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

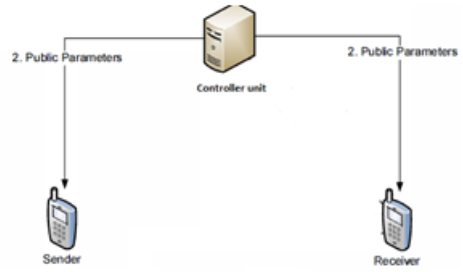
Rajesh Kumar Chinthala
M. Tech in VLSI and Embedded Systems,
Siddhartha Institute of Engineering and Technology.

Dr.D.Subba Rao, M.Tech, Ph.D
HOD,
Department of ECE,
Siddhartha Institute of Engineering and Technology.

E.Swetha
Assistant Professor,
Department of ECE,
Siddhartha Institute of Engineering and Technology.

Introduction:

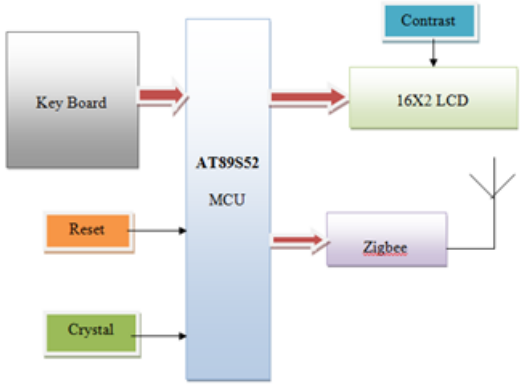
In this project, the data can be transmitted to and received from remote place using GSM communication device. Data Security is primary concern for every communication system. There are many ways to provide security data that is being communicated. However, what if the security is assured irrespective 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.



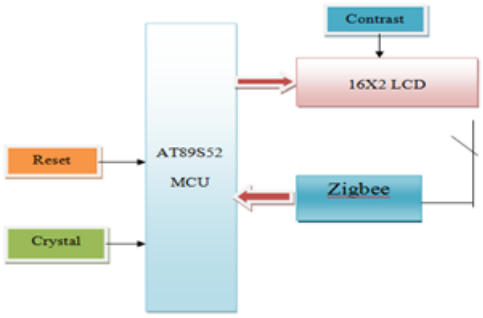
Existing Method:

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

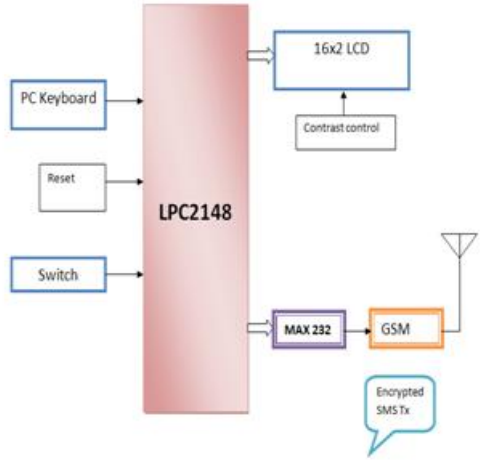
Proposed Method:

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.

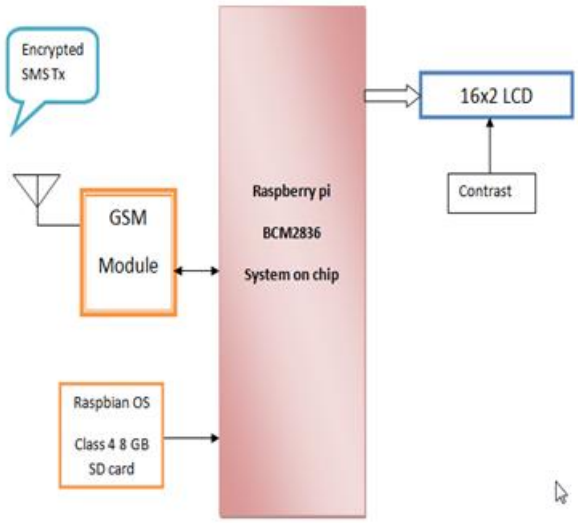
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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



Modules Used in this Project:

RPI:

The Raspberry Pi has a Broadcom BCM2836 system on a chip (SoC), which includes an a quad-core Cortex-A7 cluster. The Cortex-A7 MPCore processor is a high-performance, low-power processor that implements the ARMv7-A architecture.

