DESIGN AND CONSTRUCTION OF AN ELECTRONIC SAFELOCK WITH A CHIPCARD.

BY

IHEZUKWU MICHEAL NNADOZIE

2001/12001EE

A thesis submitted to department of electrical and computer engineering
School of engineering and engineering technology,
federal university of technology, Minna.
Niger state

NOVEMBER 2007

DEDICATION.

This project is dedicated to my mother and God almighty for seeing me through, even in my shortcomings.

DECLARATION.

I IHEZUKWU MICHEAL NNADOZIE, declares that this work was done by me and has never been presented else where for the award of a degree. I also hereby relinquish the copyright to the federal university of technology, Minna.

IHEZUKWU MICHEAL · N

STUDENTS NAME.

J·A·AJIBOYE

SUPERVISORS NAME.

3/12/07

SIGNATURE AND DATE.

3/12/07

SIGNATURE AND DATE.

HEAD OF DEPARTMENT.

NAME OF EXTERNAL SUPERVISOUR.

SIGNATURE AND DATE.

SIGNATURE AND DATE.

ACKNOWLEDGEMENT.

As always we acknowledge the invisible hands of the Almighty gently guiding and steering us towards our destiny.

Also the efforts of my parents are also acknowledged, and to my brothers Ihezukwu Emenike, Ihezukwu Chukwuemeka, and my one and only sister Ihezukwu Onyinyechi thanks for all the advice and encouragement,

And to my friends, Olasnell, Smooth, Gboka, Sammy, Chairman, Prof, GP, FJ, and J, thanks for lending me your strength.

Love you all.

ABSTRACT.

The beauty of a microprocessor based project cannot be over emphasized, this project which is a microcontroller based electronic safelock, exploits the versatility of the microcontroller. The project also makes use of a Chipcard, which are just 128 or 256 bit of EEPROM, using the first sixteen bytes of the card to identify its user. Combining this with a keypad allows for double checks, more protection and makes for a more reliable, efficient and an effective lock whose limitations are minimal.

TABLE OF CONTENT.

CHAPTER FOUR

CHAPTER FIVE

LIST OF FIGURES.

LIST OF TABLES.

LIST OF PLATES.

CHAPTER ONE.

1.0 INTRODUCTION.

The normal lock and keys of today has the limitation of the numbers of keys produced for a lock. This poses a problem where the number of people expected to access a facility or building outnumbers the keys produced for a lock, and in the case of a misplace or theft of a key, as there are no ways to check the access of the thief, unless the lock is replaced

The electronic safelock puts most of this fear to rest. Not only does it use a telecard (chip card) or a magnetic stripe card as key it also comes with a 4 digit pass code which every registered card owner must know, or the won't have access to whatever equipment, facility or building the electronic safelock grants access to. This helps in the event of theft or misplacement of the card, as who ever possesses the card must know the 4 digit code to make use of the card.

It also has the advantage of, the amount of people we can grant access to a facility as additional memory could be interfaced to the design without reconfiguring the old design.

The magnetic stripe card (same type used in the ATM cards) has a strip of magnetic material (the same type of material used in diskettes and cassette) on it's side, this magnetic strip is where the Card owner's information are stored and read whenever the card owner inserts it into a card reader.

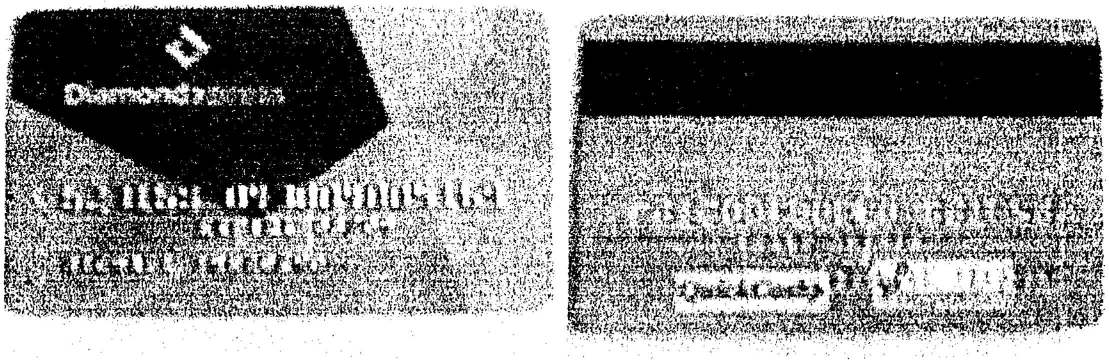

Plate 1.0 A magnetic strip card.

This magnetic strip card readers are quite complex, and needs, precise and accurate engineering. They could be bought in the market but are quite expensive as they are intended for larger projects.

Whereas materials for they TELECARD card reader could be sourced locally, and therefore this brands of cards are most suitable for our projects.

The telecard has replaced most of the magnetic cards applications notably for telecom payment and also for credit cards. These Cards are far more secure than the magnetic cards, and there are several kinds of card following the application.

Nigerian Telecommunications Ltd
200 Units
NITEL ...Your link to the world

Plate 1.1 A chip card.

The simpler ones are the Simple Memory cards like the one used as Telecard for the telecom payment in the public phone-booths (Generally all the memory content is readable, and there is a maker-area that is unwritable) , then there are more sophisticated cards: Memory Cards with some area read protected by a key, these cards can contain some private information's in the read-protected area. At the end, there are microprocessor-cards (cards working following the ISO-7816 protocol), that are the safest ones, since these cards have their own internal Operating System that prevent I/O if the PIN (Personal Identification Number) has not been entered in the cards before (These cards are used when confidentiality is needed, like in credit cards (bank), crypted TV access cards, health cards, SIM cards for GSM, etc ...).

This project makes use of a telecard it is readily available in the form of old Nitel phone booth cards and also G.S.M cards or ATM cards and as already mentioned above, there reader can be sourced and assembled locally. And therefore this does not only saves us time, but money.

1.1 AIMS AND OBJECTIVES:

1. To emphasize the versatility of a microprocessor based project.
2. To create a lock whose limitations are minimal.
3. Creating a lock whose key can be changed for every new user.

1.2 METHODOLOGY

This project is built on the versatility of a microprocessor which in this case is an AVR ATMEGA8515 microcontroller. This microcontroller comes with 8 bytes of In-System Programmable Flash with Read-While-Write capabilities, 512 bytes EEPROM, 512 bytes SRAM, an External memory interface, 35 general purpose I/O lines, 32 general purpose working registers, two flexible Timer/Counters with compare modes, Internal and External interrupts, a Serial Programmable USART, a programmable Watchdog

Timer with internal Oscillator, a SPI serial port, and three software selectable power saving modes.

This microcontroller acts as the core of this project, as it prompts the user to insert the card on initialization (with the help of the LCD) and checks if the card is a registered card by comparing the first sixteen bytes with bytes of registered cards stored in EEPROM, if the card is a registered card it prompts the user to input a four digit pin, checks for the validity of the PIN, if valid, it activates the lock which in this case is demonstrated with a LED, else it triggers on an alarm for a period and then resets itself.

