International Conference on Recent Advancement in Science & Technology- 2020
(ICRAST-2020)

Development of High Quality Routing and Encryption Algorithm for WSN

[1]Aamina Khatoon, [2]Peeyush Pathak
Dept of Computer Science
Goel Institute of Technology and Management, Lucknow, India
khatoonaamina96@gmail.com, Peeyush.pathak@gmail.com

Abstract: Today our modern era is significantly dependent on Internet and mobile applications. Concerning these web based application in every phase of life the Information Security has been critically important in the applications related to data communication. Any loss or leakage of our personal/public information can prove to be great loss to the organization, country and individuals. In this work the encryption techniques are considered due to their above importance in information security systems. This work provides an analytical comparisons between two most commonly used encryption algorithms for data ciphering RSA and RC4. A comparison has been made on the basis of these parameters: packet size, ciphering time of encryption/decryption, ciphered data size and performance in the form of throughput

Keywords: AODV, Encryption, Decryption, RC4, RSA.

1. Introduction:

As the increasing growth of the computing era and network era, it additionally increases information garage demands. Data Security has end up a crucial problem in electronic communication. Secret writing has arise as an answer, and plays a important role in data protection gadget. It uses a few algorithms to scramble facts into unreadable text which might be most effective being decrypted by using birthday celebration the ones having the associated key. These algorithms devour a chief quantity of computing assets including reminiscence and battery strength and computation time. This paper accomplishes comparative evaluation of encryption standards DES, AES and RSA considering diverse parameters such as computation time, reminiscence usages.

For secure communication over public community statistics may be blanketed with the aid of the technique of encryption. Encryption converts that information via any encryption set of rules the use of the 'key' in scrambled form. Only consumer getting access to the key can decrypt the encrypted records [4]. Encryption is a fundamental device for the safety of touchy statistics. The purpose to use encryption is privacy (stopping disclosure or confidentiality) in communications. Encryption isa way of speaking to someone whilst other humans are listening, however such the opposite humans can't understand what you are pronouncing [6].

Encryption algorithms play a huge role in supplying facts protection against malicious assaults. In cell devices security may be very important and extraordinary styles of algorithms are used to prevent malicious assault at the transmitted facts. Encryption algorithm may be categorised into symmetric key (non-public) and uneven(public) key [1].

In WSNs, it also includes assumed that an attacker may recognize the safety mechanisms which might be deployed in a sensor community; they will be able to compromise a node or even bodily capture a node. Due to the excessive value of deploying tamper resistant sensor nodes, maximum WSN nodes are regarded as non tamper- resistant. Further, as soon as a node is compromised, the attacker is capable of stealing the key materials contained inside that node.

Base stations in WSNs are typically appeared as trustworthy. Most research attention on relaxed routing among sensors and the bottom station. Deng et al. Taken into consideration strategies in opposition to threats that could cause the failure of the bottom station [6].

2. Related Work:

Priteshkumar Prajapati et. Al. (2014), [1] in keeping with them the growing boom of the computing generation and community generation, and it also will increase facts garage demands. Data Security has end up a important problem in digital communication. Secret writing has arise as a solution, and performs a critical function in records security device. It uses a few algorithms to scramble information into unreadable text which is probably most effective being decrypted by means of birthday party those having the related key. These algorithms consume a main quantity of computing assets including reminiscence and battery electricity and computation time. This paintings accomplishes comparative analysis of encryption standards DES, AES and RSA considering numerous parameters consisting of computation time, reminiscence usages. A cryptographic tool is used for appearing experiments. Experiments effects are given to analyses the effectiveness of symmetric and asymmetric algorithms.

RC4 has been the most famous movement cipher inside the records of symmetric key cryptography. Its internal nation carries a permutation over all viable bytes from zero to 255, and it attempts to generate a pseudo-random sequence of bytes

(referred to as key movement) with the aid of extracting factors of this permutation. Over the last twenty years, severa cryptanalytic effects on RC4 movement cipher have been published, a lot of that are based on non-random (biased) activities concerning the secret key, the country variables, and the important thing stream of the cipher. Though biases primarily based on the name of the game key are commonplace in RC4 literature, none of the prevailing ones depends at the duration of the name of the game key. In the primary a part of this work, we inspect the effect of RC4 key period on its key circulation, and document extensive biases related to the length of the name of the game key. In the method, they prove the 2 known empirical biases that have been experimentally suggested via Sourav Sen Gupta and Subhamoy Maitra (2014) [2] and used in recent attacks against WEP and WPA through Sepehrdad, Vaudenay and Vuagnoux in EUROCRYPT 2011. After our modern-day work, there stays no bias inside the literature of WEP and WPA assaults without a evidence.