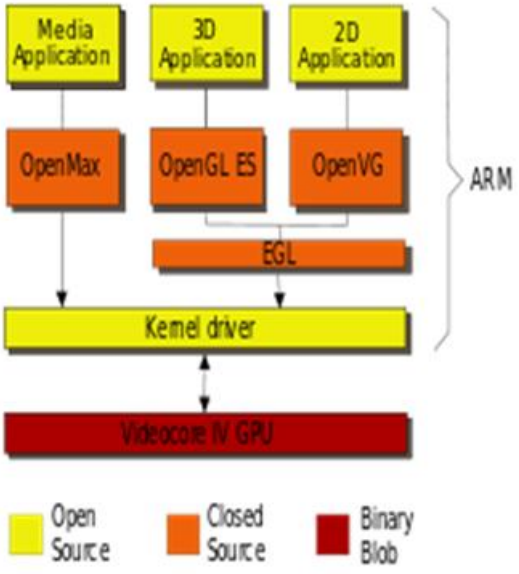
Specifications

Architecture	ARMv7-A
Multicore	1-4 cores. Symmetric Multiprocessing (SMP) within a single processor cluster, and multiple coherent SMP processor clusters through AMBA 4 technology
ISA Support	ARMv7-A Thumb®-2 Trust Zone® security technology NEON Advanced SIMD DSP & SIMD extensions VFPv4 Floating-point Hardware virtualization support Large Physical Address Extensions (LPAE)
Memory Management	ARMv7 Memory Management Unit (MMU)
Debug and Trace	Core Sight™ SoC-400

The GPU hardware is accessed via a firm ware image which is loaded into the GPU at boot time from the SD-card. The firmware image is known as the binary blob, while the associated ARM coded Linux drivers were initially closed source. This part of the driver code was later released, however much of the actual driver work is done using the closed source GPU code. Application software uses calls to closed source run-time libraries (Open Max, OpenGL ES or open VG) which in turn call an open source driver inside the Linux kernel, which then calls the closed source Video core IV GPU driver code. The API of the kernel driver is specific for these closed libraries. Video applications use Open MAX, 3D applications use Open GL ES and 2D applications use Open VG which both in turn uses EGL. Open MAX and EGL use the open source kernel driver in turn.

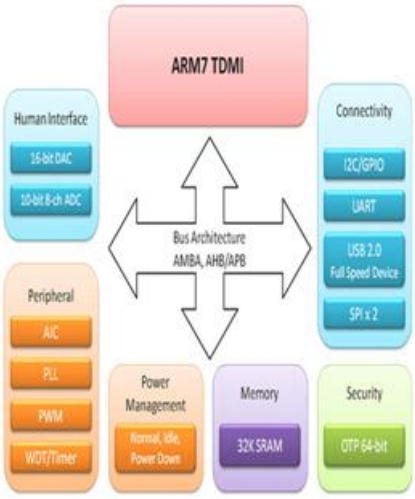
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Diagram of API-Connection:



LPC2148:

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.



ARM7TDMI Processor Core:

- Current low-end ARM core for applications like digital mobile phones
- TDMI

o T: Thumb, 16-bit compressed instruction set
o D: on-chip Debug support, enabling the processor to halt in response to a debug request
o M: enhanced Multiplier, yield a full 64-bit result, high performance
o I: Embedded ICE hardware

- Von Neumann architecture

Global System for Mobile Communication (GSM):

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.

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.

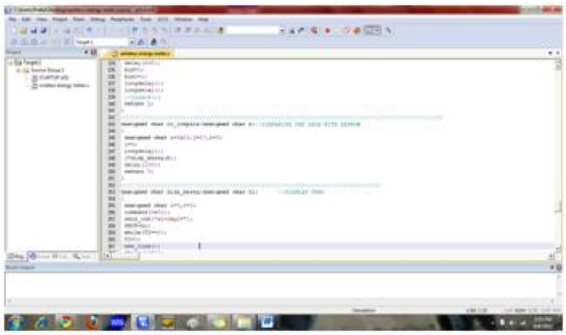
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

Software Tools:

Keil compiler for ARM7 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.



Coding will be done in C/Python language in RPI

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 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.

[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.

Author's Details:

Rajesh Kumar Chinthala

He received his B. Tech in ECE from CMR Institute of Technology Hyderabad affiliated to JNTU, Hyderabad ,A.P, India, and pursuing M. Tech in VLSI and Embedded Systems at Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad affiliated to JNTU, Hyderabad ,A.P, India.

Dr. D Subba Rao

Is a proficient Ph.D person in the research area of Image Processing from Vel-Tech University, Chennai along with initial degrees of Bachelor of Technology in Electronics and Communication Engineering (ECE) from Dr. S G I E T, Markapur and Master of Technology in Embedded Systems from SRM University, Chennai. He has 13 years of teaching experience and has published 12 Papers in International Journals, 2 Papers in National Journals and has been noted under 4 International Conferences. He has a fellowship of The Institution of Electronics and Telecommunication Engineers (IETE) along with a Life time membership of Indian Society for Technical Education (ISTE). He is currently bounded as an Associate Professor and is being chaired as Head of the Department for Electronics and Communication Engineering discipline at Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad.

E. Swetha

Is a M.Tech (Embedded Systems) Assistant Professor in Department of Electronics and Communication from Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad. Her interests of field in Embedded systems, communication and networking systems.