CHAPTER TWO

2.1 LITERATURE REVIEW.

2.1.2 HISTORICAL BACK GROUND

The history of old locks and their keys together form a subject which has received considerable attention. The Egyptian lock was first described by Eton in his Survey of the Turkish Empire, 1798. Further information about it was given early in the 19th century by Denon, the Frenchman, who said that he had found the locks sculptured in one of the grand old temples of Karnac, which shows that the same kind of lock has served Egypt for 40 centuries. Locks almost identical or with very little difference and still made of wood have been seen recently in Iraq and Zanzibar

Some references and quotations from ancient and other writers concerning primitive locks and their keys are of interest. Aratus in his description of the constellation Cassiopeia says that in shape it resembles a key. Huetius agrees, adding that the stars to the North compose the curved part and those to the South the handle of the crooked or curvey keys belonging to those early days. According to Parkhurst's Hebrew Lexicon (1807) keys of this kind with handles of wood or ivory were put through holes in the doors and turned one way or the other to move the bolt. Homer in the Odyssey says that Penelope wishing to open a storeroom picked up a well made copper key which had an ivory handle. That is the translation by a modern scholar. Pope's version is:-

A brazen key she held, the handle turn'd, With steel and polish'd elephant adorn'd;

The poet Arison in the Anthologia applies to a key an epithet meaning on that is much bent. Eustathius, a Greek commentator on Homer about AD 1170, says that keys of this kind were very ancient but still in use in his time. As they were in the shape of a sickle and awkward to carry otherwise, they were tied together and carried on the shoulder. This custom is confirmed by Callimachus in his Hymn to Ceres. Eustathius attributes the invention of keys to the Lacedemonians while Pliny and Polydore Virgil give credit to Theodorus of Samos. This, however, is disproved by other authors who hold that keys were in use before the Siege of Troy.

It has been said that the most ancient lock every discovered is that described by Mr Joseph Bonomi in Nineveh and its Palaces as having secured the gate of an apartment in one of the palaces of Khorsabad. He says that the gate was fastened by a large wooden lock like those still used in the East, the wooden key with iron pegs at one end to lift the iron pins in the lock, being as much as a man can carry. Mr Bonomi adds that the length of such keys ranged from thirteen to fourteen inches to two feet or more. In a letter which appeared in a trade journal in 1850 Mr W C Trevelyan said that it was remarkable that the locks which had been in use in the Faroe Islands, probably for centuries, were identical in their constructions with those of the Egyptians. They were, lock and key, in all their parts made of wood; of which material, he believed, were others which had been found in Egyptian Catacombs, thus making the Egyptian so like the Faroese in structure and appearance, that it would not be easy to distinguish one from the other.

The frequent mention of locks and keys in the Old Testament is further evidence of their great antiquity. In the book of Judges (Chapter iii), it is recorded that after Ehud had stabbed Eglon, King of Moab, he shut the doors of the parlour upon him, and locked them, and when the servants came and found the doors locked, they took a key, and opened them. This would probably be in the twelfth or thirteenth century B.C., and there is no reason to doubt that by that time locks and keys were in use in Palestine. In the Song of Songs (Chapter, v, v. 5) there is a poetical reference to hands dropping with Myrrh on the handles of the lock. Then in the book of Nehemiah (Chapter iii, v.6) 445

B.C., it is stated that at the time of repairing the old gate of Jerusalem, they set up the doors thereof, and the locks thereof, and the bars thereof. In confirmation of other records that keys in the early days were very large, there is in the prophecy of Isaiah (Chapter. xxii, v.22) circa 712 BC, this passage: And the key of the house of David will I lay upon his shoulder.

The name of Chubb is famous in the lock world for the invention of the detector lock and for the production of high quality lever locks of outstanding security during a period of 140 years. The detector lock, which is described elsewhere in this work, was patented in 1818 by Jeremiah Chubb of Portsmouth, England, who gained the reward offered by the Government for a lock which could not be opened by any but its own key. It is recorded that, after the appearance of this detector lock, a convict on board one of the prison ships at Portsmouth Dockyard, who was by profession a lockmaker, and had been employed in London in making and repairing locks, asserted that he had picked with ease some of the best locks, and that he could pick Chubb's lock with equal facility. One of these was given to the convict together with all the tools which he stated to be necessary, as well as blank keys fitted to the drill pin of the lock and a lock made on exactly the same principle, so that he might make himself master of the construction. Promises of a reward of £100 from Mr Chubb, and a free pardon by the Government were made to him in the event of his success. After trying for two or three months to pick the lock, during which time he repeated overlifted the detector, which was as often undetected or readjusted for his subsequent attempts, he gave up, saying that Chubb's were the most secure locks he had ever met with, and that it was impossible for any man to pick or to open them with false instruments. Improvements in the lock were subsequently made under various patents by Jeremiah Chubb and his brother Charles.

The credit of producing pin tumbler locks, as we know them, belongs to the Yales, father and son. In 1848 Linus Yale senior, who was born in Middleton, Conn. for a time devoted his attention to bank locks and later applied the pin tumbler mechanism of the ancient Egyptian lock to modern conditions. The first models had the tumblers built into the case of the lock, which had a round fluted key. Linus Yale junior developed the pin tumbler cylinder, reducing it to its present dimensions, with different kinds of keys, these being at one time flat and later corrugated, which eventually gave place to the paracentric pattern now used. Pin tumbler locks very much alike in size and construction are now made in great quantities in many countries throughout the world.

Thomas Parson's lock of 1833 was the first change key lock patented in England but old locks embodying the same idea have been seen, showing that Parsons was not the original inventor. For one of these early locks the key bit was made of a number of pieces which could be threaded on the stem in any order and there secured by a nut and a pin. The levers in the lock were rearranged to suit. A keyless combination lock superior to any so far named, is the kind made for safes and strong rooms. This was developed in the United States of America during the second half of the 19th century, so it is believed. Such locks are widely used in the States and to a smaller extent in this and other countries. Some of them are capable of one hundred million changes of combination.

As far as is known, the lock patented in 1831 by Williams Rutherford, a bank agent, of Jedburgh in Scotland, was the first time-lock made. This was a lock requiring a key to open it after a given period of time. The inventor introduced at the rear end of the bolt a circular stop plate, which prevented the withdrawal of the bolt by the key until the plate had rotated a definite amount in order to bring a notch in it opposite the end of the bolt. The rotation of the circular plate was caused by clockwork. As the notch could be set at pleasure any distance from the end of the bolt, the time could be varied, but the lock could not be opened by its own or any other key until the appointed number of hours had elapsed. The modern time-lock as used for safes and strong rooms is a much more elaborate piece of mechanism than Rutherford's. It may be used as the sole fastening of the bolts of the door, or in conjunction with locks of other kinds. It is believed that Mr James Sargent, of Rochester, NY made the fist model of this variety about 1865 and subsequently improved it. Great numbers of these locks are now in use in different parts of the world. The need for time locks arose in America when masked burglary increased to such an alarming degree. Finding that forcibly opening or attempting to open safes and strong rooms was too slow and too dangerous, burglars adopted another plan. A gang of masked and armed men in the night would seize an official of the bank and compel him by torture, if necessary, to disclose the combinations of the locks or give up his keys. Such success followed this procedure that the method soon became prevalent, and bankers were told that neither the bank officials themselves nor anyone else could open the safe doors before a determined time.[1]

In the 1970s, the lodging industry had an increasing problem with hotel crime. It was common that hotel room keys, even master keys, were sold on the street with tags identifying hotel and room number. Furthermore, these locks had few key variations and were easy to copy. The result was increasing problems with hotel room thefts and even assaults on hotel guests. As a consequence, the industry was looking for a new type of lock, where the key could be changed for every new guest. The first mechanical keycard lock was installed for testing in a hotel in 1977; the first US installation was at Peachtree Plaza Hotel, Atlanta, Georgia in 1979. In Early in the 1980s the keycard lock was electrified with LEDs that detected the holes.

