ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 4, Issue 11, November 2016

# Design of Public Key Cryptosystem Using RSA Algorithm

K. Bala Teja[1], U.V. Ratna Kumari [2]

M.Tech Student, Dept. of E.C.E., University College of Engineering Kakinada, Kakinada, Andhra Pradesh, India

Associate Professor, Dept. of E.C.E., University College of Engineering Kakinada, Kakinada, Andhra Pradesh, India

**ABSTRACT:** Cryptography is the science of protecting data and Network Security by keeping information private and secure from unauthorized users. One of the principal challenges of resource sharing on data communication network is its security. This is stated on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. One of the widely using cryptography techniques is Public-key cryptography which refers to a cryptography system that requires two different keys, one of which is secret and the other one is public. This paper presents the design of a data encryption and decryption process in a network environment using RSA algorithm with a specific message block size. This algorithm allows the information sender to generate both public and privates keys for encryption and decryption.

**KEYWORDS**: Cryptography, Encryption, Decryption

## I. Introduction

Cryptography is the science of securing data, which provides the means and methods for converting the data into unreadable form, so that only the valid user can access information at the destination. Cryptography technique is the science of using mathematics to encrypt and decrypt the message, it allows you to store the sensitive information or transmit it over unassertive networks (like the Internet) so that it cannot be read by anyone except the preconceived recipient [1]. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication.

Cryptography is an interesting subject and is of great importance in most technology today, from computers to credit cards and government to e-commerce. The message transferred from one system to another over public network can be secured by the method of encryption. In encryption process, the message is encrypted or scrambled by any of the encryption algorithm using the ‘key’. Only the users having the access to the same key can decrypt/de-scramble the encrypted message. This process is known as private key or symmetric Key Cryptography. There are several other standard symmetric key algorithms explicated. Examples are AES, 3DES etc. [1]. Thesedefined standard symmetric algorithms are proven to be highly safe and secured and also time tested. But the only problem with these algorithms is the exchange of key. The communicating parties need a shared secret ‘key’, to be exchanged between them to have a secured transmission. The safety of the symmetric key algorithm depends on the secrecy of the key. These Keys are typically hundreds of bits in length, depending on the algorithm used [2]. Since there ismore number of intermediate points between the communicating parties through which the message need to be passed, these keys cannot be transferred in online in a secured manner. In a large network, where there are thousands of systems are connected, offline key exchange seems too difficult and even unrealistic [2]. At this point public key cryptography comes to help. Using public key cryptosystem a shared secret can be established online between communicating parties without the necessity for exchanging any secret data.

## II. Related work

Public-key cryptography has been said to be the most significant new development in secure communication over a non-secure communications channel without having to share a secret key. Public Key Cryptography or Asymmetric cryptography provides the same message security guarantees as symmetric cryptography, but additionally provides the

DOI: 10.15680/IJIRCCE.2016. 0411065

non-repudiation guarantee. ‘Asymmetric’ refers to the fact that different keys are used for encryption and decryption. One key is kept secret (secret key) for decryption and the other is made public (public key) which is used for decryption [1]. The recipient’s public key should be used during the encryption process to ensure message confidentiality as only the recipient has the necessary secret key to decrypt the message. If however, the message is encrypted using the sender’s private key the sender cannot deny sending the message as his private key is unique and is only known to him [3].

Public-key cryptography serves both to authenticate a message and ensure its privacy, soit's essential that you know that the public key you are using to encrypt a message does belong to a specific person or entity. This has led to the creation of a public-key infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify the ownership of key pairs [1]. A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact [3]. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information.

## III.PROPOSED ALGORITHM

Several algorithms in common employ public-key cryptography, probably the best known being the RSA algorithm named after its inventors, Ronald Rivest, Adi Shamir and Leonard Adleman.Its principle is, if user A need to send information to user B, he can take the user B’s encryption key (public key) firstly. Then encrypt plaintext into cipher text through the encryption function and transfer it to user B. If user B receives this cipher text from user A, he will decrypt cipher text with decrypting function through their decryption key (private key). Figure 1 shows the scenario to be followed in RSA Algorithm.

