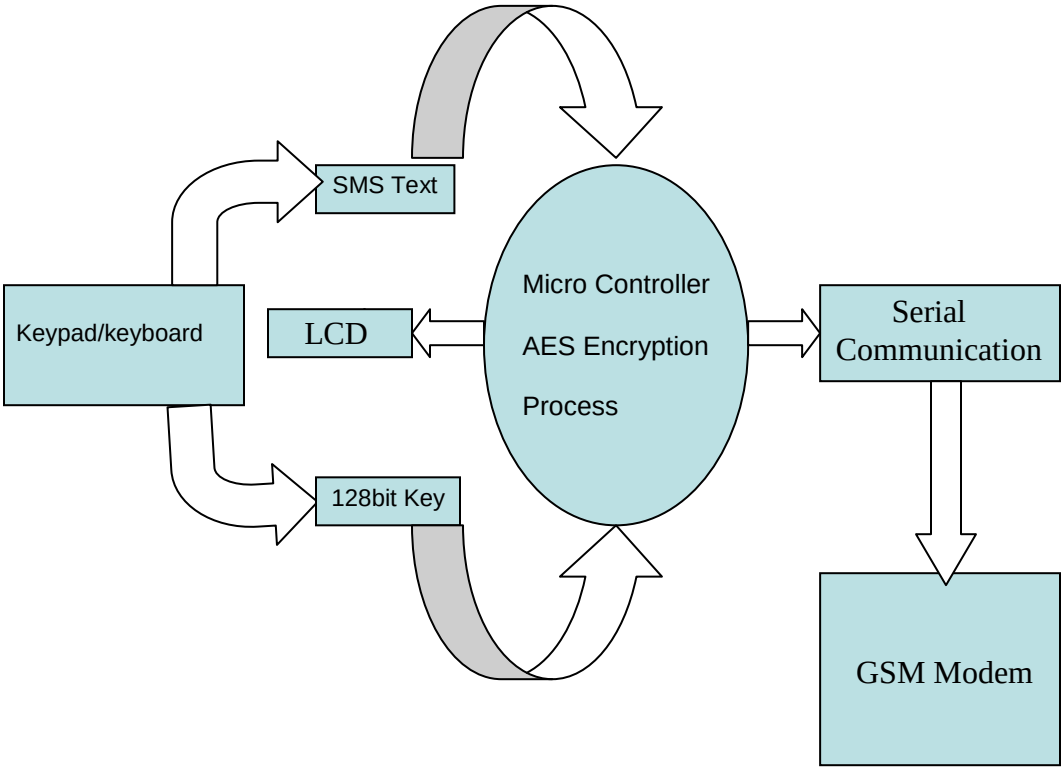


Fig 5.1: Transmitter Side Block Diagram

5.1.2 Receiver Side

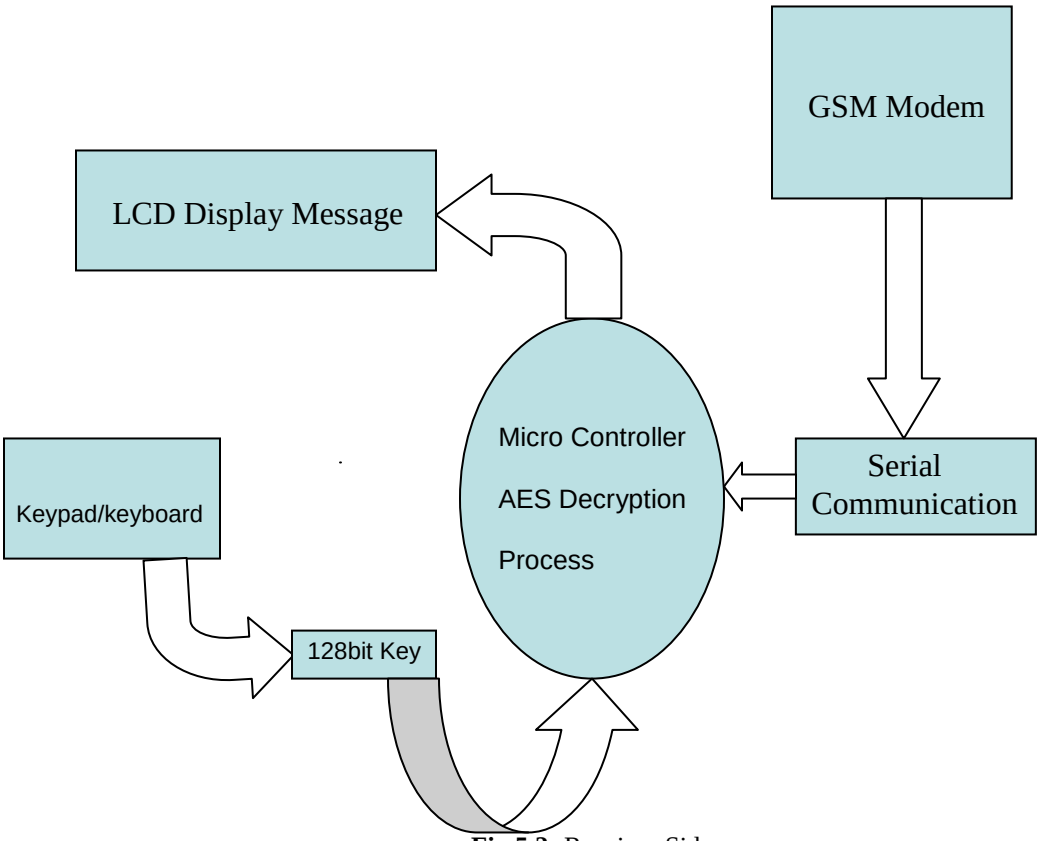


Fig 5.2: Receiver Side

5.2 Interfacing the LCD with Pic16f877a

It operates on a four bit action mode. Four pins are accustomed carry information with every pin carrying one bit at an instance. For this intention we've got chosen the number eleven,12,13,14 connected to the number thirty one,32,33,34 of PIC microcontroller. The pin