2.2 THEOREOTICAL BACKGROUND.

2.2.1 Keycard.

A keycard, while not actually considered a key, is a plastic card which stores a digital signature that is used with electronic access control locks. It is normally a flat, rectangular piece of plastic and may also serve as an ID card. There are several popular type of keycards in use and include the mechanical holecard, bar code, magnetic stripe, smart card (embedded with a read/write electronic microchip), and RFID proximity cards. The keycard is used by presenting it to a card reader; swiping or inserting of magnetic stripe cards, or in the case of RFID cards, merely being brought into close proximity to a sensor.

Bar code technology is not a secure form of a key, as the bar code can be copied in a photocopier and often read by the optical reader.

Magnetic stripe keycards are becoming increasingly easy to copy, but have the security advantage that one may change the stored key in a magnetic swipe card in case the current key may be compromised. This immediate change of the "key" information can be applied to other media, but this media probably offers the least expensive option, and the most convenient to users and managers of systems that use this media. Example: If you own a car with this system, you can change your keys anytime you want. You can buy new media anywhere a gift card is sold. At least at this point in time, you could buy a gift card for a penny, then use that as the media for the keys to your car. If the system uses digital environmental data samples to create the "key" string, every car can have a set of keys that no one else has. If a card is stolen, or copied without authorization, the card can be remade, and the car security system can be synchronized with the new card, and no longer activationally responsive to the copy of the old card. This approach can empower the system controller (owner/individual or centralized administration of a business).

Computerized authentication systems, such as key cards, raise privacy concerns, since they enable computer surveillance of each entry. Currently RFID cards and key fobs are becoming more and more popular due to its ease of use. Many modern households have installed digital locks that make use of key cards, in combination with biometric fingerprint and keypad PIN options.

The first keycard was the mechanical holecard type patented by Tor Sørnes, a concept he later developed into the magnetic stripe card key.[2]

2.3 KEYCARD LOCKS

A keycard lock is a lock operated by a keycard with identical dimensions to that of a credit card or driver's license. Keycards systems operate either by physically moving detainers in the locking mechanism with the insertion of the card or by reading digital data encoded on the card's magnetic strip or chip.

Types of Keycards

Mechanical Based.

Magnetic Strip Based.

2.3.1 Mechanical Based

Mechanical keycard locks employ detainers which must be arranged in pre-selected positions by the key before the bolt will move. This principle was the base for the first known card operated locks, the VingCard®, invented by Tor Sørnes. This was a mechanical type of lock operated by a plastic key card with a pattern of holes. There were 32 positions for possible hole locations, giving up to 2 raised to the power of 32 = 4.2

billion different keys. The key could easily be changed for each new guest by inserting a new key template in the lock that matched the new key.

2.3.2 Magnetic Strip / Chipcard Based

Magnetic strip (sometimes "stripe") based keycard locks function by running the magnetic strip or chip over a sensor that reads the contents of the strip or chip. The strip/chip's contents are compared to those either stored locally in the lock or those of a central system. Some centralized systems operate using hardwired connections to central controllers while others use various frequencies of radio waves to communicate with the central controllers. Some have the feature of a mechanical (traditional key) bypass in case of loss of power.[3]

Similar projects have been undertaken previously in the department. For example a project by Emmanuel Okon with registration number 2000/9893EE with title "DESIGN AND CONSTRUCTION OF A DIGITAL LOCK USING A CHIP CARD" (October, 2006), used a chip card that had to be assembled, this chip card was bulky and the project lacked the versatility of a microprocessor based project, as most tasks that could be carried out by the microprocessor had to be assigned a different module and fabricated as if it were entirely a different project.

But in this project, the chipcard need not be constructed and the microprocessor been the brain of the project, does most of work, regulating and coordinating activities of the other modules.

CHAPTER 3

3.1 DESIGN AND IMPLIMENTATION

The block diagram below gives a thorough description of how the system works, the entire system is broken down into several modules with each module been a section of the entire system performing a particular task.

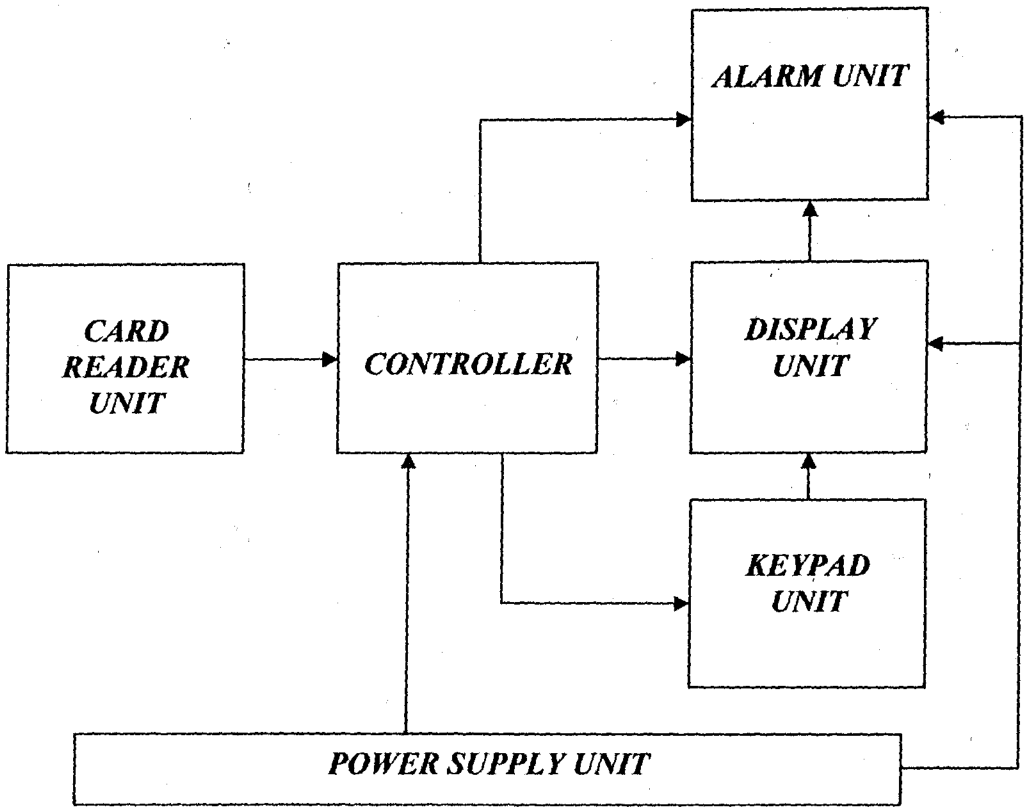

Fig 3.1 Block diagram.

3.2 CARD READER UNIT:

This unit acts as an interface between the Chipcard and the microcontroller. When the card in inserted into the reader, the reader connects the card to the controller unit, which provides the necessary clocking required, resets the card, reads the first 16 bytes of the card.

For this project, the card reader was constructed from simple materials; these materials include cardboard paper, tin, wire conductor, and masking tape. The figure below shows a picture of the card reader unit.

