IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 10 (October. 2018), ||V (IV) || PP 01-07

A Secure Cryptosystem by using Euler Totient Function and Modified RSA

Sanjeev Kumar Mandal[1], A R Deepti[2]
[1]*Research Scholar, Department of Master of Computer Applications, Visvesvaraya Technological University, Belgavi, India.*
[2]*Professor, Department of Computer Science Indian Academy Group of Institutions, Bangalore, India.*
Corresponding Author: Sanjeev Kumar Mandal

Abstract: - In the internet world, there is a need for strong cryptographic techniques for data transmission and storing confidential information. To do this, an approach has been made by using the mathematical proof of the existence of a consistent formation of the Euler totient function to generate a key. Then the principles of number theory functions have been proposed in the encryption/decryption process. Thus, this structure is simple and powerful to use; in generating a key, computation of encryption/decryption process and key transmission.

Keywords: - Cryptography, Euler Totient function, Number Theory, Testing tools, Modified RSA algorithm.

Date of Submission: 16-10-2018 Date of acceptance: 31-10-2018

I. INTRODUCTION

Technology is used in every field of science where people are more dependent on computer technology to exchange confidential information to others in a secure way. So a day-to-day use of cryptography [4] is increasing tremendously in all our life. Therefore, Cryptography is a modern encryption/decryption technology; consist of different mathematical formulas or algorithms that have been designed to secure the network communications and data authentication. Cryptography can be classified as Symmetric key algorithm and Asymmetric key algorithm. Symmetric-key algorithms [9] are also known as single- key, or private-key encryption that uses a Private (shared secret) key to execute encryption /decryption process. Some popular symmetric algorithms include DES [1], TDES [10], Blow fish [14], IDEA [5], AES [1], Two fish [2] and RC6 [11, 12]. Asymmetric key algorithms [3] also known as public key encryption where encryption and decryption are mathematically performed using different keys; one key act as public key and the other one as private key. Some popular asymmetric algorithms includes PGP [7], Diffie-Hellman keys [8], SSH [14] and SSL [16].

In the network communication, messaging of data is done by texting through components like phone, web, or mobile communication over the world. This data is potentially visible and vulnerable to eavesdroppers anywhere along its internet path or within the network. So the information at any moment can be modified by the intruder. For this reason, this paper is concern with the progress of securing the message mathematically by using cryptographic technique to protect the confidential data from unauthorized access and authenticated by the user.

This paper comprises into three sections namely, section 2 proposed the encryption and decryption process by using mathematical techniques like euler totient function and modular function. Section 3 explains the key generation, encryption/decryption process and key transmission to the authenticated users which has been implemented with an example and section 4 shows its security aspects and conclude with section 5.

II. PROPOSED SYSTEM

Data security refers to protect confidential information from unauthorized access of data. So cryptography plays an important role, where it has been attacked by few methods like brute force, dictionary attacks, side-channel attacks and targeted cipher attacks etc., To overcome these attacks, in the proposed method, the key is generated by using Euler totient function. This key is then xor'ed with the message for encryption and decryption process which is shown in fig.1. Though this proposed method looks simple, the complexity is depends on key generation process. Thus the encryption/decryption process is represented as,