pattern of pins that we tend to area unit exploitation is represented below

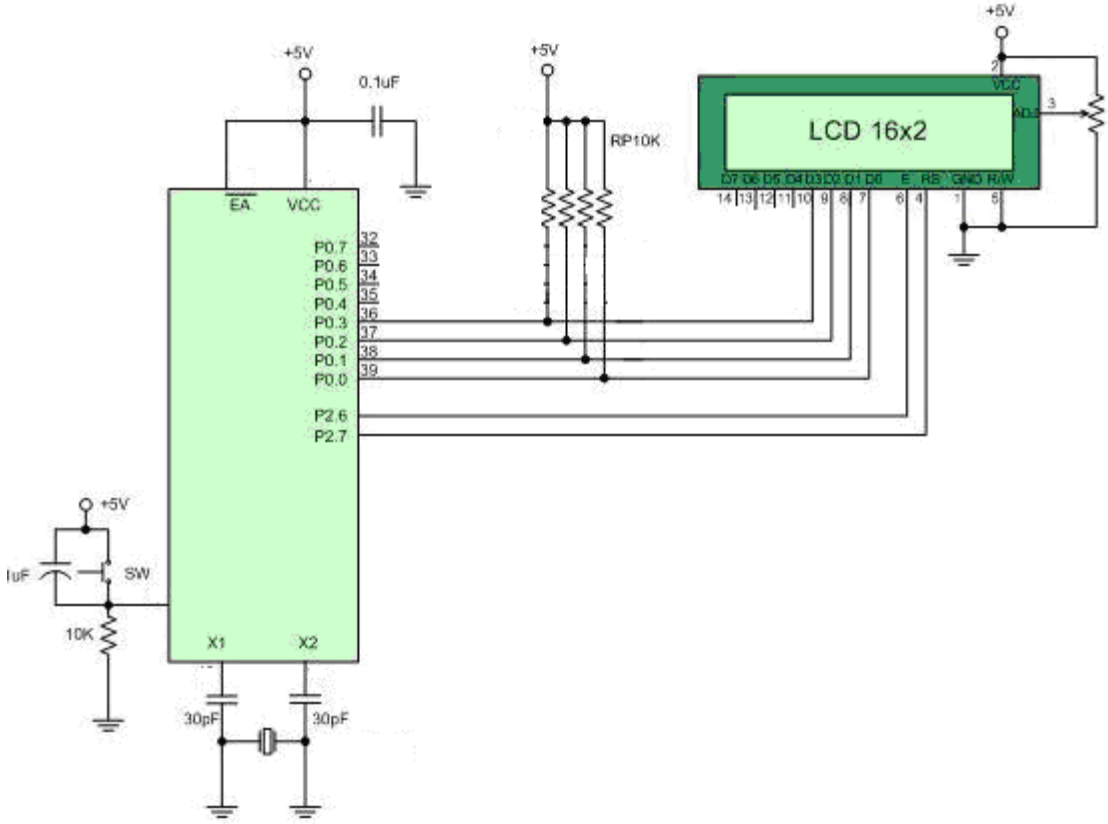


Fig 5.3: LCD interface with PIC 16f877a

5.3 Interfacing keypad with PIC 16F877A

Below is example keypad which connects directly to a PIC microcontroller. The keypad consist 8 pins and all the pin are used as input and output of microcontroller.