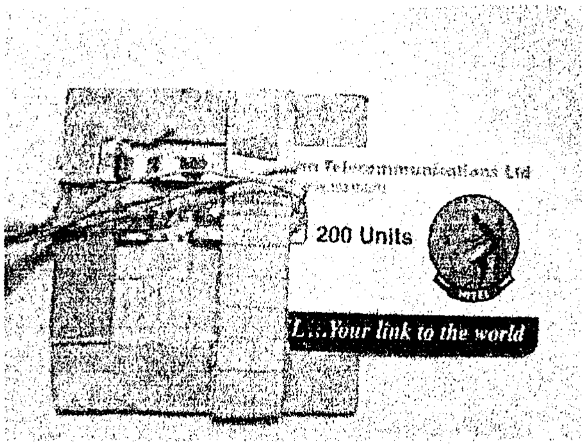

Plate 3.1 The card reader.

3.2.1 THE CHIPCARD:

3.2.2 PINOUT OF THE CARD CONNECTOR:

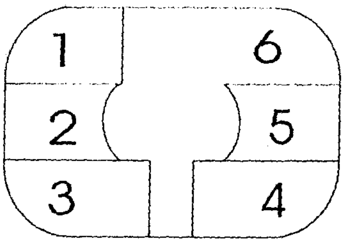

Fig 3.2.1 Pinout of card connector.

1: Vcc = 5V 6: Gnd

2: RESET 5: Vpp = 5V

3: Clock 4: I/O

The Chipcard is a 256 bits of EEprom with a serial input and output and some other control pins. Data is clocked out serially from the card.[1].

3.3 POWER SUPPLY UNIT:

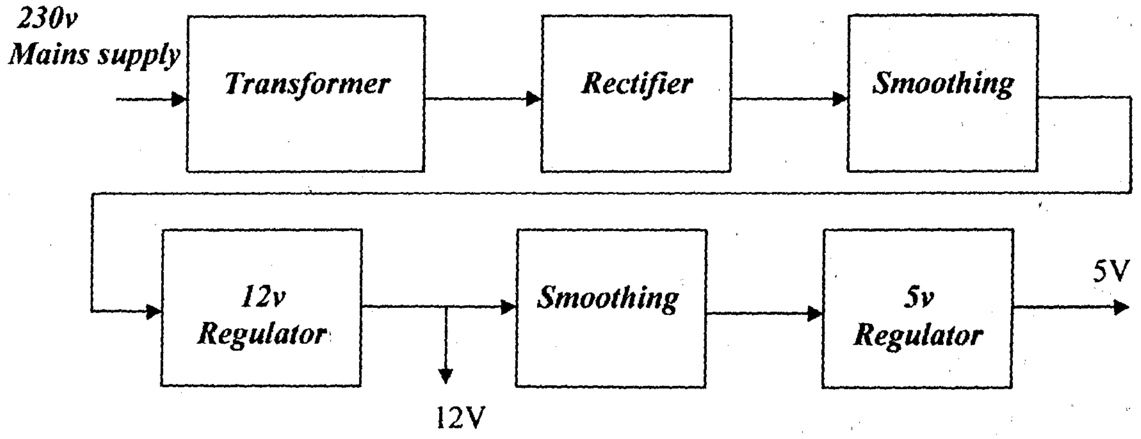

Fig 3.3. Block diagram of power supply unit.

The power supply unit provides a 12v and 5v dc regulated output from the general 230v Mains supply. This is used to as dc power supply for the other modules. A block diagram of the power supply unit is shown above.

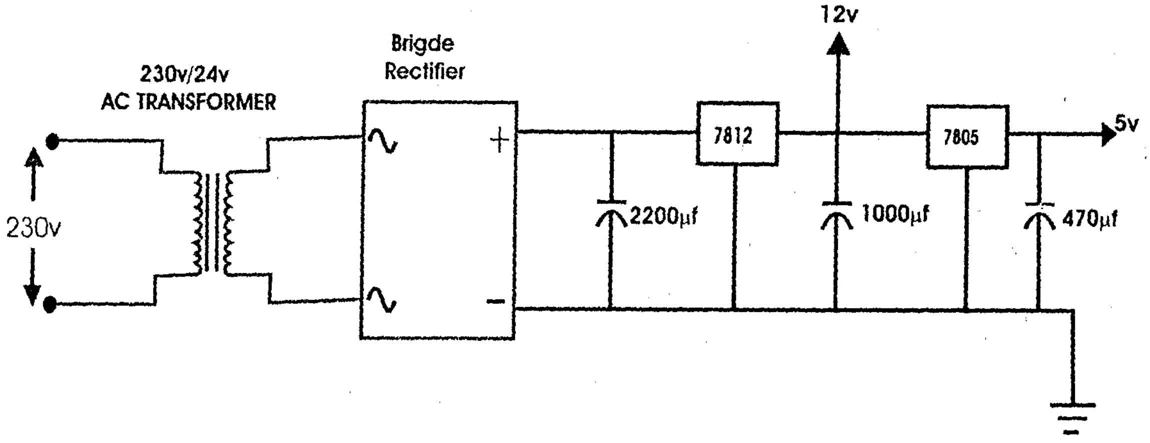

Fig 3.3.1. Circuit diagram of the power supply unit.

3.3.1 TRANSFORMER:

A transformer converts AC (alternating current) electricity from one voltage to another With little loss of power. Transformers work mainly from the primary side that is connected to the mains source and sends out the regulated output to the secondary unit. The input is drawn from a 240v mains and then steeped down by the 12v-12v transformer tapped between the two positive lines thereby giving us 24v.

The ratio turns determines the ratio of the voltage.

Turns ration =Vp/Vs =Np/Ns

Power out *power in

Vs*Is = Vp*p

Vp.............primary input voltage

Np............number of turns on primary coil

Ip..............primary input current

Vs.............secondary output voltage

Ns.............number of turns on secondary coil

Is..............secondary output current.

Calculating the voltage transformation;

The Voltage transformation was archived using a step-down transformer with specification given below

Primary Voltage	V_p,	-	-	240 V_{rms}
Secondary Voltage	V_s,	-	-	24 Vrms
Secondary Current	I_s,	-	-	1.5 A

Using the transformer equation;

$(V_P/V_S) = (I_S/I_P)$

$I_P = (V_S * I_S)/ V_P$

$= (24 * 1.5)/ 240 = 0.15$ A

Also,

$V_{peak} = \sqrt{2} * V_{rms}$

$= \sqrt{2} * 24 = 33.94$ V

$I_{peak} = \sqrt{2} * I_{rm}$

$= \sqrt{2} * 1.5 = 2.12A \approx 2$ A

3.3.2 RECTIFICATION

This is done by the bridge rectifier .The bridge rectifier IC is a four Pin IC with its two inner pins as AC input and the two outer pins as output to the voltage regulator. The dc voltage is calculated from the equation below.

$V_{dc} = (2 * V_{peak})/ \pi$

$= (2 * 33.94)/ \pi = 21.60$ V [4].

3.3.3 VOLTAGE REGULATION.

A voltage regulator is an integrated circuit whose function is to keep a voltage at a specific level. Some regulators are adjustable, others are not. Voltage regulators come in both positive and negative voltages. They have three pins, the input, output and reference. The input is usually on the left side of the square and is where the unregulated input voltage is applied. The reference is usually on the bottom of the square and is where the reference voltage is applied. For fixed regulators, this reference is usually ground.

For variable regulators, this reference is usually a small variable voltage just above ground. The last connection is the output, and is usually located on the right side of the square. This is where the regulated output voltage is taken from. On most schematics, the connections are numbered and labelled.

