COMPARATIVE ANALYSIS OF RSA AND MODIFIED RSA CRYPTOGRAPHY

By

MADHURIMA DUBEY * YOJANA YADAV **

* PG Scholar, Department of Electronics and Telecommunication Engineering, Chhatrapati Shivaji Institute of Technology, Durg, India.
** Associate Professor, Department of Electronics and Telecommunication Engineering, Chhatrapati Shivaji Institute of Technology, Durg, India.

ABSTRACT

In RSA (Rivest-Shamir-Adleman) cryptography, the basic factors are key length, calculation time, security, authentication and integrity. Generally, in public key cryptography, the key length and security is directly proportional to each other. Original RSA uses two prime numbers as input, which gives the modulus 'n'; encryption and decryption process depends on modulus 'n'. The attacker can easily break the 'n' into two factors of prime number and so to avoid this problem, the authors have used three large prime numbers, it will increase the brute force time to factorize 'n'. This paper mainly focuses on the number of prime numbers used, security and time.

Keywords: RSA Algorithm, Public Key Cryptography, Encryption, Decryption.

INTRODUCTION

Cryptography is playing a major role in data protection applications running in a network environment. It allows people to do business electronically, without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender [26]. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc, [1], [3]. The development of public-key cryptography has enabled large-scale network of users that can communicate securely with one another even if they had never communicated before. This paper considers a Public Key encryption method using RSA algorithm that will convert the information into a form not understandable by the intruder, therefore protecting the unauthorized users from having access to the information even if they are able to break into the system [8], [25].

Cryptography is defined from two Greek words Crypto and Graphy; Crypto means Hidden and Graphy means writing. It is the study of techniques for secure communication in the presence of third party [4], [28]. Figure 1 shows the description of cryptography.

Cryptography is basically classified in to two types -

- Symmetric Key Cryptography.
- Asymmetric Key Cryptography [16].

Figure 2 describes the types of cryptography on the basis of key.

Symmetric Key Cryptography

Symmetric-key algorithms use the same cryptographic keys for both encryption of the plain text and decryption of the cipher text as shown in Figure 3 [27], [28]. The keys may be identical or there may be a simple transformation to go between the two keys.

Asymmetric Key Cryptography

Asymmetric cryptography or public-key cryptography is a cryptography in which, a pair of keys is used to encrypt and decrypt a message so that, it arrives securely as shown in Figure 4 [27]. Initially, a network user receives a public and private key pair from a certificate authority.

1. Literature Survey

1.1 A Survey and Performance Analysis of Various RSA based Encryption Techniques

Sarika Khatarkar and Rachana Kamble [2] have studied

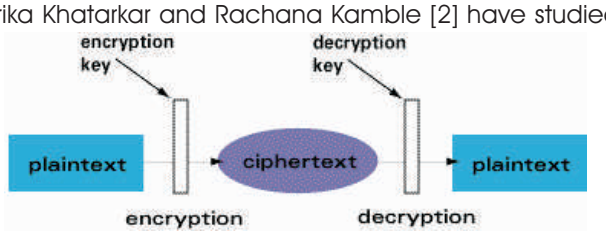

Figure 1. Basic Diagram for Cryptography

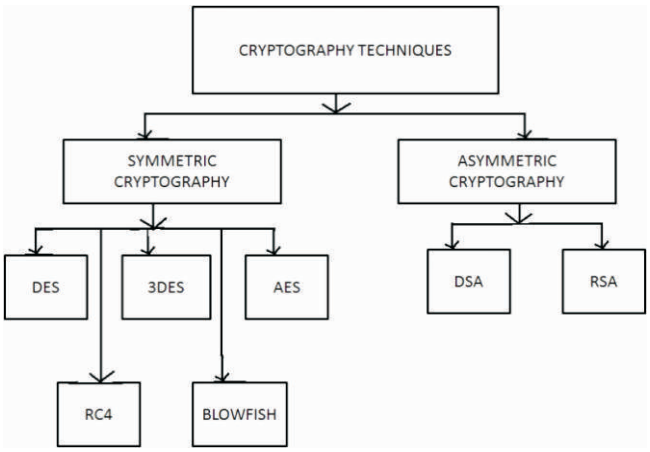

Figure 2. Classification of Cryptography

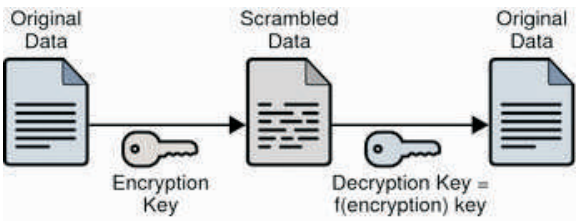

Figure 3. Symmetric Key Cryptography

many different asymmetric cryptography techniques and analyzed with different techniques. Also RSA based encryption techniques are compared, to give the advantages and disadvantages of RSA algorithm.

