International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | April-2016 www.irjet.net p-ISSN: 2395-0072

Microcontroller Based Cryptosystem Using Rc4 Algorithm

[#1]Prof. Deshpande A.S, [#2]Jagtap Suparna Sunil, [3]Jadhav Mohini Sunil, [#4]Tupe Manisha Macchindra

[#1]Prof. Department of Electronics and Telecommunication
[#234]Department of Electronics and Telecommunication
JSPM Imperial College Of Engineering. And Research, Pune.

ABSTRACT

RC4 is the most widely used stream cipher around. A lot of modifications of RC4 cipher can be seen in open literature. Most of them enhance the secrecy of the cipher and the security levels have been analyzed theoretically by using mathematics. In this paper, a new effective RC4 cipher is propose and the Security analyses has been done using Shannon's Secrecy theories where numerical values are obtained to depict the secrecy. RC4 cipher proposed by Jagtap Suparna, Jadhav Mohini, Tupe Manisha, which were published prior to this work. Combination is done in such a way that the concept used in the modified RC4 algorithm is used in the Improved RC4 cipher. Importantly, an immense improvement of performance and secrecy are obtained by this combination. Hence this particular modification of RC4 cipher can be used in software applications where there is a need to improve the throughput as well as secrecy.

Keywords : **Data encryption, RC4** modifications, Secrecy of ciphers, Stream cipher.

I. INTRODUCTION

The data security plays a central role in the design of future IT systems. Many of those IT applications will be realized as embedded systems which rely heavily on security mechanisms. The large share of those embedded applications will be wireless communication channel. Cryptosystem can still provide security to protect valuable information. The idea of the project is to prohibit the hacking of confidential information and data in IT system which increases the reliability of communication system. The work with implementation of the system to transmit the information without sending the key for decryption, the key automatically generate at the receiver by the use of pseudo random sequence generator. A key is input to pseudorandom bit generator that produces a stream of 8 bit numbers that are apparently random. A pseudorandom stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key. The output of the generator called a key stream is combined one byte at a time with the plaintext stream using the bitwise exclusive OR operation. The transmitter and receiver unit is designed by using RC4 algorithm with stream cipher in which the key is secured from hacker. The goal is to make secured, cost efficient cryptosystem. RC4 is the most widely used stream cipher in the world. It is used in protocols like SSL, WEP, WPA, and applications like Skype, Remote Desktop and Microsoft Point-to-Point. There are many other applications which use RC4 as the encryption algorithm. It is used in hardware based encryption mechanisms as well. Due to its light weight it has become popular despite of various attacks on RC4 [2].. To secure the data and information in proposed system transmission of key is avoiding in order decrypting the data at the receiver node. The objective of cryptography based security is to protect information resources by making unauthorized acquisition of the information or tampering with the information more costly than the potential value that might be gained.

II. LITERATURE SURVEY

The existing system is based on the Tiny Encryption Algorithm which can be implemented in microcontroller to adapt with the real time constraints .The key generation unit need the external memory to handling the key for the cryptography and fetching the data from the external memory is slow and increased hardware complexity. The block cipher allows feasibility for the key generating unit and these generated keys are used for cryptographic applications. Tiny Encryption Algorithm TEA implemented in microcontroller to adapt with many real time constraints such as memory data loss and low cost. It uses Key Generation Unit to produce the random key to make it optimal for sensitive data transfer in many real time applications. This system uses microcontroller and the performances of this cryptosystem is analysed by implementing the cryptographic algorithm TEA with key generation unit which offers moderate security and simplicity in implementation process.

TEA operates on two 32 bit unsigned integers and uses a 128 bit key. It has a Feistel structure with a suggested 64 rounds typically implemented in pairs termed cycles. It has an extremely simple key schedule mixing all of the key material in exactly the same way for each cycle.