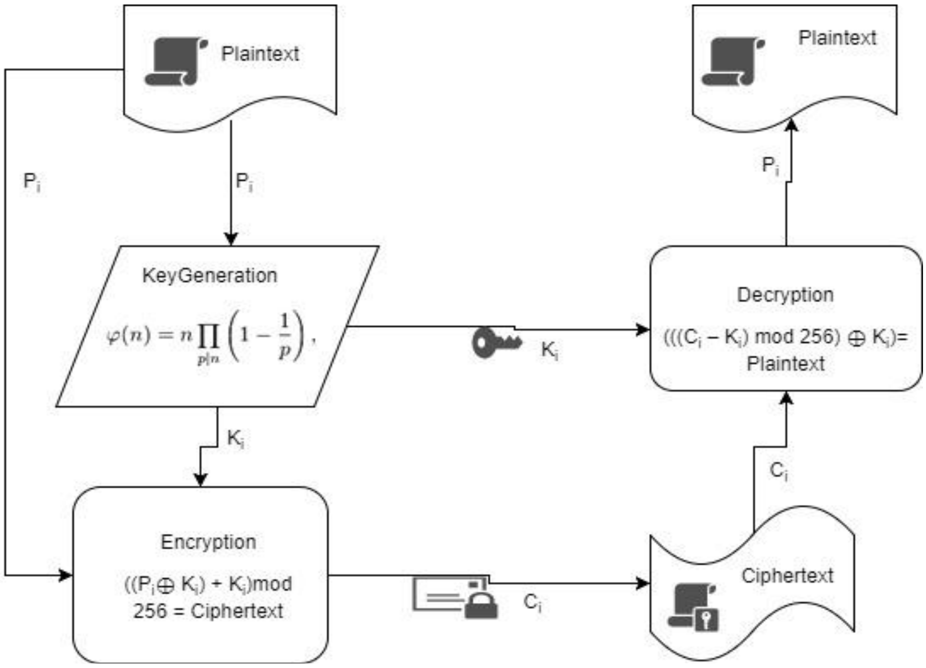

Fig 1: Encryption Process in Proposed Model

III. IMPLEMENTATION

The proposed method is explained with an example given below,

KEY GENERATION PROCESS

The key has been generated with the help of Eular totient function where,

ϕ (n) where n = $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots\dots. p_k^{\alpha_k}$

ϕ (n) = $n\left(1-\frac{1}{p^1}\right)\left(1-\frac{1}{p^2}\right)\dots\dots\left(1-\frac{1}{p^k}\right)$

(Or) $\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$ (For both prime and non-prime numbers)

Example: Let consider a word “IAMGO” as a key and is converted into its ascii value,

I	A	M	G	O
73	65	77	71	79

This ascii value is then applied to the euler totient function to generate the key as,

ϕ (n) = 73

ϕ (73) = $73\left(1-\frac{1}{73}\right)$ = 72.

ϕ (n) = 65

ϕ (65) = $65\left(1-\frac{1}{5}\right)\left(1-\frac{1}{13}\right)$ = 48

Finally, the calculated key for “IAMGO” is 72, 48, 60, 70, 78 = H0<FN

ENCRYPTION

To do the encryption,

$$((P_i \oplus K_i) + K_i) \bmod 256 = \text{Ciphertext}$$

Where P_i is plain text and K_i is the key generated from euler totient function.

Let take a plain text and is converted into its binary value and then apply modular and XOR function along with the generated key for encryption process as,

I	A	M	G	O	I	N	G	H	O
01001001	01000001	01001101	01000111	01001111	01001001	01001110	01000111	01001000	01001111
M	E								
01001101	01000101								

010010010100000101001101010001110100111101001001010011100100011101001000010011110100110101000101

Key:

72	48	60	70	78
01001000	00110000	00111100	01000110	01001110

0100100000110000001111000100011001001110

Cipher text	0010010011010000110101101010001110100111101001001101011101011011101010100010011 1101001101 10100101

This encrypted message is send to the receiver. Upon receiving the cipher text, the decryption process is done as,

DECRYPTION

The cipher text is decrypted by using inverse modular function as,

$$(((C_i - K_i) \bmod 256) \oplus K_i) = \textbf{Plaintext}$$

Ciphertext	00100100110100001101011010100011101001111010010011010111010110111010101000100111101001101 10100101
Key	010010000011000000111100010001100100111001001000001100000011110001000110010011100100100000110000
Plaintext	010010010100000101001101010001110100111101001001010011100100011101001000010011110100110101000101

Original Plaintext:

I	A	M	G	O	I	N	G	H	O
01001001	01000001	01001101	01000111	01001111	01001001	01001110	01000111	01001000	01001111
M	E								
01001101	01000101								

The time complexity for encryption/decryption is,

Result of Evaluation

Evaluated string =
"0000000101110001011100010000000010000000100000001011111100111101100001110000000C