To use a keypad without keypad decoder, the pins of the keypad will have to be separated into 2 groups (usually 4 pin to input and 4 pin to output of PIC).Users can make column as output and row as input or column as input and row as output. From the schematic diagram in Figure 3, columns are being pulled high to 5V, so they are readable pins (Input to PIC). Rows are connected directly to PIC, so they are writeable pins (Output from PIC). To check which button is pressed, users need to scan it column by column and row by row. Make rows as output and columns as input as explained earlier. For example; set (5V, high logic) all rows by default. 1st scan, clear (logic low) row 1 and scan column 1 to column 4 for low logic, this will

determine which button is pressed in row 1. If one of those buttons is pressed, record it and jump out from the scanning loop and continue with the action required.

If none button is pressed in row 1, set it back to default (logic high) and clear row 2. Scan column 1 to column 4 again. This process should be repeated until all four rows are being completed scanned.

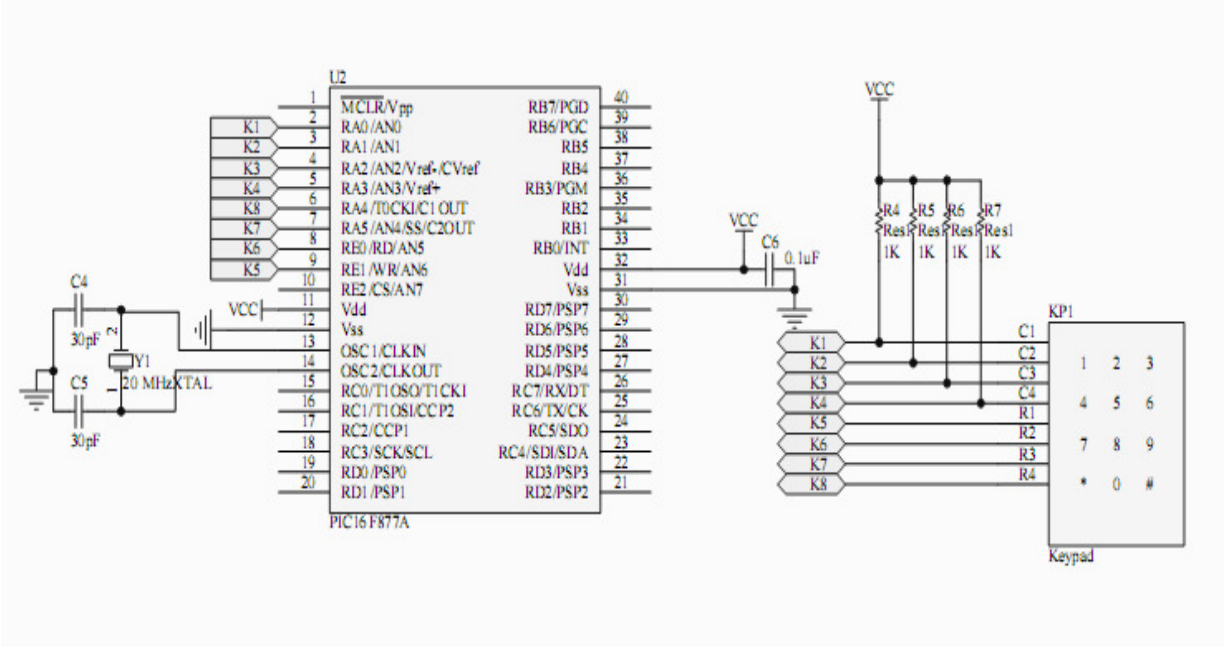


Fig 4.4: 4x3 Keypad connections to microcontroller

5.4 Micro Controller Interface with PC

We communicate microcontroller with Pc using serial communication so we use a voltage level converter (MAX232) to interface PIC with PC.

MAX 232 (Used to convert voltage levels)

USART is just used for transferring information from PIC to PIC microcontroller only. But to transfer it from PIC to computer addition of another element is needed. MAX 232 is employed for transmission whereas staying in RS 232 protocol and is additionally used for conversion of voltage level from USART to RS232. as a result of RS232 uses totally different voltage levels than USART that operates in 0-5 volts vary, soap 232 is employed. RS232 is totally different because it

uses voltages below -5 volts for the logic level “l”. And for logic level “0” it uses higher than five volts. This conversion is finished by soap 232 as MAX 232 itself operates five volts.

USART to Computer

When information is being sent from USART to laptop then pins used are:-

• Pin ten or Pin eleven attached to the output of USART.

• Pin fourteen or Pin seven send data to the pc.