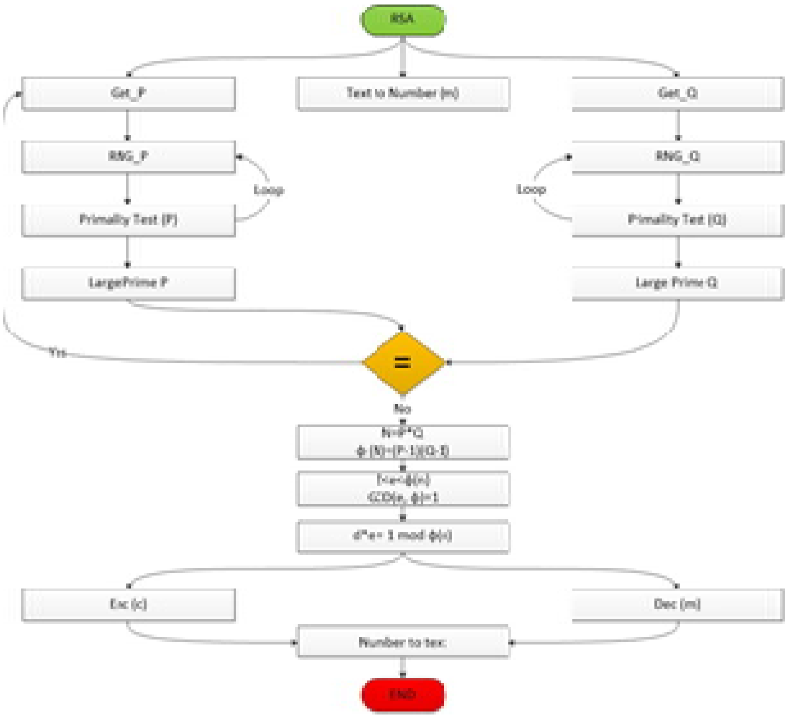

Figure 1: Flowchart of complete RSA Algorithm

DOI: 10.15680/IJIRCCE.2016. 0411065

The implementation process of RSA Algorithm contains following stages

### *A. PSEUDO RANDOM GENERATOR*

To implement the RSA cryptosystem it is need to generate two random numbers. For generating the random numbers Linear Feedback Shift Register (LFSR) is used. Linear Feedback Shift Register is one of the most promising techniques used to generate pseudo random numbers. It generates a periodic sequence so that the numbers generated by the LFSR will be repeated only after certain interval. Linear feedback shift register can generate a (2n-1)-bit long random sequence without repeating. It can produce a sequence of over 4 billion random bits. In this paper the RSA algorithm contains 32 -bit LFSR. This LFSR consists of 32 registers and one XOR gate. It performs a XOR operation between the certain inputs and feedback the output to 32nd register. The random numbers that are generated from LFSR are stored in FIFO and it stops working when it’s full. The numbers from the FIFO are given as input to the primality tester and check for the number to prime. If the number is found to be prime number then it is saved or else the number is discarded. This process is repeated until two prime numbers are obtained.

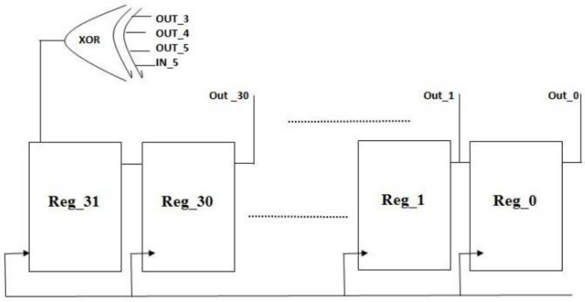

Figure 2: Pseudo random number generator

### *B. PRIMALITY TEST*

The pseudo random numbers which are generated by the LFSR may contain both composite and prime numbers. But algorithm need only prime numbers to implement the RSA cryptosystem. The basic purpose of the primality test is to find whether the random number generated by the LFSR is prime number or not. The Miller-Rabin probabilistic primality test is one of the fast methods to determine the prime number. This process is stopped as soon as two prime numbers are obtained. The flow chart for the primality test is shown in figure 2 below