BDM algorithmic complexity estimation	224.0849 bits
BDM logical depth estimation	255.0000 steps
Shannon entropy	0.9464 bit(s)
Second order entropy	1.8608 bit(s)
Compression length (using gzip)	304 bits
String length	96
# of symbols in string	2
# of symbols in CTM alphabet	2
Block size	12
Block overlap	0

$$BDM = \sum_{i=1}^{n} K(block_i) + log_2(|block_i|)$$

Fig 2: Encryption/Decryption Process - Time complexity

KEY TRANSMISSION

To do encryption/decryption, the generated key must be transmitted to the authenticated users by using modified RSA Algorithm. The RSA Algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman in 1977[13]. This algorithm has been used widely in Internet communications by Netscape Navigator, BitCoin, SSH, PGP and Microsoft Explorer web browsing programs. For RSA key exchange, secret keys are exchanged securely online by encrypting the secret key with the intended recipient's public key. Only the intended recipient can decrypt the secret key because it requires the use of the recipient's private key. Therefore, a third party who intercepts the encrypted, shared secret key cannot decrypt and use it. Unfortunately RSA is not much secure to various attacks like man-in-middle attack, brute force attack because of its key size . So to ensure the key is secure, a modified RSA algorithm is proposed by increasing the value of key size to improve its complexity. Thus, the Modified RSA can be generated by the following steps:

1. Selecting 3 prime numbers such as p, q and r.
2. Compute the modulus N as n = p × q × r
3. Select an exponent value E in a manner it should be 1 < E < ϕ (n), where ϕ is an Euler's function.
4. Calculate ϕ (n) = (p-1) (q-1) (r-1)
5. Calculate the private exponent D from e, p, q and r.
6. Output (n, e) as the public key and (n, d) as the private key.

The encryption is done by,

$$\mathbf{C = m^e \bmod n}$$

Where *m* is the message which needs to transmit to the receiver and the output *C* is the resulting ciphertext.
The decryption is done by

$$\mathbf{M = c^d \bmod n}$$

ILLUSTRATION

The generated key is 72, 48, 60, 70, 78 = H0<FN is transmitted to the receiver by using modified RSA algorithm
Let consider P= 3, q= 5, r=7 where N = p*q*r,
N= 105, and ϕ (n) = (p-1) (q-1) (r-1) = (2, 4, 6) = 48
E = 11 (public key)

ENCRYPTION

$C = m^e \bmod n$
$C = 72^{11} \bmod 105 = 18$

DECRYPTION

$M = c^d \bmod n$
Finding decryption Key D = $\frac{1+K\,\phi(n)}{e}$ = 35, (private key)
$D = 18^{35} \bmod 105 = 72$

The time complexity is,

Result of Evaluation

Evaluated string = "72, 48, 60, 70, 78"

BDM algorithmic complexity estimation	76.1284 bits
BDM logical depth estimation	NA steps
Shannon entropy	2.7947 bit(s)
Second order entropy	3.3816 bit(s)
Compression length (using gzip)	184 bits
String length	18
# of symbols in string	8
# of symbols in CTM alphabet	2
Block size	12
Block overlap	0

$$BDM = \sum_{i=1}^{n} K(block_i) + log_2(|block_i|)$$

Fig 3: Key Generation: Time complexity

IV. SECURITY ANALYSIS

The proposed method is tested by using cryptographic tools like wireshark and translator binary tools to check its security against vulnerability attacks as,

BY USING TRANSLATOR BINARY TOOLS

To check the cipher text is secure or not, a translator binary testing tool is used in fig 4. This tool helps to identify whether the cipher text can be decrypted easily or not and prove the proposed method is secure against binary attacks.