Avala Ramesh et. Al. (2013) [3] finish that the Bio-cryptography performs a inevitable function in the authentication mechanism. To offer sturdy safety, RSA encryption changed into used on the special biometrics samples with specific edge detection techquies. All the samples were simulated using the Matlab software. The encrypted image and their histograms photographs have been analyzed. It changed into discovered that the Canny operator image appears more secure

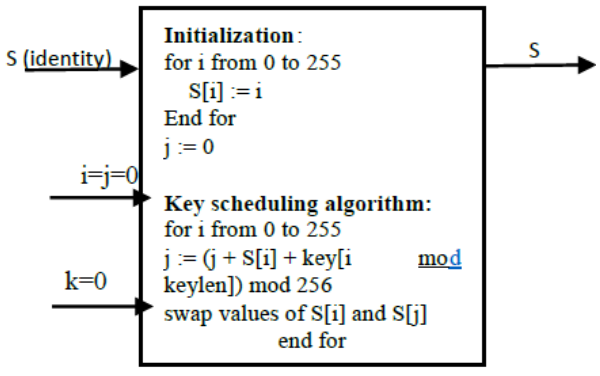
Ayesha Khan (2013), [4] says that the RSA cryptosystem became first published extra than 25 years ago with the aid of Ronald Rivest, Adi Shamir and Leonard Adleman in 1997. It has been extensively used for many years on the net for security and authentication in lots of packages including credit card bills, electronic mail and faraway login sessions. Her work discusses but every other use of RSA set of rules that is using designing of an encryption approach the usage of RSA algorithm. She can use geo-vicinity (latitude and longitude of source and destination) as keys along with the private and non-private keys of RSA set of rules.

Sourav Sen Gupta et. Al. (2013), [5] in keeping with them the first three bytes of the RC4 key in WPA are public as they may be derived from the general public parameter IV, and this derivation leads to a sturdy mutual dependence among the first two bytes of the RC4 key. In this work, we offer a disciplined have a look at of RC4 biases ensuing especially in this type of state of affairs. Motivated through the work of AlFardan et al. (2013), we first prove the interesting sawtooth distribution of the primary byte in WPA and the same nature for the biases inside the preliminary keystream bytes toward 0. As we note, this sawtooth traits of these biases surface due to the dependence of the first bytes of the RC4 key in WPA, both derived from the equal byte of the IV. Our end result on the character of the first keystream byte offers a notably advanced distinguisher for RC4 utilized in WPA than what have been supplied by Sepehrdad et al. (2011-12). Further, we revisit the correlation of initial keystream bytes in WPA to the first three bytes of the RC4 key. As those bytes are recognized from the IV, possible achieve new in addition to substantially improved biases in WPA than the absolute biases exploited earlier by using AlFardan et al. Or Isobe et al. We note that the correlations of the keystream bytes with publicly recognised IV values of WPA probably reinforce the sensible plaintext restoration assault on the protocol.

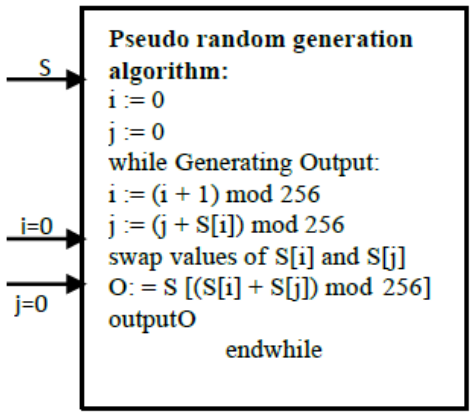
3. Methodology:

3.1 RC4 Description:

RC4 follows the design strategy used in stream ciphers. To extract the pseudorandom data bytes from a pseudorandom permutation is the basic design principle of RC4 stream cipher. RC4 has two working modules: first there is a KSA with key K as input (with typical size of 40-256 bits), and second is PRGA which generates a pseudo-random output sequence. The pseudo code for RC4. Fig 3.6 presents the complete working of RC4 encryption algorithm. KSA generates the 256 byte initial state vector S, by scrambling input state vector with a random key K. The S contains a permutation of 8 bit words i.e. 256 bytes. The secret key k is generally of length between 8 to 2048 bits and the expanded key K (K of length N=256 bytes) is produced by performing simple repetitions. The expanded key is generated in the manner such that if secret key k is of length l bytes, the expanded key will be K[i] = k [i mod l] for $0 \leq i \leq N-1$. Further S pairs are swapped and an initial state SN-1 is achieved at the end which is the input to the second module PRGA. It generates the keystream of words and is further XORed with the plaintext to produce a ciphertext. To figure axis labels, use words rather than symbols. Do not label axes only with units. Do not label axes with a ratio of quantities and units. Figure labels should be legible, about 9-point type. It is to be noted that each time a new keystream byte 0 is required, RC4 runs the loop of PRGA and each time with the generation of new keystream the internal state S is updated.



a) RC4 Key scheduling algorithm



b) RC4 Pseudo random generation algorithm

Fig. 1: RC4 Stream Cipher

3.2 Introduction of RSA:

This Ronald Rivest, Adi Shamir and Leonard Adleman in 1997 provided maximum security for the data over network by giving this RSA algorithm. This security system is composed of three phases namely Key Generation, Encryption and Decryption. Also we can note that many security systems are built using this three phase scheme. In this method there are two keys Private Key and Public Key. Public Key is used to encrypt the message and can be seen by all, where as the private key also called as the secret key is used to decrypt the messages.

Also there are methods to break RSA security [1] Public key cryptography is one of the system which is not very secure because it is very much prone to insecurities while sending which is seen in the internet today. But, there are many algebraic assumptions which we have considered as an important key in this issue. For example, integer factoring problem and finding out prime numbers. To find out n in RSA we have to find out p and q which are prime numbers. Also , modulo n is a NP hard problem and many of the Public key cryptography are relied upon it[2] but it is not practically possible because the quadratic sieve is used for factorizing RSA-120 by Thomas, Bruce, Arjen and Mark[3] . Also, the RSA-140 is factored using number field sieve by Cavallar, Dodson, Lenstra, Leyland, Lioen, Montgemery, Murphy and Zimmermann [4]. While RSA-155 is factored in 1999, also, the RSA-160 is factored in April 2003, and the RSA-576 is factored in December 2003 by Eric [5]. The RSA-200 is factored in 2004; the RSA-640 is factored in November 2, 2005 by Bahr, Boehm, Franke and Kleinjung [6] and verified by RSA Laboratories. The relation between factoring and the public key encryption schemes is one of the main reasons that researchers are interested in factoring algorithms [7]. In 1976 Diffie-Hellmam [8] creates the first revolutionary research in public key cryptography via presented a new idea in cryptography and to challenge experts to generate cryptography algorithms that faced the requirements for public key cryptosystems. However, the first reaction to the challenge is introduced in 1978 by RSA [9].

RSA has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions [10]. After seeing several examples of “classical" cryptography, where the encoding procedure has to be kept secret (because otherwise it would be easy to design the decryption procedure), we turn to more modern methods, in which one can make the encryption procedure public, without sacrifice of security: knowing how to encrypt does not enable you to decrypt for these public key systems [11]. To understand how the algorithm was designed, and why it works, we shall need several mathematical ingredients drawn from a branch of mathematics known as Number Theory, the study of whole numbers. In recent times it has been found very useful, as we shall see. Here are the ingredients we will draw from number theory:

- Modular arithmetic
- Fermat's “little" theorem
- The Euclidean Algorithm

This idea omits the need of a carrier to deliver keys to recipients over another secure channel before transmitting the originally intended message. In RSA encryption keys are public, while the decryption keys are not, so only the person with the correct decryption keys can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key cannot be easily deduced from the public encryption key

3.3 RSA Algorithm:

Ronald Rivest, Adi Shamir and Leonard Adleman in 1997 also proposed a method for digital signatures and RSA cryptosystems. A digital signature is mathematical scheme which provides authenticity of a digital message and assures the recipient that the message was created by an authorized sender and was not modified in transit[12]. Generally, digital signature algorithms are based on a single hard problem like problem like prime factorization problem or discrete logarithmic or elliptic curve problem. If we can find the solution of any of one of these NP Hard problem then we can easily tamper with the security of the RSA DSA (RSA Digital Signature Algorithm). The RSADSA is an asymmetric cryptographic technique, whose security is based on the level in which we are factorizing [13].