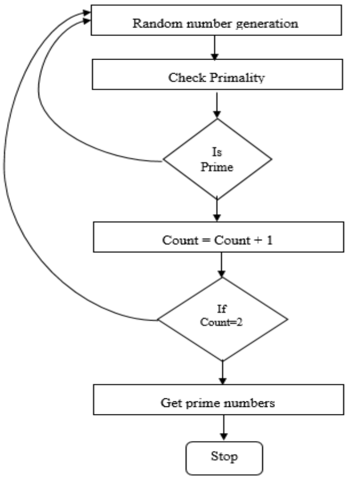

Figure 2: Flowchart for Primality test

The pseudo code for the Miller- Rabin test is as follows

```
Write n-1 as 2s*d with d odd by factoring powers of 2 from n-1
LOOP: repeat k times:
Pick a randomly in the range [2, n − 1]
x ← ad mod n
If x = 1 or x = n − 1 then do next LOOP
For r = 1... s − 1
x ← x2 mod n
If x = 1 then return composite
If x = n − 1 then do next LOOP
return composite
return prime
```

This algorithm doesn’t need any even numbers hence the even numbers generated by the LFSR are eliminated and feed the odd numbers as input to the primality test. The odd integer from the LFSR to which primality to be tested is considered as the integer ’n’ and another integer k is chosen between 2 and n-1 which determines the accuracy of the test. If the result of any round is 1 then the number is composite and if it is n-1 then it’s a prime number.

### *C. KEY GENERATION*

In RSA algorithm two separate keys are generated namely encryption key ’e’ and decryption key’d’. At first, two prime numbers (p, q) are taken from the primality tester. By applying some mathematical operations on these two prime numbers the values of n and Φ(n) are calculated , where n=p*q and Φ(n) = (p-1)*(q-1). Now select the value for ‘e’ such that it is relatively prime to Φ(n) i.e. GCD of (e, Φ(n) ) =1,and the value of ‘e’ should be less than Φ(n), thus it is required to calculate the value decryption key ‘d’ which satisfies the following equation 1

$$d*e \bmod \Phi(n) = 1 \qquad (1)$$

The following block diagram gives the scenario of the key generation of the RSA Cryptosystem.

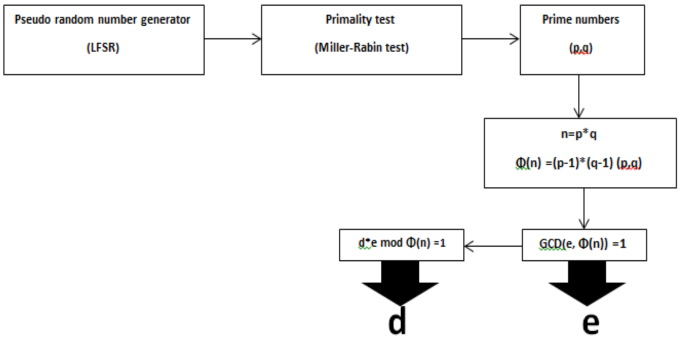

Figure 3: Flowchart for key generation

The Euclidean algorithm is used for finding theGCD of two numbers A and B.The Euclidean Algorithm for finding GCD (A, B) is as follows:

A. If A = 0 then GCD(A,B) =B, since the GCD (0,B) =B.

B. If B = 0 then GCD(A,B) =A, since the GCD (A,0) =A.

C. Write A in quotient remainder form (A = B·Q + R).

D. Find GCD(B, R) using the Euclidean Algorithm since GCD(A,B) = GCD(B, R).

### *D. ENCRYPTION / DECRYPTION*

The data or messages which need to be transmitted from one system to another system over any medium are needed to be encrypted to secure the data from the eavesdroppers or hackers. Encryption is the process of converting the plain text into the cipher text, and it is done by using the encryption key generated in the previous step. RSA encryption is done by using the following mathematical expression. The cipher text is represented by 'C' and the plain text is represented by 'M.