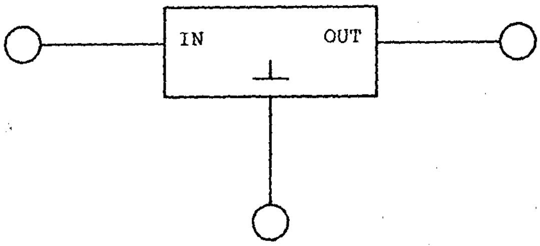

Fig 3.3.2. Symbol of a Voltage Regulator

3.3.4 SMOOTHING

This is done by an electrolytic capacitor (2200μF).the capacitor was chosen based on the stipulation that RL>1/f for effective smoothing with RL=load resistance which is about 30ohmns and frequency of the ac signal whose mains supply which is approximately 50 Hz and a 1000μF capacitor and a 470μF capacitor was used at the output of the 12v and 5v regulator respectively, to ensure proper smoothing.[4]

3.4 CONTROLLER

The controller unit acts as the brain of this project, coordinating the operations of other modules i.e. reading a card inserted into the card reader, scanning the keypad, sending different messages to the display unit at times, and finally operating the relay.

And sitting at the heart of the controller unit is an ATMEGA8515 microprocessor. The circuit diagram of the controller unit is shown in the figure below

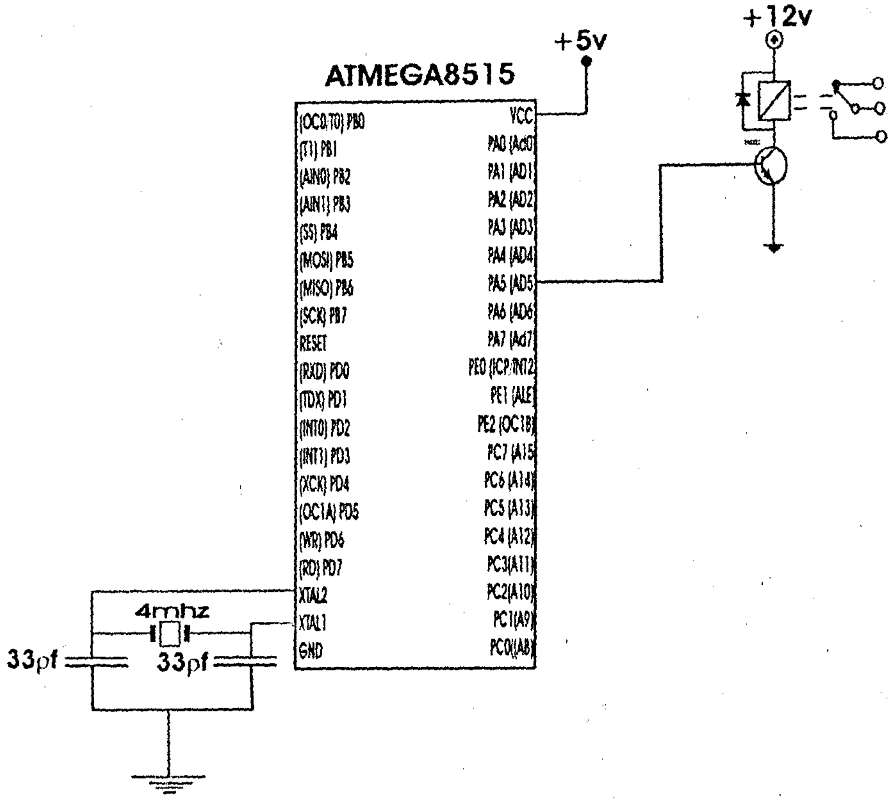

Fig 3.4 Controller unit connection.

THE ATMEGA8515 MICROCONTROLLER:

The ATmega8515 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega8515 achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.

The ATmega8515 also provides the following features: 8K bytes of In-System Programmable Flash with Read-While-Write capabilities, 512 bytes EEPROM, 512 bytes SRAM, an External memory interface, 35 general purpose I/O lines, 32 general purpose working registers, two flexible Timer/Counters with compare modes, Internal and External interrupts, a Serial Programmable USART, a programmable Watchdog Timer with internal Oscillator, a SPI serial port, and three software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, SPI port, and Interrupt system to continue functioning. The Power-down mode saves the Register contents but freezes the Oscillator, disabling all other chip functions until the

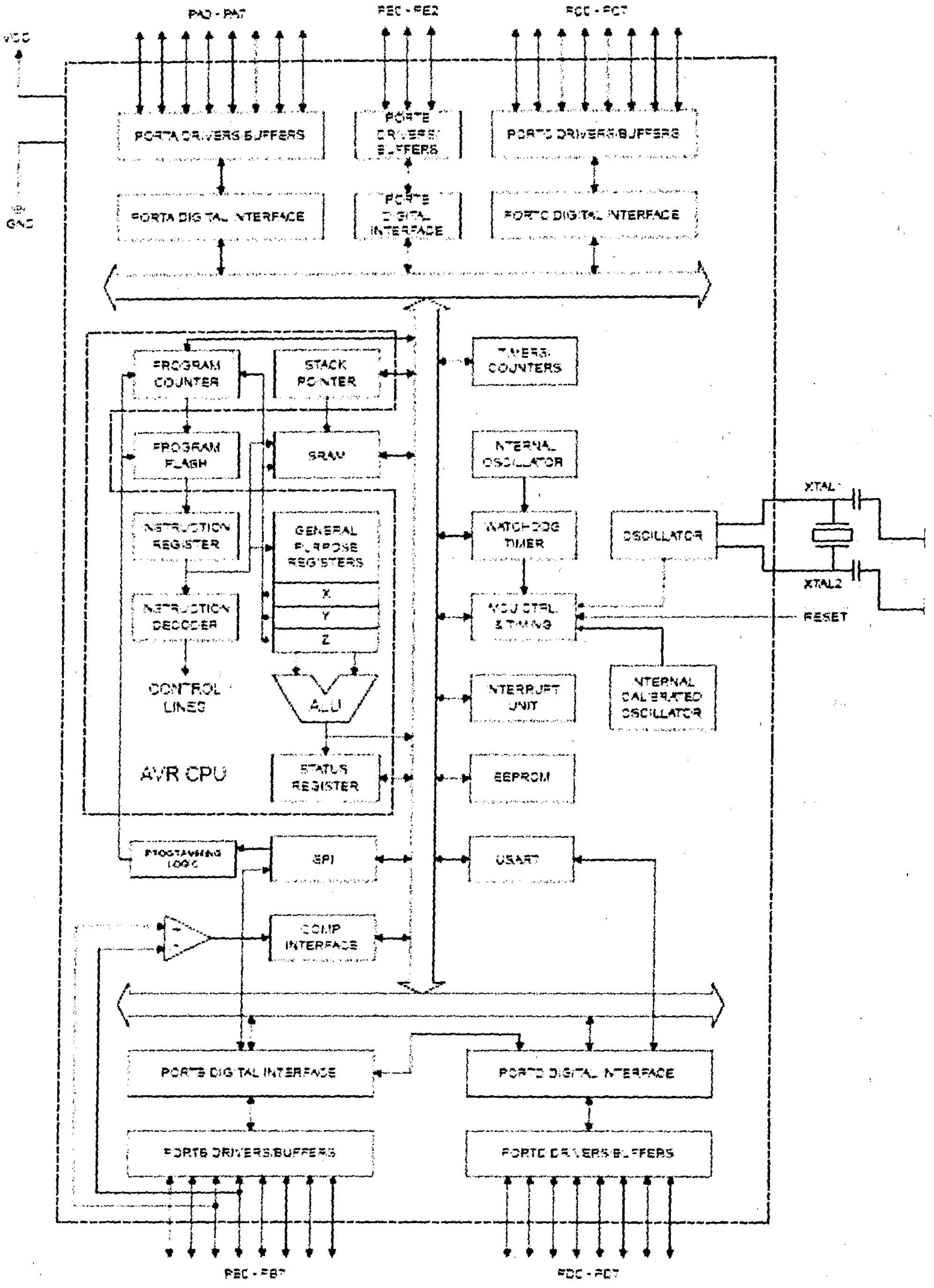

Fig 3.4.1. Block diagram of the internal structure of the ATMEGA8515.

next interrupt or hardware reset. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low-power consumption.