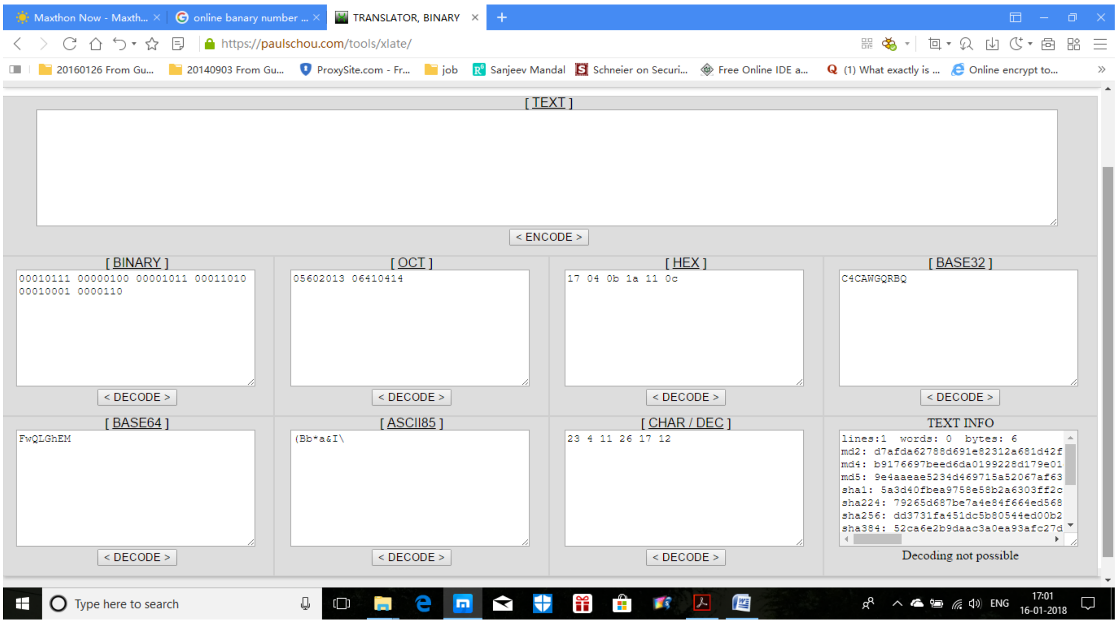

Fig 4: Security analysis for cipher text by using translator binary tools

BY USING WIRESHARK TOOLS

Our proposed method have been tested by using wireshark tools and proven secure against SQL, intrusion attack, rapping attacks and cipher text attacks is shown in fig 5 and 6.