III. PROPOSED SYSTEM

This project relates to communications and more particularly to wireless crypto graphic communication systems and methods. It aims to integrate the area of wireless embedded communication systems and cryptography. Although the system can transfer any type of file, cryptography is implemented only to text files due to the limitation of memory and processing speed of an 8 bit microcontroller. The radio operates within the 2.4 to 2.48 GHz band, the unlicensed Industrial Scientific and Medical band. The wireless communications channel is coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. The PIC microcontroller acts as the encoding and decoding device. A message to be transferred is enciphered to cipher text at the encoding terminal by means of RC4 stream cipher algorithm.

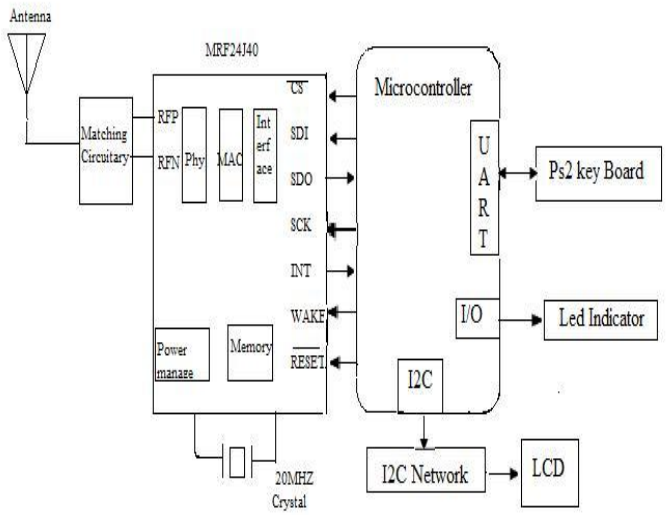


Fig 1. Data Transmitting Node

The cipher text is deciphered to the original message at the decoding terminal. RC4 cryptography involves a 64 bit key. It also involves pseudo random number generator. The transmitter and receiver must be accurately synchronized for this type of type of cryptographic algorithm. IEEE802.15.4 protocol is intended for battery operated devices since it consumes very less power.

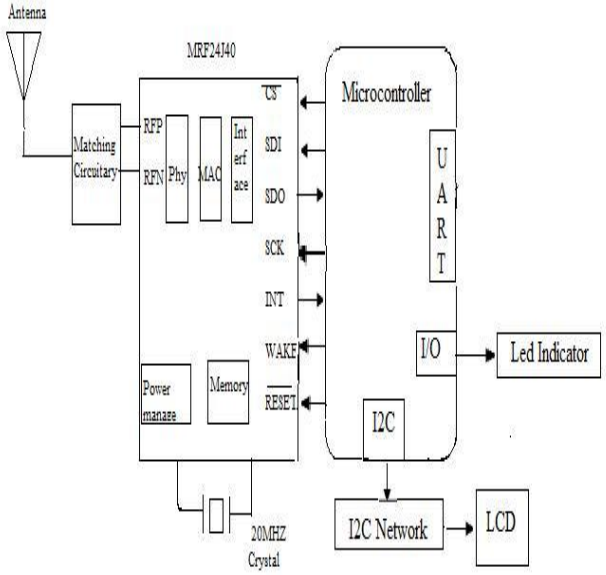


Fig 2. Data Receiving Node

There are three units. They are sender, receiver and hacker.
The following are the blocks of these units:

i. PIC Microcontroller
ii. UART
iii. I2C
iv. I2C Network
v. LCD
vi. RF Transceiver
vii. SPI

i. PIC MICROCONTROLLER

PIC Microcontroller is a low power and high performance 8 bit MCU with pe-ripheral flexibility in a small package for cost sensitive applications in the PIC18J se-ries. It is designed with RISC architecture. The PIC18F45J11 is ideal for applications requiring cost effective low power solutions with a robust peripheral set in a small package. The security algorithm for secure data transmission is written and loaded in the microcontroller. It performs encryption and decryption of data and information at sender and receiver node. The microcontroller unit is connected with UART, I2C, PS2 keyboard and transceiver unit.