Pin Descriptions

VCC: Digital supply voltage.

GND: Ground.

Port A (PA7...PA0): Port A is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The PortA output buffers have symmetrical drive characteristics with both high sink and source capability. When pins PA0 to PA7 are used as inputs and are externally pulled low, they will source current if the internal pull-up resistors are activated. The PortA pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port B (PB7...PB0): Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port C (PC7...PC0): Port C is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port C output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port D (PD7...PD0): Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port E (PE2...PE0): Port E is a 3-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port E output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port E pins that are externally pulled low will source current if the pull-up resistors are activated. The Port E pins are tri-stated when a reset condition becomes active, even if the clock is not running. Port E also serves the functions of various special features of the ATmega8515

RESET: Reset input. A low level on this pin for longer than the minimum pulse length will generate a reset, even if the clock is not running.

XTAL1: Input to the inverting Oscillator amplifier and input to the internal clock operating circuit.

XTAL2: Output from the inverting Oscillator amplifier.

3.5 DISPLAY UNIT:

The display unit consists of a 2 × 16 line LCD display working in four bit mode. For 4-bit interface data, only four bus lines (DB4 to DB7) are used for transfer. Bus lines DB0 to DB3 are disabled. The data transfer between the LCD and the ATMEGA8515 is completed after the 4-bit data has been transferred twice. As for the order of data transfer, the four high order bits (for 8-bit operation, DB4 to DB7) are transferred before the four low order bits (for 8-bit operation, DB0 to DB3). The busy flag must be checked (one instruction) after the 4-bit data has been transferred twice. Two more 4-bit operations then transfer the busy flag and address counter data.

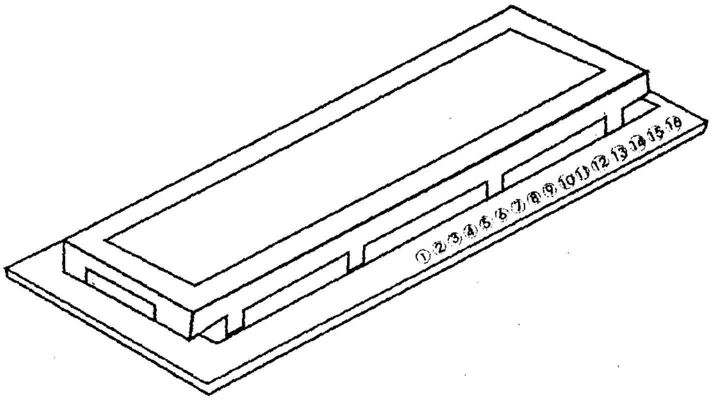

Fig 3.5 An LCD display unit.

Table 3.1. LCD pinout.

NO	SYMBOL	FUNCTION
1	VSS	GROUND,0V
2	VDD	LOGIC POWER SUPPLY,+5V
3	VD	VOLTAGE FOR LCD DRIVE
4	RS	DATA/INSTRUCTION REGISTER SELECT
5	R/W	READ/WRITE
6	E	ENABLE SIGNAL, START DATA READ/WRITE
7	DB0	DATA BUS LINES.
8	DB1	
9	DB2	
10	DB3	
11	DB4	
12	DB5	
13	DB6	
14	DB7	

15	LED A	LED ANODE,POWER SUPPLY+5
16	LED K	LED CATHODE, GROUND 0V.

In this project the data bus lines (D7-D4) are interfaced to PortC of the ATMEGA8515 microprocessor, while the power supply to the unit and drive voltage are connected as shown below.

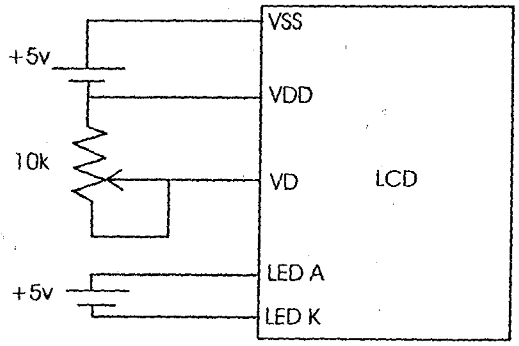

Fig 3. 5.1 Power supply connection to the LCD unit.

3.6 ALARM UNIT:

The alarm unit makes use of an LM386 IC. The LM386 IC is a power amplifier designed for use in low voltage consumer applications. The gain is internally set to 20 to keep external part count low, but the addition of an external resistor and capacitor between pins 1 and 8 will increase the gain to any value up to 200.

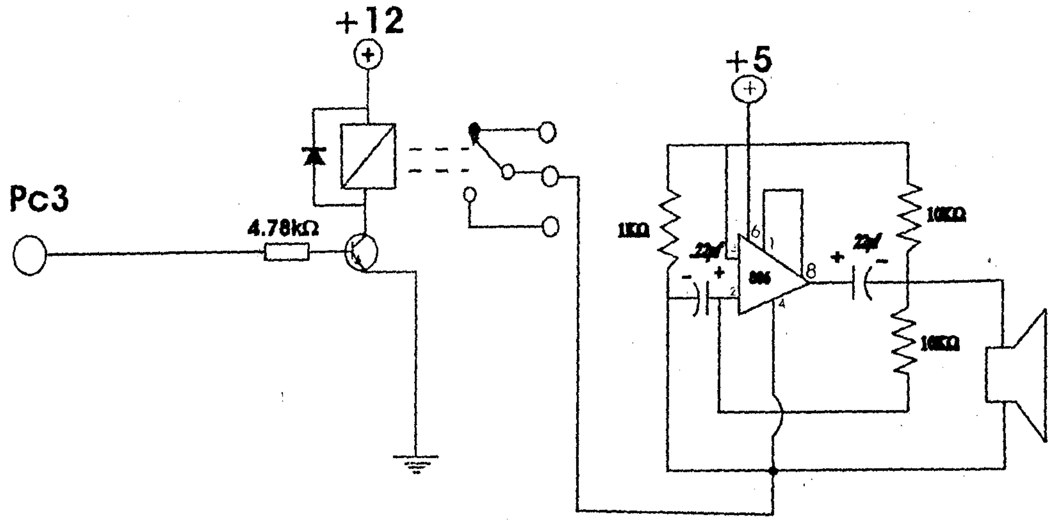

Fig 3 .6. The alarm unit

In the circuit above, the LM386 acts as a signal generator with the effective frequency set by the 1KΩ resistor and the .22μf capacitor. The pins 1 and 8 are connected together to obtain a gain of about 200. The 22μ f capacitor acts as a decoupling capacitor. The microprocessor turn the alarm on by operating the relay for a time period and thereby connecting pin 4 of the 386 to ground. On this basis of operation, the alarm unit not only acts as an alarm but also as a keypad tone generator.