We have attached Pin ten of MAX with our microcontroller’s PIN number twenty six. This will carry the information that is sent to the pc attached to the output of USART. Pin seven can send this data to the laptop by changing the voltage level that's appropriate to RS 232. This Pin is attached to the laptop finish with Pin three of DB9 instrumentality.

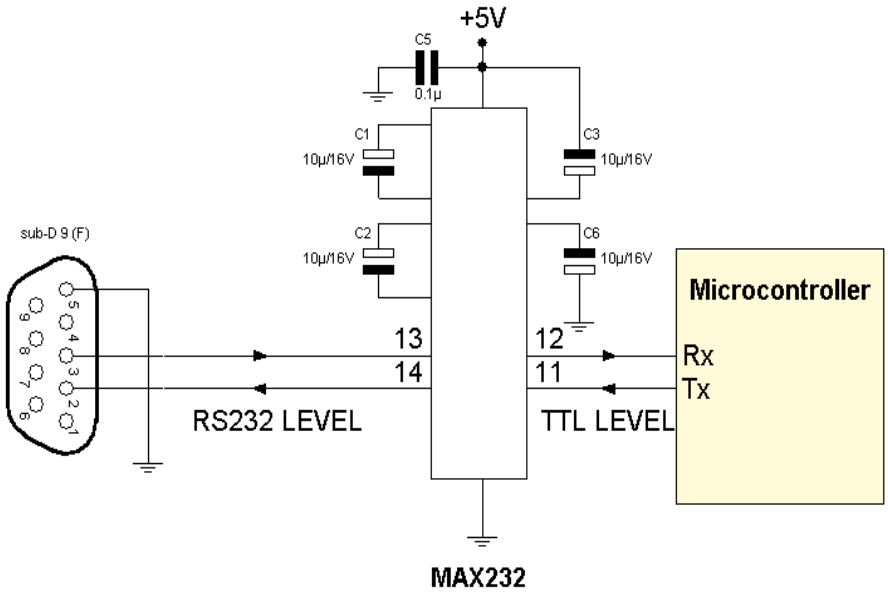
Computer to USART

When information is being sent from laptop to USART then pins used are

• Pin nine or Pin twelve attached to transmit information to USART.

• Pin thirteen or Pin eight connected to the information returning from laptop.

The information returning from computer is transmitted through the Pin eight of MAX 232. We’ve got connected this to PIN number a pair of DB9 connective. Once more the method of voltage conversion is performed however now around its regenerate consistent with specification of USART. The voltage level conversion is already delineating in previous sections. Pin nine is connected to Pin twenty five of microcontroller .It transmits the incoming information from laptop to USART.



.