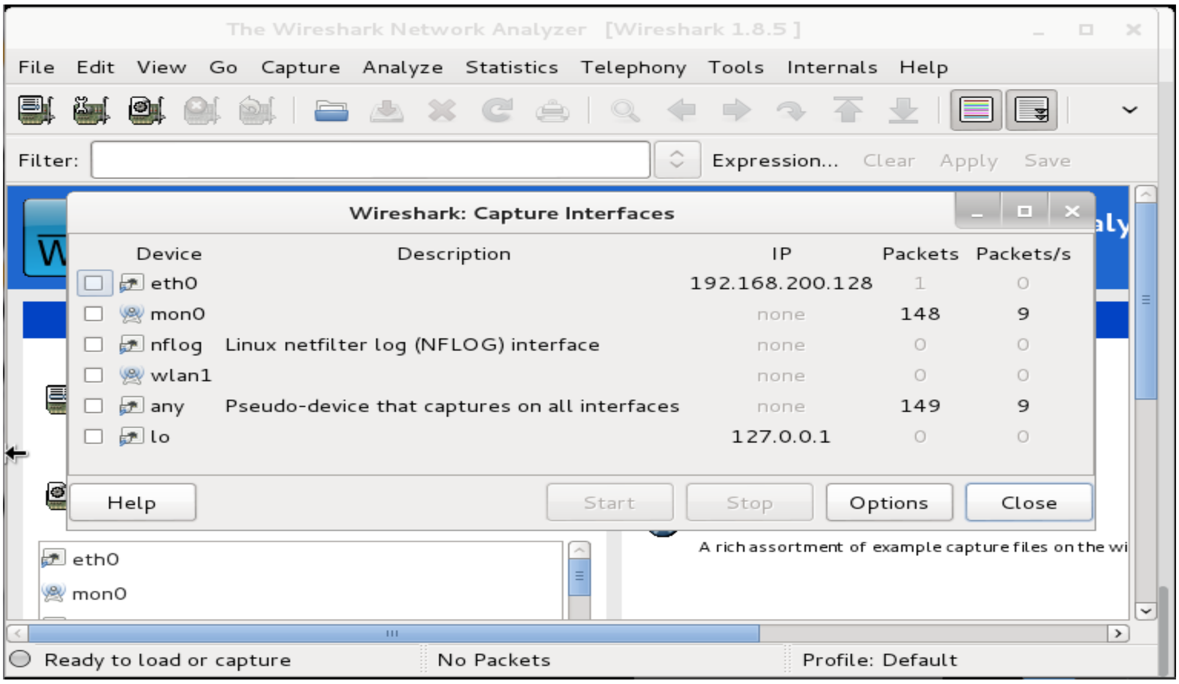

Fig 5: Captured target details

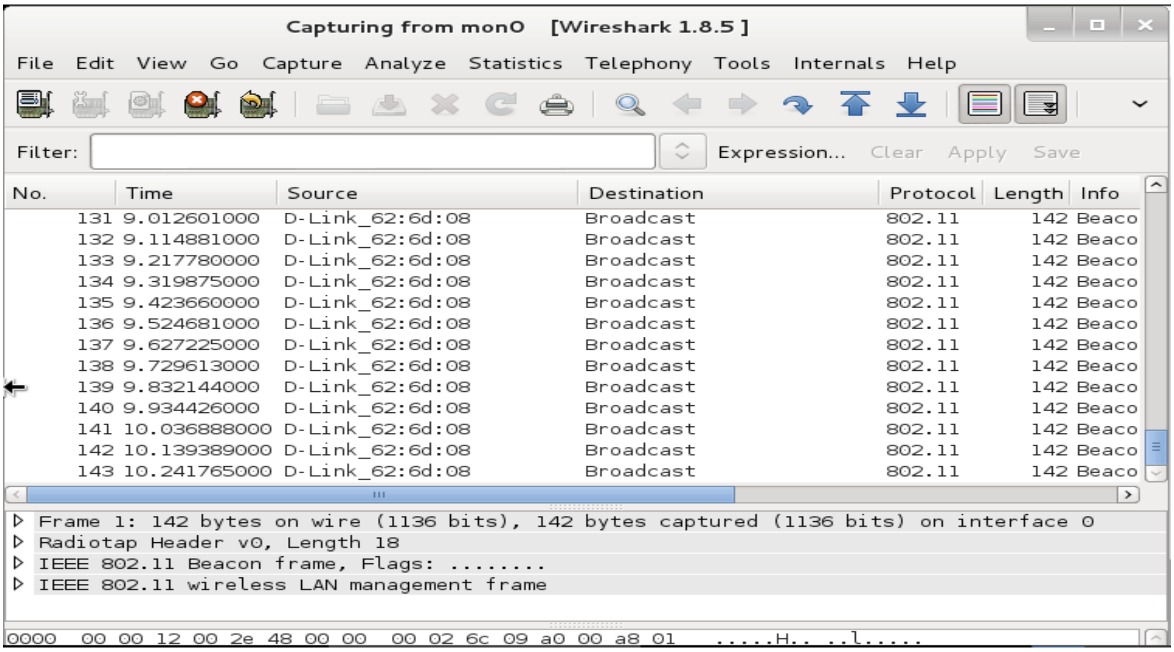

Fig 6: Capturing a data between sender to receiver

By using wireshark tools, it has been tested to check security leakage between sender and receiver and vice versa while selecting the IP Address which is shown in Fig.5. Fig. 6 helps to check whether any leakage is visible or not. So this shows our proposed method is secure against man-in-middle Attack.

Finally the overall time complexity of our proposed method is $18T+18T_x+1T_o$ which is shown in fig.7 is more secure.