$$C = M^{e} \text{ modn} \qquad (2)$$

When the data or messages are received at another end, the cipher text has to recovered or it need to be converted to the original message 'M'and it is done by decryption. Decryption is the process of converting the encrypted text to the plain text, and the decryption is done by using the decryption key 'd' generated in previous stepRSA decryption is done by using the following mathematical expression.

$$M = C^{d} \text{ modn} \qquad (3)$$

The basic block diagrams of the RSA encryption and decryption are shown in the following figures

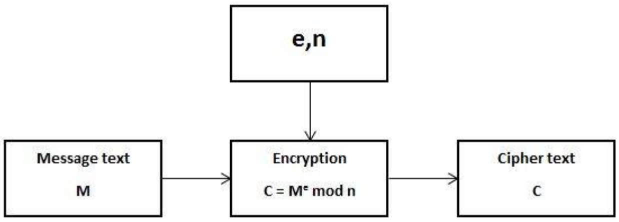

Figure 4: Block diagram of RSA encryption

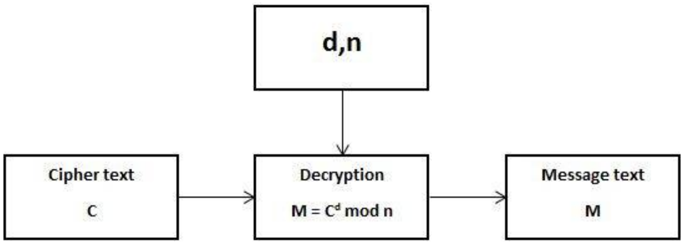

Figure 5: Block diagram of RSA decryption

Both the RSA encryption and decryption process are modular exponentiation which includes modular addition and modular multiplication. In this paper modular exponentiation is simplified by using the square-multiply algorithm, and it is done by using the left-to-right-binary method. The main purpose of using theleft-to-right-binary method is to calculate the modular exponential terms like $M^{e}$ or $C^{d}$. In this method of approach the exponentiation operation is divided into a series of squaring and multiplication. This process speeds up the calculation and reduces the number of clock cycles needed for the operation. Theleft-to-right-binary exponentiation algorithm or the LSB exponentiation algorithm starts from the least significant bit position ad it calculates the exponential term and proceeds to the most significant bit. This algorithm works on the principle of scanning the each bit from left to the right i.e., for every iteration, if the scanned exponent bit is 1, the current result is squared and multiplication of current result with M is followed by squaring.

## IV. SIMULATION RESULTS

Linear feedback shift register, Miller-Rabin test, the Euclidean algorithm and the left-to-right-binary exponentiation algorithm have been successfully implanted using the Verilog Compiler and Simulator (VCS) Tool. The simulation shows the desired results for these algorithms and simulation results for these algorithms are shown in figure.6.

### A. *LINEAR FEEDBACK SHIFT REGISTER*

The pseudo random numbers are generated using the 32-bit linear feedback shift register and it is simulated in VCS tool.

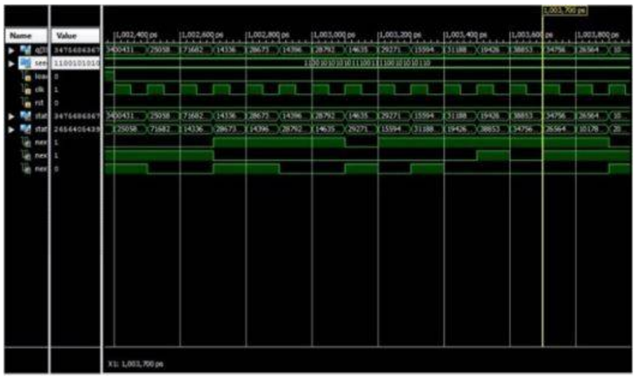

Figure.6 shows some 32 bit random numbers which are generated using 32-bit linear feedback shift register.

### B. *PRIMALITY TESTER*

The primality testing is implemented by using the Miller-Rabin algorithm and it is simulated using VCS tool.