Fig-5.5: Serial communication between microcontroller and computer

5.5 PIC16F877A Interface with GSM modem

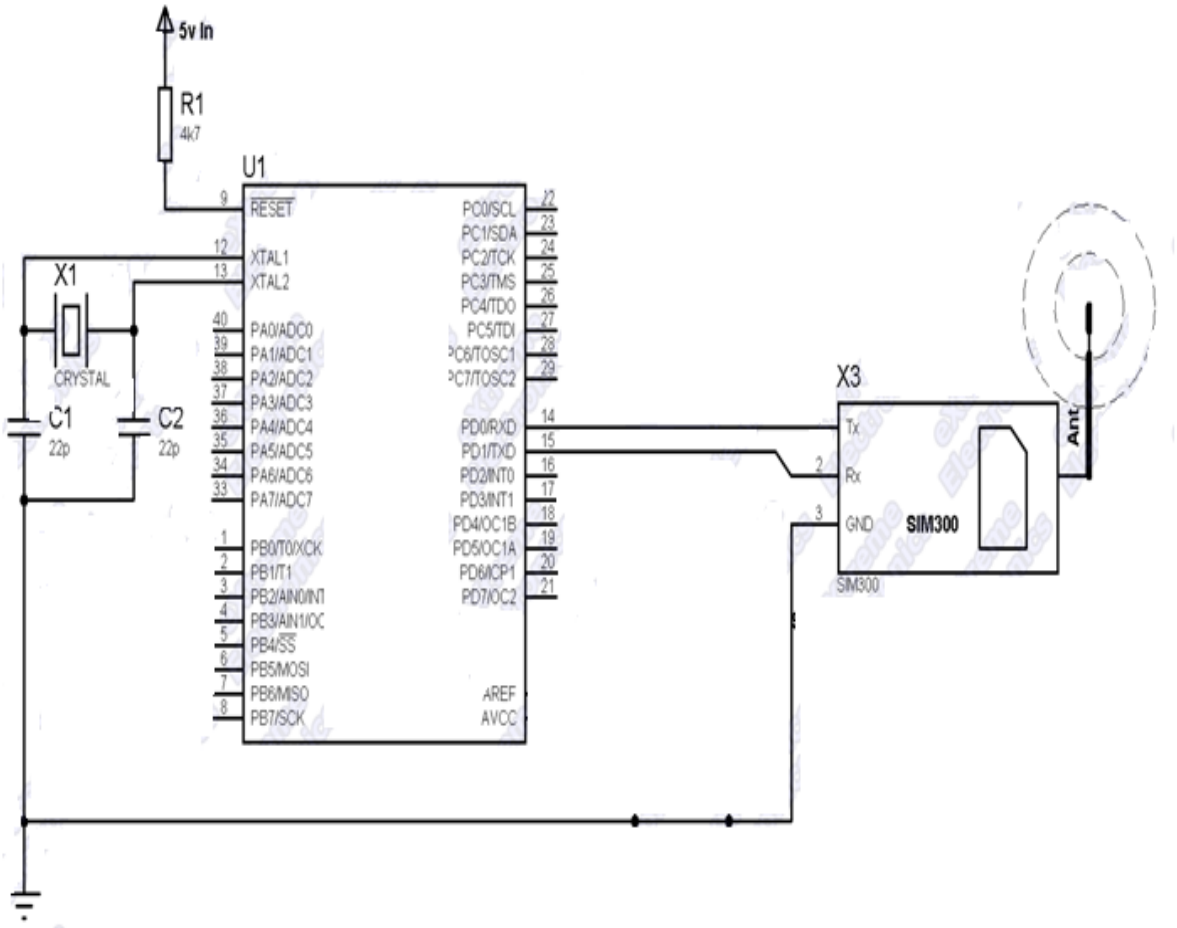


Fig 5.6: PIC16F877A Interface with GSM modem

5.6 Project PROTIUS Simulation

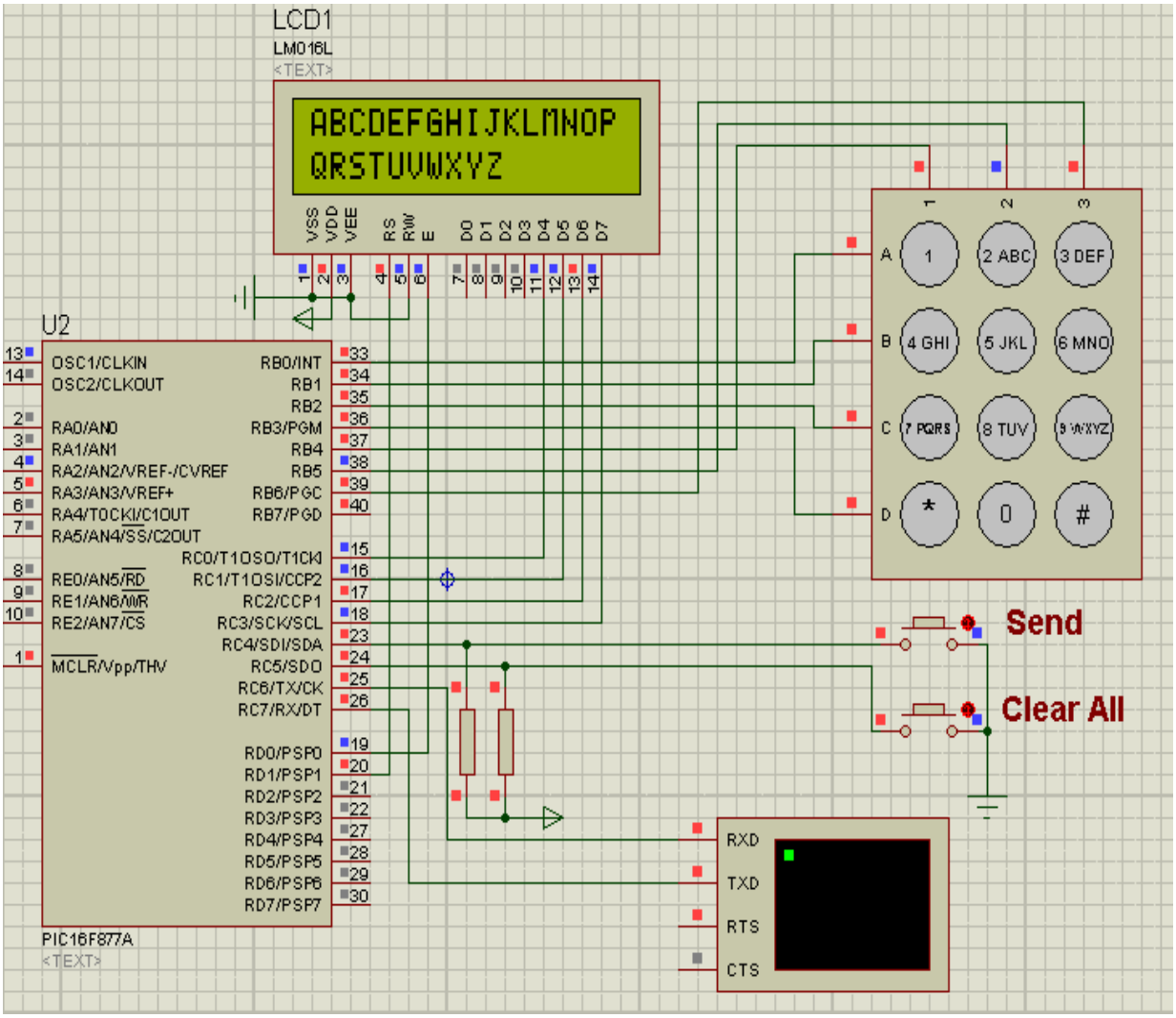


Fig 5.7 Project PROTIUS Simulation

5.7 Project Hardware

Fig 5.8: Project Hardware

Chapter # 06

Conclusion and Future Work

Conclusion and Future Work

As a conclusion the necessities for speed and compactness were met. The program size is twenty five K and it may be programmed into a Microcontroller acting on GSM electronic equipment. The user experiences no delays while utilizing the program that may be a clear indication that the speed demand is met. Most significantly, the messages containing delicate data are hold on firmly and stay unrevealed even once the device is accessed by an opponent. The foremost distinctive and important purpose to be thought-about is that the security of the encrypted information against numerous attacks like Brute Force attack, pattern attack etc. This application guarantees secure finish to finish transfer of information with none corrupt data segments.

As future work, we plan to implement the same algorithm using FPGA and compare performance against the Microcontroller implementation. Another direction of future work is to find other novel areas besides AES encryption that could benefit for secure communication.

Another direction of future work for this project can be developing the software based project e.g. developing an Android based application for smart phones utilizing the hardware of the phone, so it will enable a lot of people to install the application on their phone and to communicate securely without using any extra hardware.

Appendix A – Test Cases

Legend for CIPHER (ENCRYPT) (round number r = O to 1O)
input: cipher input
start: state at start of round[r]
s_box: state after SubBytes()
s_row: state after ShiftRows()
m_col: state after MixColumns()
k_sch: key schedule value for round[r]
output: cipher output

Legend for INVERSE CIPHER (DECRYPT) (round number r = 0 to 10)
iinput: inverse cipher input
istart: state at start of round[r]
is_box: state after InvSubBytes()
is_row: state after InvShiftRows()
ik_sch: key schedule value for round[r]
ik_add: state after AddRoundKey()
ioutput: inverse cipher output