1.2 Survey of Different Modifies RSA Techniques and Analysis

Joshi Maitri and Fenil Khatiwala [3] have studied on public key generation, RSA algorithm and various improved algorithm by applying various modifications on the existing algorithms and represents the summarized results through different open sources.

1.3 A Comprehensive Study on Various Modifications in RSA Algorithm

Gaurav Patel, Krunal Panchal and Sarthak Patel [30] have surveyed various modification approaches applied to the RSA algorithm in order to enhance it. The main

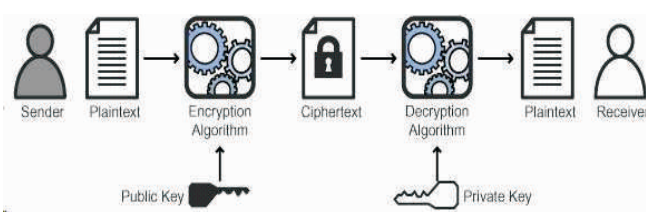

Figure 4. Asymmetric Key Cryptography

disadvantage of RSA cryptography is the computational time, so many researchers apply various methods to improve the speed of RSA algorithm.

1.4 Modified RSA Encryption Algorithm

Ravi Shankar Dhakar and Amit Kumar Gupta [13] have presented a new cryptographic algorithm based on Additive Homomorphic properties called Modified RSA Encryption Algorithm (MERA). In this proposed algorithm, two pairs of different keys are used. The mathematical attack and problems of trying all possible private keys has brute force attack which can be improved by MERA algorithm.

1.5 A Modified RSA Cryptosystem Based on 'n' Prime Numbers

Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar [1] have proposed the RSA with 'n' prime numbers, which provide better security in the network. It is implemented by four prime numbers; if large prime numbers are used, then it is not breakable. But if cryptanalyst factories the 'n' then easily the algorithm lock can be opened.

1.6 Research and Implementation of RSA Algorithm for Encryption and Decryption

Xin Zhou and Xiaofei Tang [16] have discussed and implemented the encryption and decryption with RSA algorithm in detail. Also the RSA algorithm with digital signature and other related technology plays an important role for the communication purpose.

2. Methodology

2.1 RSA (Rivest Shamir and Adleman)

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology [18], [28]. RSA includes the public and private key. The public key is only used to encrypt the messages and it can be seen to all [22]. The private key is used to decrypt the messages. Private Key is also called as the secret key [5], [6], [7], [14].

2.1.1 Key Generation Process

- Select two prime numbers p and q.
- Find n=p*q, where, n is the modulus that is made public. The length of n is considered as the RSA key

length [29], [2].

- Choose a random number 'e' as a public key in the range $0<e<(p-1)(q-1)$ such that [20],

  $gcd(e,(p-1)(q-1))=1$

- Find private key d such that [13],

  $e * d = 1 (mod (p-1)*(q-1))$.

2.1.2 Encryption

It is the process of converting the plain text into cipher text; the mathematical calculation is given by,

$$C = M^e \bmod n$$

where, M is the original message i.e. plaintext and C is the cipher text [9], [12].

2.1.3 Decryption

The reverse process of encryption is called decryption; converting the cipher text to plain text [11], [15]. Figure 5 describes the flowchart of RSA algorithm.

$$M = C^d \bmod n$$

2.2 Proposed Algorithm

RSA algorithm is basically based on the prime numbers and 'n' [17], [19]. Brute force attack and the time taken for the attack is totally dependent on the factorization of 'n' [21]. Traditional RSA use only two prime numbers (p and q); as 'n' is the modulus that is made public and length of 'n' is considered as the length of key in the RSA cryptography [13].

2.2.1 Key Generation Process

- Select three prime numbers p, q and r.
- Find $n=p*q*r$.
- Choose a random number 'e' as a public key in the range $0<e<(p-1)(q-1)(r-1)$ such that [10],

  $gcd(e,(p-1)(q-1)(r-1))=1$.