3.7 KEYPAD UNIT

The keypad section consists of a four by four keypad and a register and unregister button. The 3 rows of the keypad are connected to PortB0 – PortB2, while the 4 columns are connected to PortB4 – PortB7 of the microprocessor.

This port is configured (by program) such that PortB0 – PortB3 acts as outputs while PortB4 – PortB7 are pulled high (configured as an input pin). The inputs to every push switch on a particular row is connected to the corresponding output port while the output of the push switch is connected to the corresponding input port

The microprocessor outputs a high to each of the output ports in quick succession and for every output port that is made high, the input ports are scanned , if any input port is high, the number on the keyboard that is pressed is calculated from the output port and the input port that are high.

The other two buttons (i.e. the register and unregister button) are connected to PortA6 and PortA7, this port pins are configured as inputs and pulled high. The input to the push switches are connected to the corresponding port while the output of this switches are grounded. A low on any of these pins signifies that a corresponding key has been pressed and the microprocessor therefore, carries out a specific task.[2]

The final circuit diagram is shown below

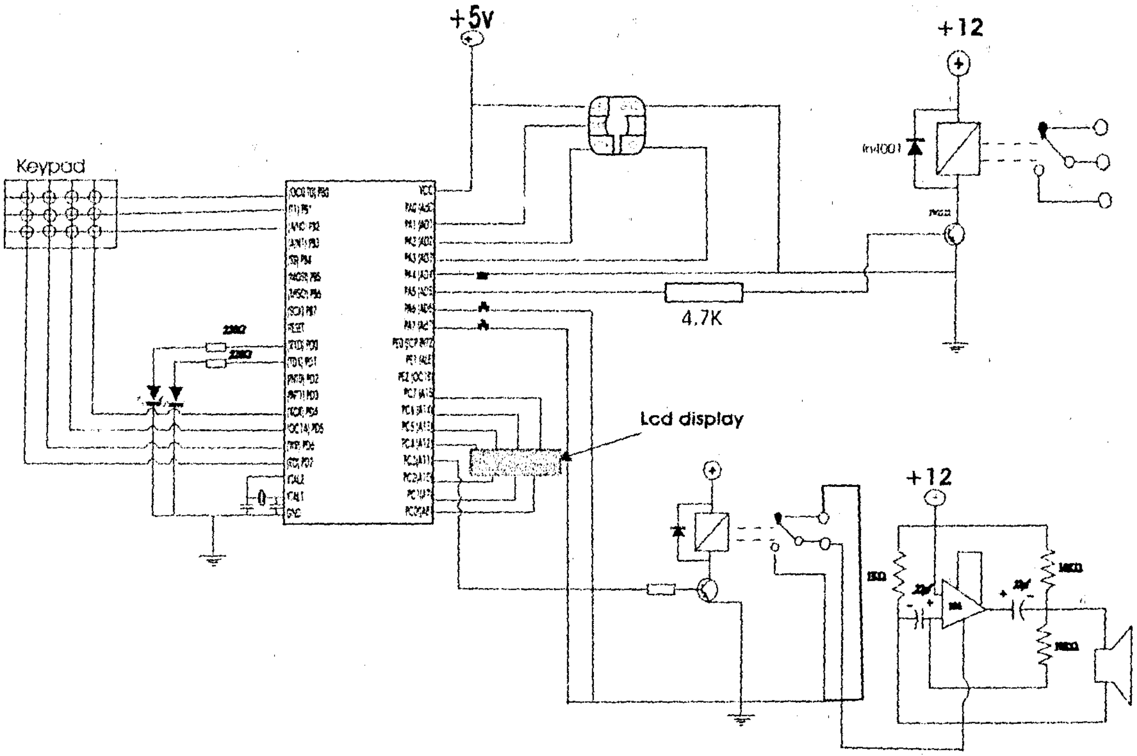

Fig. 3.7 Final circuit diagram.

3.8 DESCRIPTION OF OTHER COMPONENTS USED:

3.8.1 RELAY

A relay is an electromagnetic switch. Applying current causes the electromagnet to become active and pull the contacts together. On the schematic, the electromagnet is the part of the symbol that looks like half a transformer or inductor.

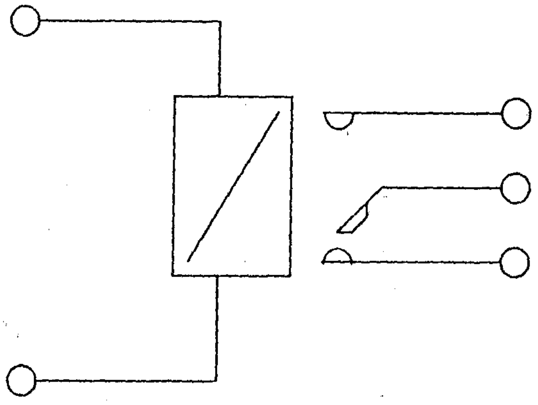

Fig. 3.8 Symbol of a Relay

The contacts are right beside (or above or below) the coil. These contacts can take on any of the normal switch configurations. Pictured here is a simple SPST (or Single Pole Single Throw) relay. This means that the Relay contains one set of contacts and can only be switched one way (on or off). Other types of relays include SPDT (Single Pole Double Throw-A relay with one contact that can be toggled both ways), DPST (Double Pole Single Throw-A relay with two contacts that can only be on or off) and DPDT (Double Pole Double Throw-A relay with two contacts that can be toggled both ways). [5]

3.8.2 CRYSTAL

This component is made of pure quartz and behaves as a quartz crystal resonator, a circular piece of quartz with electrodes plated on both sides mounted inside an evacuated enclosure. When quartz crystals are mechanically vibrated, they produce an

AC voltage. Conversely, when an AC voltage is applied across the quartz crystals, they vibrate at the frequency of the applied voltage. This is known as the piezoelectric effect and quartz is an example of a piezoelectric crystal.

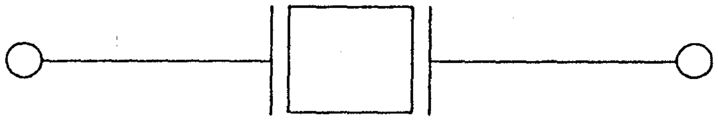

Fig. 3.8.1 Symbol of a Crystal

The piezoelectric characteristics of quartz give the crystal the characteristics of a very high Q tuned circuit. The piezoelectric effect of quartz crystal links the mechanical and electrical properties of the resonator. Electrode voltage causes mechanical movement. Likewise, mechanical displacement generates an electrode voltage.

An equivalent circuit for a crystal shows a large inductor in series with a small resistance and a capacitance. When mounted in a holder with connections, a shunt capacitance is added to the equivalent circuit. The resultant equivalent circuit means that the crystal has both a series and parallel resonant frequency very close together.