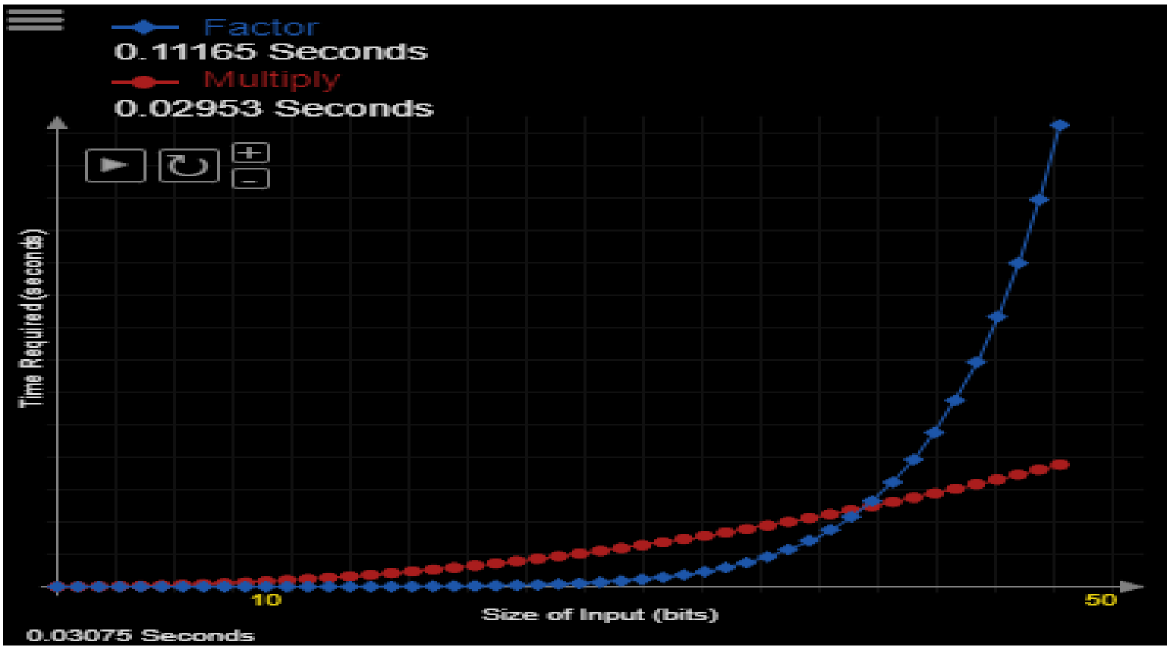

Fig.7: Proposed method of securing message: Time complexity

V. CONCLUSION

Security plays a vital role in the wide area of data exchange and so the development of cryptographic algorithms also helps to secure such information. Mathematically, number theory functions have been used in almost all encryption and decryption algorithms. So in this paper we perceive a mathematical approach like Euler totient function, modular arithmetic and xor function which plays an important role in providing security aspects of transmitting the messages. The proposed method, thus helps to secure from the crypto attacks, reduce computation time and ease to access the chosen cryptosystem.

REFERENCES

[1]. Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" *International Journal of Computer Applications*, pp. 0975 – 8887.
[2]. The web page gives the AES contains: http://www.nist.gov/ CryptoToolkit.
[3]. Annapoorna Shetty, Shravya Shetty and Krithika, "A Review on Asymmetric Cryptography RSA and ElGamal Algorithm", *International Journal of Innovative Research in Computer and Communication Engineering*, 2014.
[4]. Coron, J. S. "What is cryptography?", *IEEE Security & Privacy Journal*, 12(8), 2006, pp. 70-73.
[5]. Harivans Pratap Singh, Shweta Verma , Shailendra Mishra, "Secure-International Data Encryption Algorithm", *International Journal of Advanced Research in Electrical*, Electronics and Instrumentation Engineering, Vol. 2, Issue 2, February 2013.
[6]. Huang, Y., Chen, L., Tang, S, "Information security and encryption decryption core technology", *Electronic Press*, 2001.
[7]. Huiping, H., Yan, R., Lan, Z, "Using PGP software to realize safe sending and receiving email", *Comput. Secur*. **1**, 2011, pp. 52–54.
[8]. Li Xin, "An Improvement of Diffie-Hellman Protocol", *Network & Computer Security*, vol. 12, 2007, pp. 22-23.
[9]. Massey, J.L, "An Introduction to Contemporary Cryptology", *Proceedings of the IEEE*, Special Section on Cryptography, May 1988, pp. 533-549.
[10]. Nisha Rani, Mrs. Neetu Sharma, "Suspicious Email Detection System via Triple DES Algorithm: Cryptography Approach", *International Journal of Computer Science and Mobile Computing*, Vol.4, Issue 5, May 2015.
[11]. RSA Laboratories, "RC6 Block Cipher", Historical: RSA Algorithm: Recent Results on OAEP Security: *RSA Laboratories submissions*, 2012.
[12]. R.L. pavan, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "The RC6 Block Cipher", v1.1, August 1998.
[13]. Ronald L. Rivest, Adi Shamir, Len Adelman, "On Digital Signatures and Public Key Cryptosystems," *MIT Laboratory for Computer Science Technical Memorandum 82*, April 1977.
[14]. Saikumar Manku, and K. Vasanth, "Blowfish Encryption Algorithm for Information Security", *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 10, June 2015.
[15]. Ylonen, T. and Lonvick, C, "The Secure Shell (SSH) Protocol Architecture", *RFC 4251*, January 2006.
[16]. W.Chou,"Inside SSL: accelerating secure transactions," *IEEE IT Pro*, September/October 2002, pp. 37-41.

Sanjeev Kumar Manda. " A Secure Cryptosystem by using Euler Totient Function and Modified RSA." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10, 2018, pp. 01-07.