- Find private key d such that,

  $e * d = 1 (mod (p-1)*(q-1)*(r-1))$

Encryption and Decryption process is same as the original RSA cryptography [23]. Figure 6 describes the process of the proposed algorithm.

3. Results & Discussion

The original RSA and the proposed algorithm are implemented in MATLAB R2013a successfully. Figure 7 describes the input of the original RSA algorithm. According to the algorithm, the public key and private key are calculated, with the use of those keys, encryption and decryption process are performed as shown in Figure 8.

Figure 9 shows the input for the proposed algorithm.

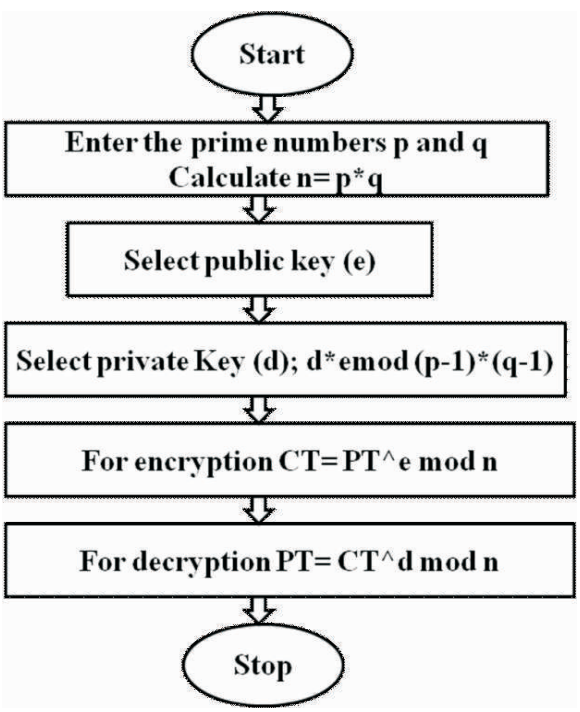

Figure 5. Flowchart of RSA Algorithm

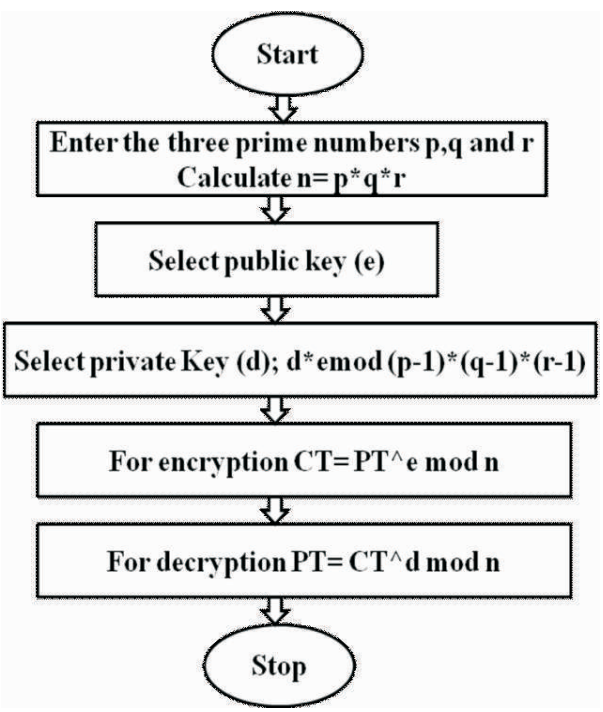