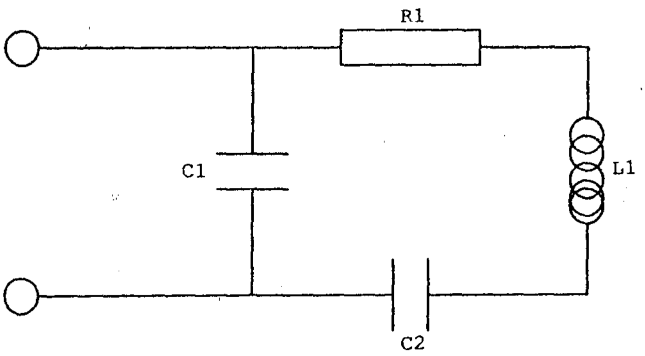

Fig. 3.8.2 Equivalent circuit of a Crystal

Oscillators that employ crystals, typically quartz, offer excellent oscillation frequency stabilities of 0.001 percent. Crystal oscillators are used in digital Wristwatches and in clocks that do not derive their frequency reference from the AC power line. In this project, the crystal (4 MHz) in parallel with two 22pf was used to clock the microprocessor. [5]

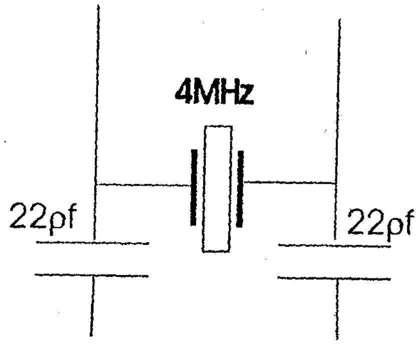

Fig. 3.8.3 Clock source.

CHAPTER FOUR

4.1 TESTING AND RESULTS.

Testing during and at the end of construction is necessary to ensure that not only does the project, but also that it works according to specifications.

In this project every module was bread boarded and tested separately.

4.1.1 TESTING THE ALARM UNIT.

The alarm unit was first bread boarded. And then tested, varying the value of the capacitance at the negative input, a suitable alarm sound was selected so that the alarm could also be used as a keypad tone generator.

It was allocated a section in the vero board that was to hold the final project, and confining it to this section, the alarm unit was then soldered the unit on the vero board.

4.1.2 TESTING THE DISPLAY UNIT.

The display unit consisting of mainly an LCD unit, and a variable resistor was put on a breadboard, and then supplied +5v, the variable resistor was now tuned until blocks appeared on the LCD. This test was just to ensure that the LCD unit was functional and any malfunctioning during display was not due to a faulty display. And hence the cause of the malfunction could be isolated and solved immediately.

The display unit was then soldered on a different vero board so that during casing, it wouldn't be difficult placing it.

4.1.3 TESTING THE POWER SUPPLY UNIT.

Components making up the power supply unit i.e. the transformer, the bridge rectifier, capacitors, 5v and 12v regulators were connected to the bread board, the then the transformer was connected to mains and using a digital meter output voltage was measured to make sure that voltage output was 12v and 5v respectively.

Then it was soldered on the bread board.

4.1.4 FINAL TESTING AND SOLDERING.

The circuit was soldered on the vero board , with positions were the IC sockets placed were the IC's are to placed , then the microprocessor inserted into it' socket. Then the circuit was powered and tested.

4.2 PROGRAMMING SIMULATION AND DEBUGGING.

The program was written in assembly language and the debugged and simulated with the help of an AVR Studio4 IDE software.

AVR Studio is an Integrated Development Environment (IDE) for writing and debugging AVR applications in Windows 9x/Me/NT/2000/XP environments. AVR Studio provides a project management tool, source file editor, chip simulator and In-circuit emulator interface for the powerful AVR 8-bit RISC family of microcontrollers. The program was then burned on the microcontroller using an AVR programmer, and then inserted into the IC socket on the main vero board.

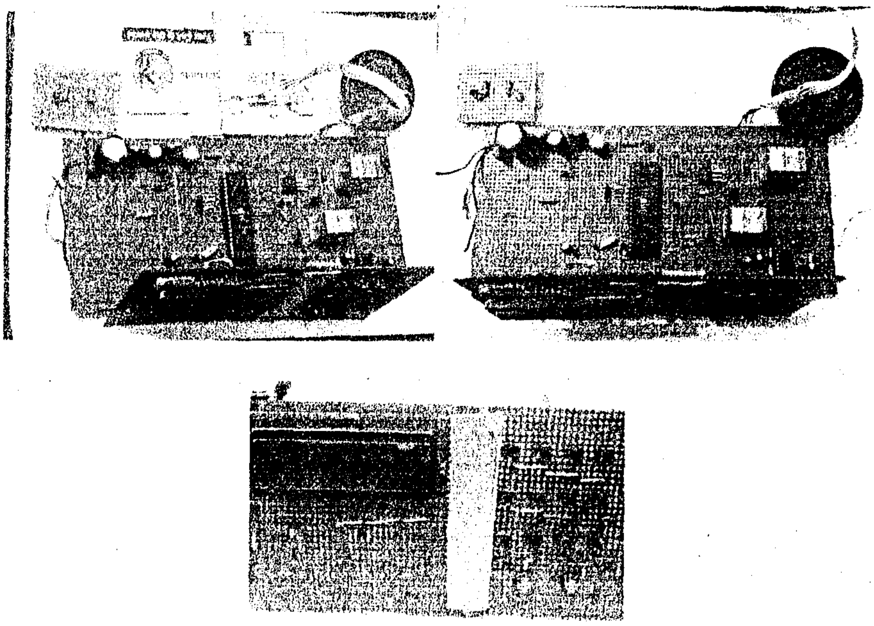

Plate 4.1 Picture of the final construction.

CHAPTER FIVE.

5.1 CONCLUSION, RECOMMENDATION AND PROBLEMS.

5.2 CONCLUSION.

The design and implementation of a microcontroller based electronic safelock with Chipcard and four digit pin as key had been achieved in this project.

This project is only a model, and therefore needs a more detailed analysis and testing than the one carried out if it is to be integrated as security in a facility, building or used as protection to secure devices.

5.3 RECOMMENDATION.

The project been a security feature should be made as small as possible, this could not be achieved in this project because most ideas relating even though not original had to treated as if original. e.g. the construction of the cardreader, even though it could be bought from the market.

Also reduction in size can also be achieved by the use of a printed circuit board, miniature components e.g. using a surface mount microprocessor instead. Also the use of magnetic strip cards are advisable since every bank account holder has one and this, could serve as key, the only disadvantage is the card reader cannot be made locally and has to be bought, therefore whoever is going to undertake this project should be capable of the financial obligations involved.

Also the LCD display unit should have a backlight so that it could be used during the day and at night.

5.4 PROBLEMS ENCOUNTERED.

Problems encountered in this project were unavailability of components, as most of the components had to be ordered untested and at very exorbitant rates, this components, if faulty are at your own risk.

Also the chipcards, which are available as old NITEL phone booth cards are not readily available as phone booths in Nigeria, has virtually vanished since the advent of GSM.

Also the unavailability of funds, greatly limits one's creativity, therefore it is to be recommended that the department should subsidize the costs of projects by making readily available the basic components required, at reduced rates.

REFERENCES.

[1] http://perso.wanadoo.fr/telecard.

[2] http://www.serasidis.gr

[3] http://en.wikipedia.org/wiki/Keycard_lock

[4] V.K. MEHTA, ROHIT MEHTA, principle of electronics, First Multicolour Illustrative and Thoroughly Revised Edition 2005, S. chand and company ltd.

[5] Tom Duncan "Success in Electronics" Longman (1983) pages 44 – 75 & passive components.

[6] www.datasheetcatalog.com.

[7] www.alldatasheet.com.

[8] Luecke G., J.P Mize and application (chapter 3 & 4 general references). Published by Mc Graw- Hill Book Company (1979).

[9] Millman J.; (1979), Microelectronics: Digital and Analogue Circuits and Systems. McGraw-Hill Inc. Singapore, pp 215-216.

[10] B.L THERAJA AND A.K THERAJA, Electrical Technology Twenty Third Revised Edition 2002, S.CHAND and CO.LTD.

Appendix.

Flow chart and Assembly program