PLAINTEXT: 0101122344556778890aabbccddeeff
KEY: 0100102030540506070809a0b0c0d0e0f

```
CIPHER (ENCRYPT):
round[ 0].input 0101122344556788990aabbccddeeff
round[ 0].k_sch 00201020304050607080g0a0b0c0d0e0f
round[ 1].start 10102030405060708090a0b0c0d0e0f0
round[ 1].s_box 603cab70409503d051cd60e0e17ba70e18c
round[ 1].s_row 63513e08c0960e1045cd70b751bacad07e7
round[ 1].m_col 5f7264315557f5bc92f47be3b291db9f917a
round[ 1].k_sch d6aa74f3dd2a5f72fadaa678f61gd6ab76fe
round[ 2].start 89d810e85t855ace6852d184g3d8cb128fe4
round[ 2].s_box a761ca9b9tf7be8b45d8ad761a611fc97369
round[ 2].s_row a7be1a6997ad739bd8c9ca4534f1f618b61
round[ 2].m_col ff874968431d86a51g645151fa773gad009
round[ 2].k_sch b692cf40b643dbdf1be49bc50046830b3fe
round[ 3].start 4915598f545e54d7a0daca94fa1f0a463f7
```

```
round[ 3].s_box 3b59cb73f4cd90e4e055774222dc067fb68
round[ 3].s_row 3bd92268gfc74fb735767cbe0c0590e2d
round[ 3].m_col 4c9c1e66f7f71f70762c3f6868e534df256
round[ 3].k_sch b6ff744edg2c2c9bf6hc590cbf0u469bf41
round[ 4].start fa63ed6a2825b339c940j668a3157244jd17
round[ 4].s_box 2dfb02r343f6d1h2dd09337ec75hb36e3f0
round[ 4].s_row 2d6hd7ef03f33e33h4093602dd5bfbh12c7
round[ 4].m_col 6385bh79ffc538df99h7be478e754h7d691
round[ 4].k_sch 47f7f7bc95353e03f96c32bcf2d058defd
round[ 5].start 2472402369166b3fa6ed2753288425b6c
round[ 5].s_box 236400926f93g36d25d9fb596d23c42c3950
round[ 5].s_row 1c36339d50f9b3539269f2c0942dc4406d23
round[ 5].m_col cf4bcd45432e5g54d07t5f1d6c5r1dd03b3c
round[ 5].k_sch 13fcaaa3e8a99f9deb50ff3af57adf622aa
round[ 6].start 1dcg81677bcg9b7gac93b25027992b0261996
round[ 6].s_box 3eg847f56514dhadde23f77b64fe7f7d490
round[ 6].s_row 1e8dab6901477d4653ff7f5e2e747dd4f
round[ 6].m_col a98g16ee7400f8f7f556b2c049c8ef5ad036
round[ 6].k_sch a5e390f7fdf7a69f296a7553dc10afa31f6b
round[ 7].start o4c62fe10f9f75eedc3cc793f95d84f9cf5d
round[ 7].s_box ibs415f8016858552e4bb6124c5f998ga4c
round[ 7].s_row vbf458124c68b68a014b99f82e5f15554cg
round[ 7].m_col 1c537e1c159a9bd2486f05f4be098c63439
round[ 7].k_sch 144f9701ae35fe28c2440adf4d4ea9c026
round[ 8].start 2d1876ct0f79c4300ab4w5594add66ff41f
round[ 8].s_box 13e175076b61ct04678dfc2295tf6a8bfc0
round[ 8].s_row 1h3e1c22c0b6fjcbf768da8506a7f6170495
round[ 8].m_col 0hbaa03de7a1f9b56ed5512cba5f414d23
round[ 8].k_sch 074e38735a41ece6e5b9e016baf4aebf7ad2
round[ 9].start 1hbfde3bad205e5d0gd73547964ef1fe37f1
round[ 9].s_box 65411f4bd56bd9700e96a0902fa1bdb9aa1
round[ 9].s_row 0gw54d990a16ba09ab596bbf40ea111702f
round[ 9].m_col 3rghe9f74eec023020f61bf2ccf2353c21c7
round[ 9].k_sch 1549932d1f085g57681093ed9gcbe2c974e
round[10].start 1bd6e7c3df2b57789e0b61216e89b10b689
round[10].s_box 17a9f102789d65f50b2beffd9hf3dca4ea7
round[10].s_row 17ad5fda789ef4e2h72bca100b3d9fhf59f
round[10].k_sch 113111hd7fe3944a17f307a78b4d2b30hc5
round[10].output9nm969c4e0d86a7b0430d8cdb78070b4c5a

INVERSE CIPHER (DECRYPT):
round[ 0].iinput 169c4e0d86a57b0430d8cdb78070b4c55a
round[ 0].ik_sch 513111d7fe39544a17f307a78b4d2b30c5
round[ 1].istart 7ad5frda789ef45e272bca100b3d9ff59f
round[ 1].is_row 17a9f102789d5f50b2b5effd9f3dca4ea7
round[ 1].is_box hbd6e7c3df2b577h9e0b61216e8b10b689
round[ 1].ik_sch 3549932d1f085576881093ed9cbe2c974e
round[ 1].ik_add e9f74eec023020f6157bf2ccf2353c21c7
round[ 2].istart 754d990a16ba09a7b596bbf40ea111702f
round[ 2].is_row 5411f4b56bd9700e196a09702fa1bb9aa1
round[ 2].is_box 6fde3bad205e5d0d773547964ef1fe37f1
round[ 2].ik_sch g4743873a5a41c65b9e016baf4aebf7ad2
round[ 2].ik_add abaa03de7a1f95b56ed5512cba5f414d23
round[ 3].istart g3e1c22gc0b6fcbf768da85067f6170495
round[ 3].is_row c3e175076bh61c04678dfc2295f6a8bfc0
round[ 3].is_box 7d1876c0f779c4300ab45594add66ff41f
round[ 3].ik_sch 814f97018ae35fe28c440adf4d4ea9c026
```