Figure 6. Flowchart of Proposed Algorithm

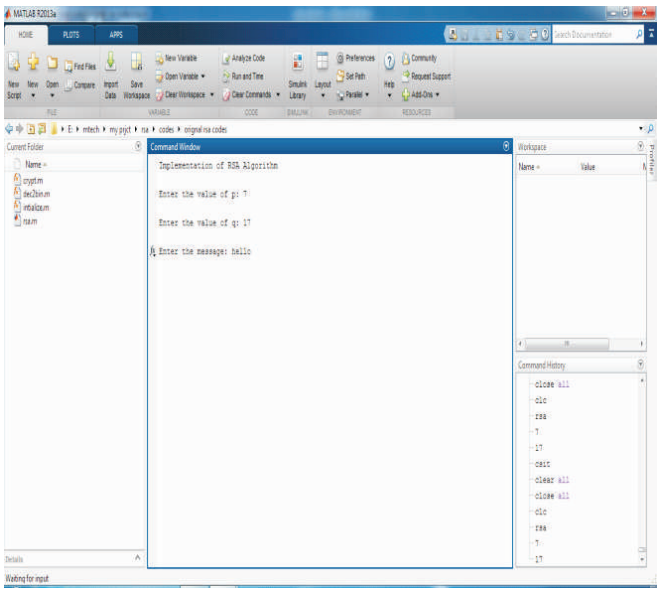

Figure 7. Input of Original RSA Algorithm

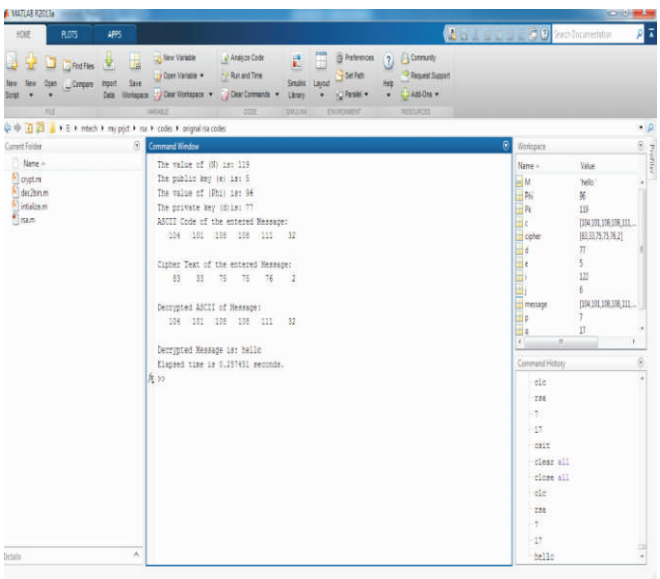

Figure 8. Output of Original RSA Algorithm

According to that algorithm, keys are generated and encryption and decryption process are performed successfully as it is shown in Figure 10.

The total time taken for key generation, encryption and decryption is more in the proposed algorithm, as compared to the original RSA. Also the length of the key is large in the proposed work. In public key cryptography, the large size of key length provides more security to the algorithm, such that the proposed work provides more security and authentication to the user [19], [24].

