ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure End-To-End SMS Communication over GSM Networks

Vattemula Mallesham
M.Tech (Embedded Systems),
Bharat Institute of Engineering and Technology.

N.Raj Kumar
Associate Professor
Bharat Institute of Engineering and Technology.

Introduction

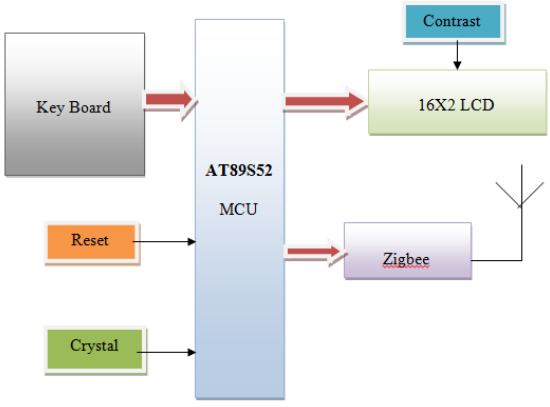
In this project, the data can be transmitted to and received from remote place using GSM communication device. Data Security is primary concern for every communication system. There are many ways to provide security data that is being communicated. However, what if the security is assured irrespective of the hackers are from the noise. This Project describes a design of effective security for data communication by designing standard algorithm for encryption and decryption.

Existing method

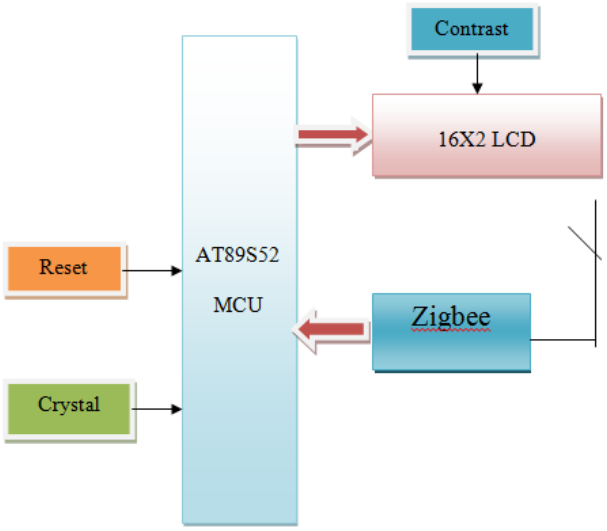
The source information is generated by a key Board and this will be encrypted and is sent to destination through zigbee communication. The receiving system will check the data and decrypt according to a specific algorithm and displays on the LCD.

The zigbee modules used here acts as a Transceiver. Encrypted information at the Transceiver end will send the information to the other end. This decrypted data will be displayed. And note that at the decrypted end the user has to press a special key "Decryption "to get the as it is information on the 16X2 LCD.

Block Diagram: Transmitter – Data Encryption and Decryption



Block Diagram: Receiver – Data Encryption



Draw backs

- Limit range
- Low efficiency

Proposed method:

The source information is generated by PS2 Keyboard and this will be encrypted and is sent to destination through GSM modules. The receiving system will check the data according to a specific algorithm and displays on the LCD.

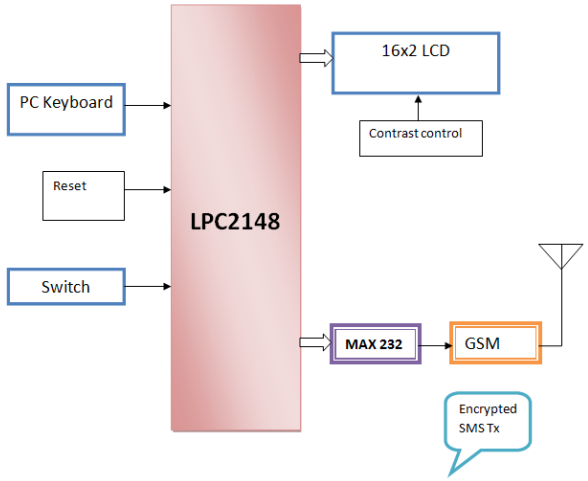
The project is built around the controller in the transmitter and receiver section. This controller provides all the functionality of the display and wireless control. It also takes care of creating different display effects for given text.

Alphanumerical keyboard is interfaced to the transmitter to type the data and transmit. The message can be transmitted to multi point receivers. After entering the text, the user can disconnect the keyboard.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

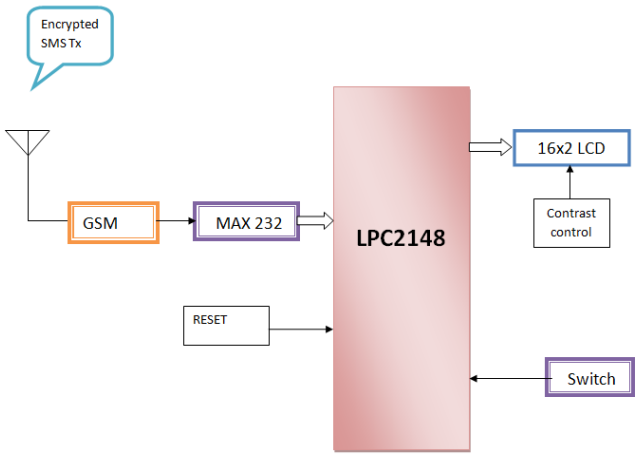
At any time the user can add or remove or alter the text according to his requirement. When ever the message is transmitted to the receiver section the garbage or junk message will be displayed on the receiver section 16X2 LCD. In order to read the original message the user should press the encryption key which is connected in the receiver section.