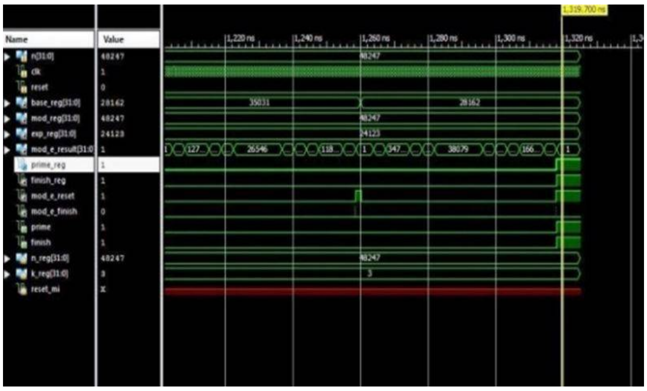

Figure 7: Simulated waveform for Miller-Rabin test

Figure.7 shows some values have been calculated for to find out whether prime number or not and the output is 1 for the prime number and 0 for the composite number.

### C. *KEY GENERATION*

The Euclidean algorithm is used to calculate the GCD for finding the encryption key and modular inversion operation is also used to calculate the decryption key. These are simulated in VCS tool and the following figure.8 shows the simulated waveforms of the key generation process.

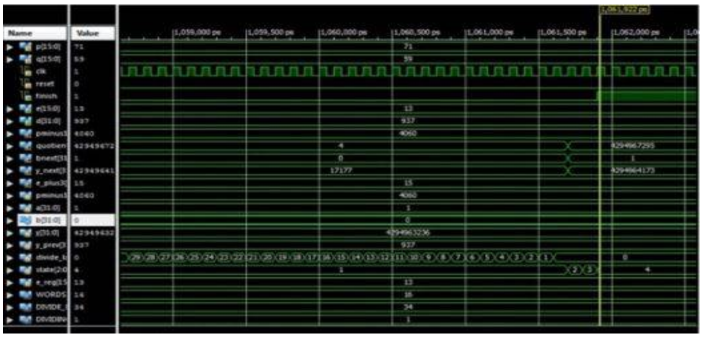

Figure 8: Simulated waveforms of Euclidean algorithm

The waveforms in the above figure shows the Euclidean algorithm for the calculation of GCD and modular inverse shows that the two inputs given are p=71,q=59, and as a result these algorithms gives output e13=,d=937.

### *D. ENCRYPTION/DECRYPTION*

Both RSA encryption and decryption involves the modular exponentiation operation hence the left-to-right-binary exponentiation algorithm or LSB algorithm is used to solve it. The simulated waveforms of encryption and decryption process are shown in below figure.9 and figure.10 respectively.

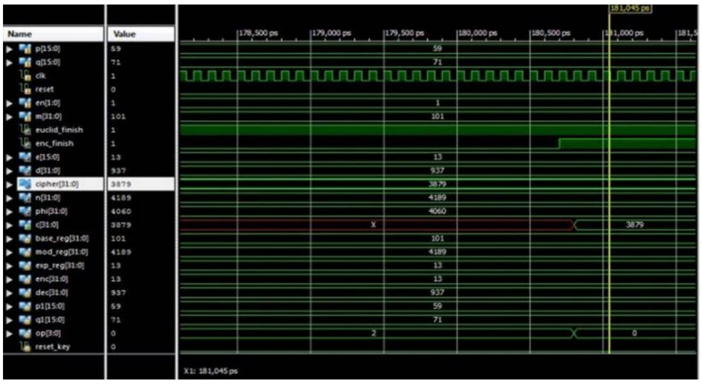

Figure 9: Simulated waveforms of Encryption process

Figure.9 shows the encryption of message text to cipher text, where the message text is 101 and n is set to 4189 .the exponent term i.e., encryption key is 13.