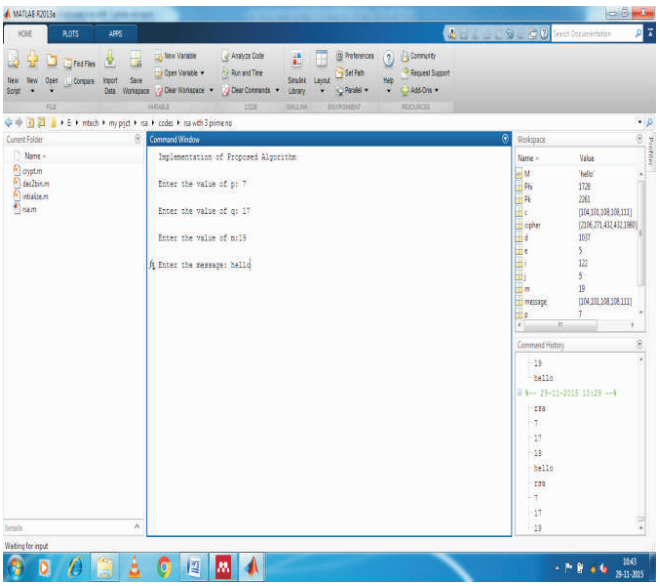

Figure 9. Input of Proposed Algorithm

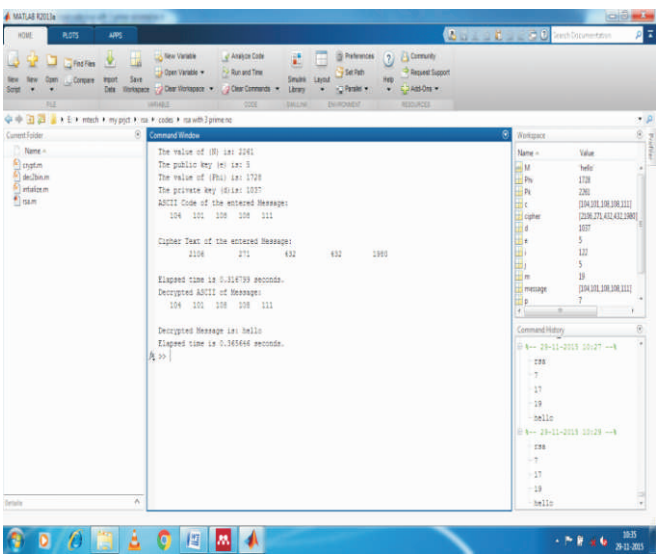

Figure 10. Output of Proposed Algorithm

From the above performed experiment, results are compared with respect to their execution time and the prime numbers are used as it is briefly described in Table 1.

Conclusion

In this paper, the original RSA algorithm and the proposed algorithm is implemented in MATLAB R2013a. Both the algorithms are compared in terms of security, time and the

Algorithm	No. of Prime Numbers Used	Execution Time (in Seconds)
RSA	2	0.25345
Proposed Algorithm	3	0.33291

Table 1. Comparison of RSA and Proposed Algorithm

number of prime numbers used in it. The proposed method is a modification of the RSA algorithm. In this paper, only few concepts were modified further, RSA can be modified with many logical change in mathematical calculation and also, it can be merged with Diffie-Hellman key exchange and Digital signature. However, RSA is mostly applied in text data, it can be further implemented in image, video, etc.

References

[1]. Srinivasan Nagaraj, Raju and V. Srinadth, (2015). "Data Encryption and Authentication using Public Key Approach". *International Conference on Intelligence Computing, Communications and Convergence*, pp.126-132.

[2]. Sarika Khatarkar and Rachana Kamble, (2015). "A Survey and Performance Analysis of Various RSA based Encryption Techniques". *International Journal of Computer Applications*, Vol.114, No.7, pp. 30-33.

[3]. Joshi Maitri and Fenil Khatiwala, (2015). "Survey of Different Modified RSA Techniques and Analysis". *International Journal of Engineering Technology, Management and Applied Sciences*, Vol.3, No.2, pp.126-132.

[4]. Shyam Deshmukh and Prof. Rahul Patil, (2014). "Hybrid Cryptography Technique using Modified Diffie-Hellman and RSA". *International Journal of Computer Science and Information Technologies*, Vol.5, No.6, pp.7302-7304.

[5]. Ali E. Taki El_Deen, El-Sayed A. El-Badawy and Sameh N. Gobarn, (2014). "Digital Image Encryption Based on RSA Algorithm". *International Journal of Electronics and Communication Engineering*, Vol.9, No.1, pp.69-73.

[6]. Norhidayah Muhammad, Jasni Mohamad Zain and Md Yazid Mohd Saman, (2013). "Loop Based RSA Key Generation Algorithm using String Identify". *13th International Conference on Control, Automation and System*, pp.255-258.

[7]. B. Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, (2013). "A Modified RSA Cryptosystem based on 'n' Prime Numbers". *International Journal of Research in Science and Engineering*, Vol.1, No.8, pp.63-66.

[8]. Nentawe Y. Goshwe, (2013). "Data Encryption and Decryption Using RSA Algorithm in a Network Environment". *International Journal of Computer Science and Network Security*, Vol.13, No.7.

[9]. S.H. Mortazavi and P.S. Avadhani, (2013). "RSA Cryptography Algorithm : An Impressive Tool in Decresasing Intrusion Detection System (IDS) Vulnerabilities in Network Security ". *International Journal of Innovative Technology and Exploring Engineering*, Vol.2, No.4, pp. 306-310.

[10]. Alaa Hussein Al-Hamami and Ibrahem Abdallah Aldariseh, (2012). "Enhanced Method for RSA Cryptosystem Algorithm". *IEEE International Conference on Advanced Computer Science Applications and Technologies*, pp.402-408.

[11]. Sami A. Nagar and Saad Alshamma, (2012). "High Speed Implementation of RSA Algorithm with Modified Keys Exchange". *IEEE 6th International Conference on Science of Electronics, Technologies of Information and Telcommunication*, pp.639-642.

[12]. Shilpi Gupta and Jaya Sharma, (2012). "A Hybirid Encryption Algorithm based on RSA and Diffie-Hellman". *IEEE International Conference on Computational Intelligent and Computing Research*, pp.1-4.