Transmitter Section:



Encryption Algorithm:- Caesar Cipher

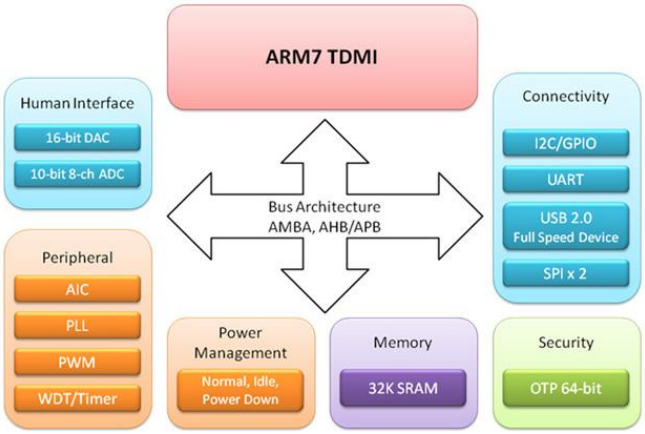
Receiver Section:



Modules used in this project

The **LPC2148** are based on a 16/32 bit ARM7TDMI-S™ CPU with real-time emulation and embedded trace support, together with 128/512 kilobytes of embedded high speed flash memory.

A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at maximum clock rate. For critical code size applications, the alternative 16-bit Thumb Mode reduces code by more than 30% with minimal performance penalty. With their compact 64 pin package, low power consumption, various 32-bit timers, 4- channel 10-bit ADC, USB PORT,PWM channels and 46 GPIO lines with up to 9 external interrupt pins these microcontrollers are particularly suitable for industrial control, medical systems, access control and point-of-sale. With a wide range of serial communications interfaces, they are also very well suited for communication gateways, protocol converters and embedded soft modems as well as many other general-purpose applications.



This project uses regulated 3.3V, 500mA power supply. Unregulated 12V DC is used for relay. 7805 three terminal voltage regulator is used for voltage regulation. Bridge type full wave rectifier is used to rectify the ac out put of secondary of 230/12V step down transformer.

ARM7TDMI Processor Core

- Current low-end ARM core for applications like digital mobile phones
- TDMI
  - T: Thumb, 16-bit compressed instruction set

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- D: on-chip Debug support, enabling the processor to halt in response to a debug request
- M: enhanced Multiplier, yield a full 64-bit result, high performance
- I: Embedded ICE hardware

- Von Neumann architecture

Global System for Mobile Communication (GSM)

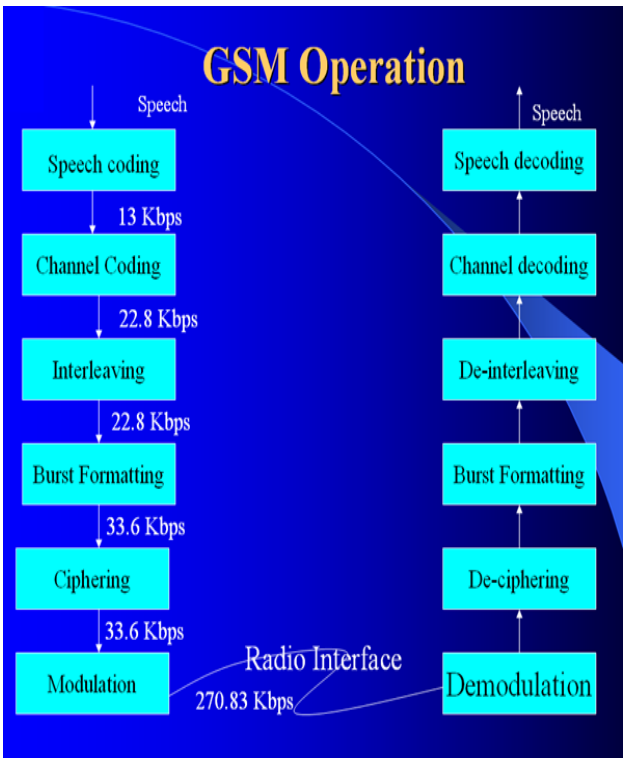
Definition:

GSM, which stands for Global System for Mobile communications, reigns (important) as the world's most widely used cell phone technology. Cell phones use a cell phone service carrier's GSM network by searching for cell phone towers in the nearby area. Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication.

GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership.