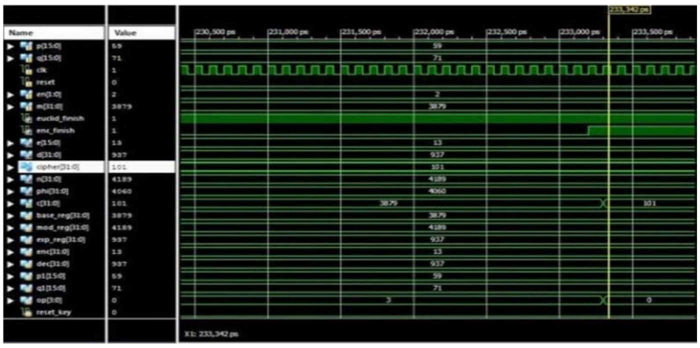

Figure 10: Simulated waveforms of Decryption process

Figure.10 shows the decryption of cipher text to message text, but for the decryption process n remains same and the exponent term i.e., decryption key changes to 197, the cipher text is 3879.

## V. CONCLUSION AND FUTURE WORK

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the sender of an electronic message to verify the receiver, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transit. This paper describes the cryptographic concepts of symmetric key encryption, public-key encryption, and RSA algorithm. RSA algorithm is a bit slower when compared to the other, but it is much more secure than symmetric key algorithms. Cryptography is a particularly interesting fieldbecause of the amount of work that is, by necessity,done in secret. The strength of cryptography lies in the choice of the keys; longer keyswill resist attack better than shorter keys.

## REFERENCES

1. Networks Qasem Abu Al-Haija*, Mashhoor Al Tarayrah, Hasan Al-Qadeeb and Abdulmohsen Al-Lwaimi. “A Tiny RSA Cryptosystem based on Arduino Microcontroller useful for small scale”. International Symposium on Emerging Internetworks, Communication and Mobility (EICM 2014).
2. [Zafar Jafarov, The use of Cryptography in Network Security “Information Technology and Programming" department, Azerbaijan Technical University, Azerbaijan, Baku.
3. Na Qi Jing Pan Qun Ding,”The implementation of FPGA-based RSA public-key algorithm and its application in mobile-phone SMS encryption system “, 2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control.
4. R.Bhaskar, Ganapati Hegde, P.R.Vaya, “An efficient hardware model for RSA Encryption system usingVedic mathematics”, International Conference on Communication Technology and System Design 2011.
5. [AnkitAnand, Pushkar Praveen, “Implementation of RSA Algorithm on FPGA”, International Journal of Engineering Research& Technology (IJERT), Vol. 1 Issue 5, July – (2012).
6. REUTERS. Aramco Says Cyberattack Was Aimed at Production. Saudi Aramco Company, December 9, 2012,
7. Richard A.Mollin. An Introduction to Cryptography: 2nd edition. Chapman and Hall/CRC, ISBN-10: 1584886181, 2006 pp 37-39.
8. Like Zhang, Gregory B. White, ―Anomaly Detection for Application Level Network Attacks Using Payload Keywords‖, Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007).
9. SuhailaOrner Sharif, S.P. Mansoor, ―Performance analysis of Stream and Block cipher algorithms‖, 3$^{rd}$International Conference on Advanced ComputerTheory and Engineering (ICACTE), 2010.
10. Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.
11. Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.
12. Q. Abu Al-Haija, et. al. Hardware and Software Simulation for Classical Cryptosystems. 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-13), Ontario, Niagara Falls, Canada, 21-24, Oct-2013.

## BIOGRAPHY

**Bala TejaKatam**is M.tech studentin Electronics and Communication Engineering Department, University college of Engineering Kakinada, Kakinada Andhra Pradesh, India. He received Bachelor of Engineering (BE) degree in 2014 from Sir C R Reddy College of Engineering, Eluru Andhra Pradesh, India. His research interests are VLSI, Communication, Algorithms, etc.

Smt. **U.V.Ratna Kumari** received B.Tech from Acharya Nagarjuna University and M.Tech from Andhra University. At present she is working as Associate Professor in the Department of ECE University college of Engineering Kakinada, JNTUK, She is in the teaching field for the last 16 years. Her research area of interest are Electromagnetic fields, Antennas and wave Propagations, Microwaves, Radar Signal Processing and EMI/EMC . She is a Life member of EMC Engineers, Fellow of IETE.

DOI: 10.15680/IJIRCCE.2016. 0411065