[13]. Ravi Shankar Dhakar and Amit Kumar Gupta, (2012). "Modified RSA Encryption algorithm (MERA)". *IEEE 2nd International Conference on Advanced Computing and Commnication Technologies*, pp.426-429.

[14]. Vishal Grag and Rishu, (2012). "Improved Diffie-Hellman Algorithm for Network Security Enhancement". *International Journal of Computer Technology and Applications*, Vol.3, No.4.

[15]. P. Saveetha and S. Arumugam, (2012). "Study of Improvement in RSA Algorithm and its Implementation". *International Journal of Computer and Communication Technology*, Vol.3, No.6.

[16]. Xin Zhou and Xiaofei Tang, (2011). "Research and Implementation of RSA Algorithm for Encryption and Decryption". *IEEE The 6th International Forum on Strategic Technology*, pp.1118 - 1121.

[17]. Liang Wang and Yonggui Zhang, (2011). "A New Personal Information Protection Approach Based on RSA

Cryptography". *IEEE International Symposium on IT in Medicine and Education*, pp.591-593.

[18]. Shashi Mehrotra Seth and Rajan Mishra, (2011). "Comparitive Analysis of Encryption Algorithms For Data Communication". *International Journal of Computer Science and Technology*, Vol.2, No.2, pp. 292-294.

[19]. Wenxue Tan, Xiping Wang, Xiaoping Lou and Meisen Pan, (2011). "Analysis of RSA based on Quantitating Key Security Strength". *Advanced in Control Engineering and Information Science*, pp.1340-1344.

[20]. Sonal Sharma, Prashant Sharma and Ravi Shankar Dhakar, (2011). "RSA Algorithm Using Modified Subset Sum Cryptosystem". *IEEE International Conference on Computer & Communication Technology*, pp.457-461.

[21]. Yunfei Li, Qing Liu and Tong Li, (2010). "Design and Implementation of an Improved RSA Algorithm". *IEEE International Conference on E-Health Networking, Digital Ecosystems and Technologies*, pp.390-393.

[22]. Allam Mousa, (2005). "Sensitivity of Changing the RSA Parameter on the Complexity and Performance of the Algorithm". *Journal of Applied Science*, Vol.5, No.1, pp.60-63.

[23]. Aloka Sinha and Kehar Singh, (2003). "A Technique for Image Encryption using Digital Signature". *Optic Communications*, pp.239-234.

[24]. Subbarao V. Wunnava and Ernest Rassi, (2002). "Data Encryption Performance and Evaluation Schemes". *IEEE Proceedings of Southeastcon*, pp.234-238.

[25]. David A. Carts, (2001). "A Review of the Diffie-Hellman Algorithm and its use in Secure Internet Protocol". SANS Institute, pp.1-7.

[26]. Rajorshi Biswas and Shibdas Bandyopadhyay, "A Fast Implementation of the RSA Algorithm Using the GNU Implementation". Retrived from: http//www.alumni.cs.ucr.edu

[27]. Atul Kahate, (2013). *Cryptography and Network Security*. Fourth Edition, Tata McGraw-Hill.

[28]. William Stallings, (2010). *Cryptography and Network Security – Principles and Practice*. Fifth Edition, Pearson Publication.

[29]. R.L. Rivest, A. Shamir and L. Adleman, (1978). "A Method for Obtaining Digital Signatures and Public Key Cryptosystem". *Communication of ACM*, Vol.21, pp.120-126.

[30]. Gaurav R Patel, Kurnal Panchal, and Sarthak R. Patel, (2013). "A Comprehensive Study on a various Modifications in RSA Algorithm". *International Journal of Engineering Development and Research*, Vol.1, No.3, pp.161-163.

ABOUT THE AUTHORS

Madhurima Dubey is currently pursuing M.E. Degree in the Department of Electronics and Telecommunication Engineering at Chhatrapati Shivaji Institute of Technology, Durg, India. She received BE Degree in the Department of Electronics and Telecommunication Engineering from Chhattisgarh Swami Vivekanand Technical University, Bhilai, India.

Yojana Yadav is presently working as Associate Professor in the Department of Electronics and Telecommunication Engineering at Chhatrapati Shivaji Institute of Technology, Durg, India. She received her M.Tech Degree from the Chhattisgarh Swami Vivekanand Technical University, Bhilai, India and B.E. Degree from Jawaharlal Institute of Technology, Khargone, India.