ii. UART

The Universal Asynchronous Receiver and Transmitter are interfaced with Ps2 key-board. The data is loaded into the microcontroller by the keyboard and UART inter-face. The heart of the transmitter is the transmit shift

register. The shift register obtains its data from the read/write transmit buffer TXREG. The TXREG register is loaded with data in microcontroller.

iii. I2C

I2C is a serial peripheral interface to a motherboard embedded system. The I2C bus physically consists of 2 active wires and a ground connection. The active wires called SDA and SCL are both bi directional. SDA is the Serial data line and SCL is the Seri-al Clock line. Each of these chips can act as a receiver and/or transmitter depending on the functionality. The I2C bus is a multi-master bus in which more than one IC ca-pable of initiating a data transfer can be connected to it. The I2C protocol is connected to the I2C network, which is an expander IC and hence with the LCD display.

iv. I2C NETWORK

The I2C Network is a silicon CMOS circuit. It provides general purpose re-mote I/O expansion for microcontroller through the two-line bidirectional I2C bus. The PCF8574 has a low current consumption and includes latched outputs with high current drive capability for directly driving LEDs. The interrupt line of I2C network is connected to the interrupt logic of the microcontroller. By sending an interrupt signal on this line, the remote I/O can inform the microcontroller if there is incoming data. The I2C expander IC provides 16 pins to the LCD display and saves the important pins of microcontroller for future use and connections.

v. LCD

The 14 pin LCD display with 20 rows and 4 columns are used to display the da-ta characters such as string, integer and characters. The encrypted data and respective string of pseudorandom keys are displayed on it.

vi. SERIAL PERIPHERAL INTERFACE

Serial Peripheral Interface is a simple interface which enables to communicate microcontroller and transceiver. SPI bus consists of four signal wires:

a. Master Out Slave In
b. Master in Slave Out
c. Serial Clock
d. Chip Select for the peripheral.

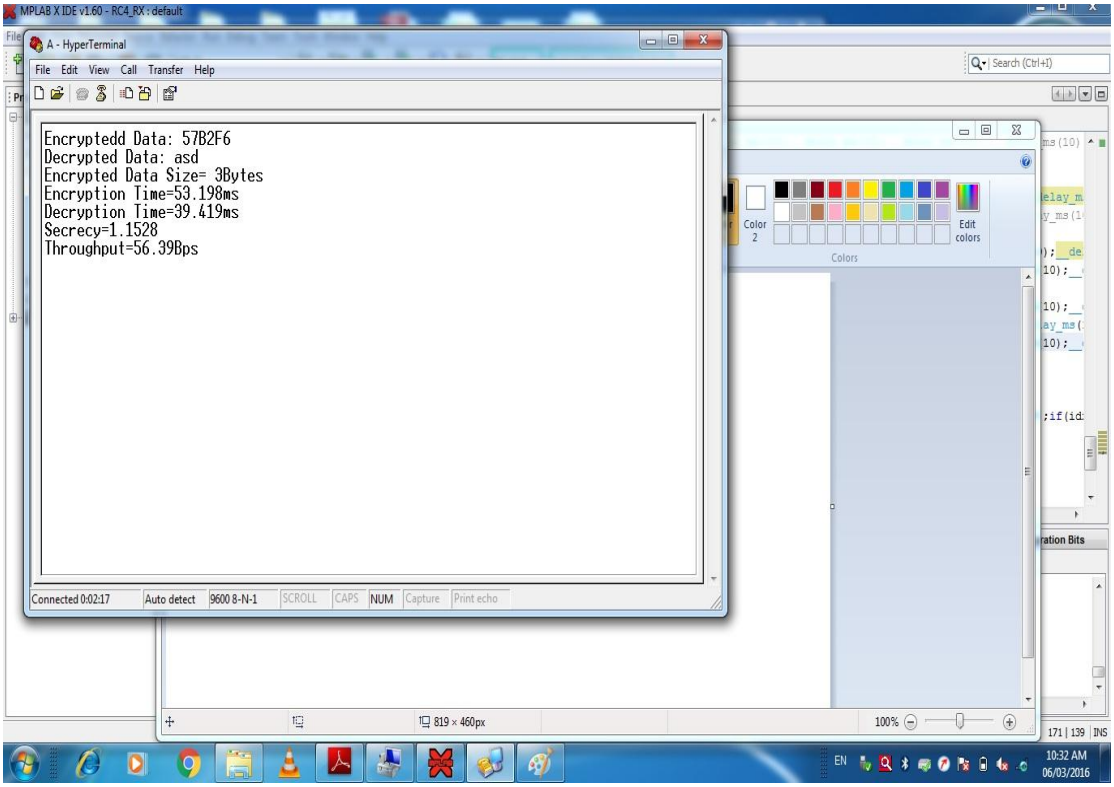
The master controller initiates the data transfer by sending the SCK signal. Data is shifted out of both shift registers on their programmed clock edge and latched on the opposite edge of the clock. Both processors are programmed to the same Clock. Whether the data is meaningful depends on the application software.