round[3].ik_add afc57e1c159a9bd286f05f4be098c63439
round[4].istart ab458124c68b68a01g4b99f82e5f15554c
round[4].is_row 7b415f80168578552e4bb6124c5f998a4c
round[4].is_box 3c62fe10h9f75eedc3cc79395d84f9cf5d
round[4].ik_sch 35e390f7df7a6929y6a7553dc10aa31f6b
round[4].ik_add g9816ee7400f87f55h6b2c049c8e5ad036
round[5].istart 7e8dab6901477d465h3ff7f5e2e747dd4f
round[5].is_row 6e847f56514da6dde23f77b64fe7f7d490
round[5].is_box 3c81677bc9b7ac93b250279392b0261996
round[5].ik_sch 1caaa3e8a99f9dteb50f3af57adf622yaa
round[5].ik_add r14bcd45432e554d075f1d6c151dd03b3c
round[6].istart 363339d50f9b539269f23c092dc4406d23
round[6].is_row 664t00926f9336d2d9fb59d23cf42c3950
round[6].is_box 3247240236966b3fa6ed27d53288425b6c
round[6].ik_sch 147f7f7bc95353ge03f96c32bcfd058dfd
round[6].ik_add 16385b79ffgc538df997be478e7547d691
round[7].istart 62d6d7ef03f33eh334093602dd5bfb12c7
round[7].is_row r2dfb02343f6d12dd09337c75bgg36e3f0
round[7].is_box fa636a2825b339c9403w668a3157g24gd1
round[7].ik_sch bb6ff744ed2c2c9bbf6c590cbf0469bf4g
round[7].ik_add 4c9c1e66f771f0762c3fb868e534df25g6
round[8].istart b3bd92268fhc74fb735767cbe0c0590e2d
round[8].is_row b3b5j9cb73fcd90ee05774222dc067fb68
round[8].is_box 64915598f55e5d7a0dggaca4fa1f0a63f7
round[8].ik_sch ab692cf0bg643dbdf1be9bc5006830b3fe
round[8].ik_add gff8796843g1d86a51645151fa773ad009
round[9].istart ga7be1a6997ad739bd8gc9ca451f618b61
round[9].is_row va761ca9b97be8b45d8agd1a611fc97369
round[9].is_box 289d810e8855acge682d1843d8cb128fe4
round[9].ik_sch 3d6aa74fdd2af72gfadaa678f1d6ab76fe
round[9].ik_add 45f72641557f5bgc92f7be3b291db9f91a
round[10].istart 56353e08c0960e1g04cd70b751bacad0e7
round[10].is_row 963cab7040953d0g51cd60e0e7ba70e18c
round[10].is_box 0g000102030405060708090a0b0c0d0e0f0
round[10].ik_sch 0100102030405060708090g0a0b0c0d0e0f

round[10].ioutput 0101122334455667788 99aabbccddee0ff

References

[1] J.Daemen and V.Rijmen, AES Proposal: Rijndael, NIST"s AES home page, http ://www:nist:gov/aes."Announcing the Advanced Encryption Standard (AES)",Federal Information Processing Standards Publication 197, November 2001

[2] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.

[3] Hassinen M.: SafeSMS 1.0 user manual. October 2004,Department of Computer Science, University of Kuopio.

[4] G. Racherla, D. Saha, "Security and Privacy Issues in Wireless and Mobile Computing", Proceedings of 2000 IEEE International Conference on Personal Wireless Communications, Dec 17-20, 2000, pp.509-513.

[5] H. Marko, H. Konstantin, "Strong Mobile Authentication",Proceedings of 2nd International Symposium on WirelessCommunication Systems, Sept 5-7 2005, pp.96-100.

[6] Xinmiao Zhang and Keshab K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm", 1531-636X/12, IEEE 2002.

[7] Chun Yan,Yanxia Guo, "A Research and Improvement Based on Rijndael Algorithm", 2009 First International Conference on Information Science and Engineering,Nanjing, Jiangsu China, December 26- December 28, ISBN:978-0-7695-3887-7

[8] J. Nechvatal, et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, October 2, 2000, available at

[9] http://elastic.org/~fche/mirrors/www.jya.com/aes/fips-197.htm

[10] www.waset.org/journals/waset/v49/v49-153.pdf,

[11] http://visualbasic.freetutes.com/index.html

[12] http://www.mecanique.co.uk/proton-ds/ide/index.html

WEB LINKS

http://en.wikipedia.org/wiki/AdvancedEncryptionStandard

http://www.cs.uku.fi/ ~ mhassine/SafeSMS/Manual en.pdf

http://software.intel.com/en-us/articles/advanced-encryption-standard-aes-instructions-set/

http://www.esat.kuleuven.ac.be/rijmen/square/fse.ps.gz.

http://www.nist.gov/CryptoToolkit

http://topics.udm4.com/online_aes_encrypt_decrypt/

http://en.wikipedia.org/wiki/AES_implementations