General Features:

- Tri-band GSM/GPRS900/1800/1900Mhz
- GPRS multi-slot class 10
- GPRS mobile station class –B
- Complaint to GSM phase 2/2+
  - i. -class 4(2W @900MHz)
  - ii. -class 1(1W @/18001900MHz)
- Dimensions: 40x33x2.85 mm
- Weight: 8gm
- 7. Control via AT commands
- (GSM 07.07, 07.05 and SIMCOM enhanced AT commands)
- SIM application tool kit
- supply voltage range 3.5…….4.5 v
- Low power consumption
- Normal operation temperature: -20 'C to +55 'C
- Restricted operation temperature : -20 'C to -25 'C and +55 'C to +70 'C
- storage temperature: -40 'C to +80 'C



Algorithm used in this project

The Caesar cipher, also known as a shift cipher, is one of the simplest forms of encryption. It is a substitution cipher where each letter in the original message (called the plaintext) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet.

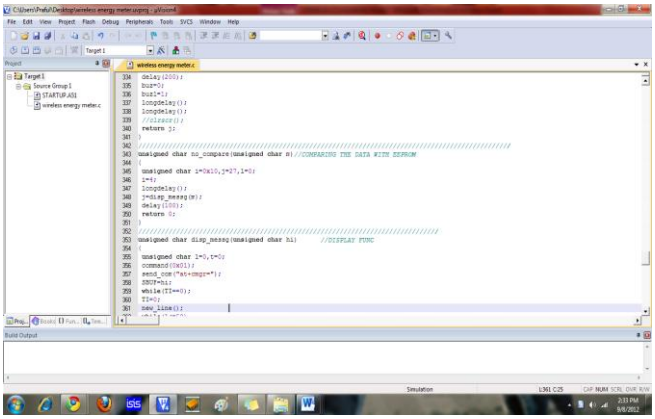
Advantages of using a Caesar cipher include:

- One of the easiest methods to use in cryptography and can provide minimum security to the information
- Use of only a short key in the entire process
- One of the best methods to use if the system cannot use any complicated coding techniques
- Requires few computing resources

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Software tools

Keil compiler is a software used where the machine language code is written and compiled. After compilation, the machine source code is converted into hex code which is to be dumped into the microcontroller for further processing. Keil compiler also supports C language code.



Flash Magic

Flash Magic is a tool which is used to program hex code in EEPROM of micro-controller. It is a freeware tool. It only supports the micro-controller of Philips and NXP. It can burn a hex code into that controller which supports ISP (in system programming) feature. Flash magic supports several chips like **ARM Cortex M0, M3, M4, ARM7 and 8051.**

Advantages

- Wireless System
- Text can be entered from remote place
- Data will not be lost in power failure condition

Applications

- Schools
- Offices
- Courts
- Library

CONCLUSION

Here We Have Designed and implemented **Secure end-to-end SMS communication over GSM networks** Communication with ARM7 LPC2148 controller.

References:

[1] Prof. Rashmi Ramesh Chavan, Prof. Manoj Sabnees "Secured Mobile Messaging" 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[2] Nor Badrul Anuar, Lai Ngan Kuen, Omar Zakaria, Abdullah Gani, Ainuddin Wahid Abdul Wahab "GSM Mobile SMS/MMS using Public Key Infrastructure: m-PKI" WSEAS TRANSACTIONS on COMPUTERS

[3] M. Toorani, A. Shirazi, "SSMS-A secure SMS messaging protocol for the m-payment systems," IEEE ISCC, 2008, pp. 700–705.

[4] Dr. V.K. Govindan & B.S. Shajee mohan "An intelligent text data encryption and compression for high speed and secure data transmission over internet".

[5] M. Hassinen, "Java based Public Key Infrastructure for SMS Messaging," ICTTA, 2006, pp. 88-93.

[6] S. H. Shah Newaz, A Proposal for Enhancing the Security System of Short Message Service in GSM, IEEE International Conference on Anti-counterfeiting Security and Identification, 2008, 235-240.

[7] Mary Agoyi, Devrim Seral, "SMS security: an asymmetric encryption approach", IEEE-20 I 0, 978-0-7695-4 182-211 0 University Science, 1989.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] Na Qi Jing Pan Qun Ding, The Implementation of FPGA-based RSA PublicKey Algorithm and Its Application in MobilePhone SMS Encryption System, IEEE International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2011, 700-703.

[9] Ch. Rupa and P.S. Avadhani, Message Encryption Scheme Using Cheating Text, IEEE International Conference on Information Technology, 2009, 470-474.

[10] Rishav Ray, Jeeyan Sanyal, Tripti Das, Kaushik Goswami, Sankar Das and Asoke Nath, A new Randomized Data Hiding Algorithm with Encrypted Secret Message using Modified Generalized Vernam Cipher Method: RAN-SEC algorithm, IEEE Information and Communication Technologies World Congress, 2011, 1211-1216.

[11] Hongbo Zhou, Mutka and Lionel M. Ni, Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks, IEEE proceedings of GLOBECOM, 2005, 1681-1685.

[12] David Lisoněk and Martin Drahanský, SMS Encryption for Mobile Communication, IEEE International Conference on Security Technology, 2008, 198 – 2011