vii. RF TRANSRECEIVER

The MRF24J40MA is a 2.4 GHz IEEE Std. 802.15.4 compliant surface mount module with integrated crystal internal voltage regulator matching circuitry and PCB antenna. The protocol provides reliable direct wireless communication via an easy to use programming interface. The encrypted data and information from sender node is transmitted and received at the receiver through this transceiver in wireless communi-cation medium. The microcontroller unit is interfaced with transceiver for sending the encrypted data and information through transport layer. The crystal oscillator con-nected with it generates the pulses for performing the operation. The transceiver con-tains temporary memory unit for fetching the data as well as hold it during busy peri-od of transmission. It also holds the internally generated Pseudo random key. The matching circuitry matches the impedance of transceiver and antenna and transform the data depends upon the transmission medium.

IV Result

Hyper Terminal output:



V. CONCLUSION

The project "Microcontroller Based Cryptosystem Using Rc4 Algorithm" can successfully develop and implement with the least cost components. The project was successfully able to work up to the radius of 300m around the kit using ISM band. The experimental setup has three nodes, which can be emulated with different distance to evaluate the performance of the proposal. The correctness of the results has been checked and secure transmission is done. The specifications were all met according to the design and the cryptanalysis is made difficult for the hacker.

REFRENCES

[1] P. Israsena, Thailand IC Design Incubator, National Electronics and Computer Technology Center, Thailand Science Park, Thailand. "Design and Implementation of Low Power Hardware Encryption for Low Cost Secure RFID Using TEA".

[2] Thomas Eisenbarth, Sandeep Kumar and Axel Poschmann, Department of Infor-mation Technology,Ruhr University Bochum. "A Survey of Lightweight Cryptog-raphy Implementations

[3] Eka Stuwarad, CandraGunawan, Ary Setijadi, Carmadi Machbub, Laboratory for Control and Computer Systems, Department Of Electrical Engineering, Bandung In-stitute
Of Technology, "First Step toward Internet Based Embedded Control System"

[4] Devesh C. Jinwalaldhiren, R. Patelkankar, S. Dasgupta, Department of Computer Engineering, National Institute of Technology, surat. "Investigating and Analyzing the Light weight ciphers for Wireless Sensor Networks"

[5] Dalel BouslimiMember of IEEE Gouenou CoatrieuxMichel and Christian rouse, Nigeria. "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images"

[6] Nico Dottling Rafael Dowsley Jorn Muller Quade and Anderson C. A. Nascimen-to, "A CCA2 Secure Variant of the McEliece Cryptosystem"

[7] A. G. Chefranov Eastern Mediterranean University, Famagusta, North Cyprus and Taganrog State University of Radio Engineering, Taganrog "Pseudo-Random Number Generator RC4 Period Improvement.

[8] Jun-Dian Lee and Chih-Peng Fan,Department of Electrical Engineering, National Chung Hsing University"Efficient Low Latency RC4 Architecture Designs for IEEE 802.11i WEP/TKIP".