3.3.1. Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encryption of message. Messages encrypted with the public key can only be decrypted using the private key. The key for the RSA algorithm are generated the following way

1. Choose 2 distinct prime numbers p and q

For security purpose the integers p and q should be chosen at random and should be of similar bit length. Prime integers can be efficiently found using a primality test.

Compute n = pq.

n is used as the modulus for both the public and private keys

Compute φ (n) = (p – 1)(q – 1), where φ is Euler's totient function.

Choose an integer e such that 1 < e < φ (n) and greatest common divisor of (e, φ(n)) = 1; i.e., e and φ (n) are coprime.

e is released as the public key exponent.

e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of e (such as 3) have been shown to be less secure in some settings.[4]

Determine d as:

$$d=e^{-1} \pmod{\varphi(n)}$$

i.e., d is the multiplicative inverse of e mod φ(n).

This is more clearly stated as solve for d given (de) = 1 mod φ (n)

This is often computed using the extended Euclidean algorithm.

d is kept as the private key exponent.

3.3.2 Encryption:

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c = m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice. Note that at least nine values of m could yield a ciphertext c equal to m, [5] but this is very unlikely to occur in practice.

3.3.3. Decryption:

Alice can recover m from c by using her private key exponent d via computing

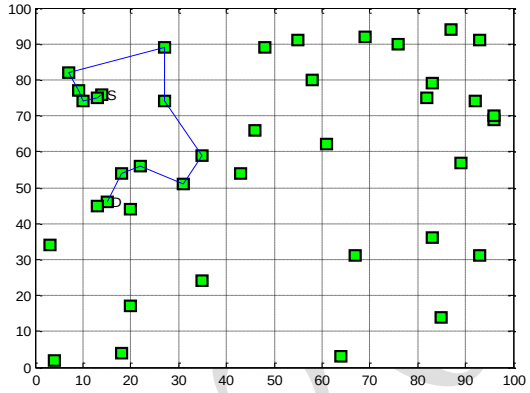
$$m = c^d \pmod{n}$$

Given m, she can recover the original message M by reversing the padding scheme

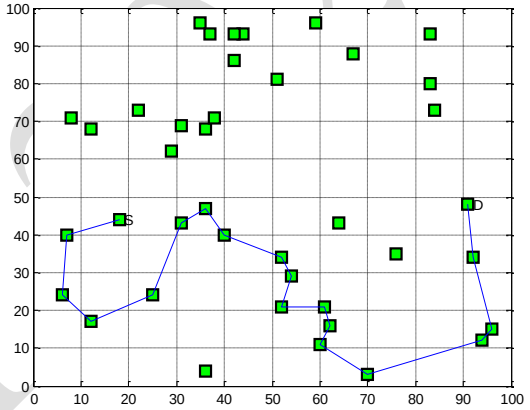
4. Result and Discussion:

Results for AODV routing at different number of nodes in WSN at various packet size for variety of network distribution are performed at MATLAB platforms. The upcoming section covers results for following cases for source to destination routing and throughput values for RSA and RC4 coding:

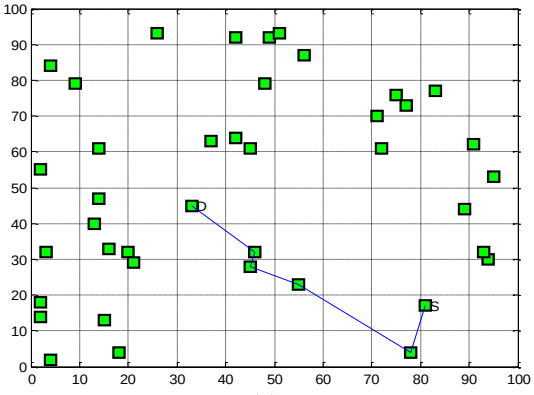
Case: Routing for Node= 40 and packet size 500:



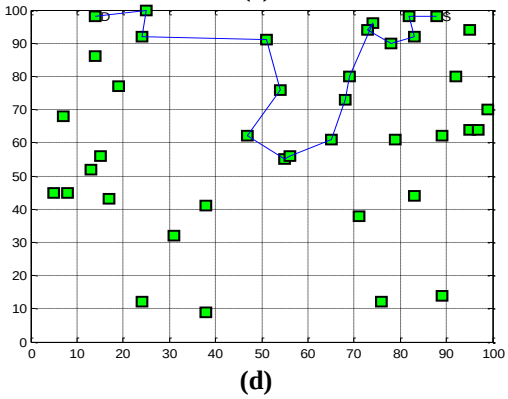
(a)



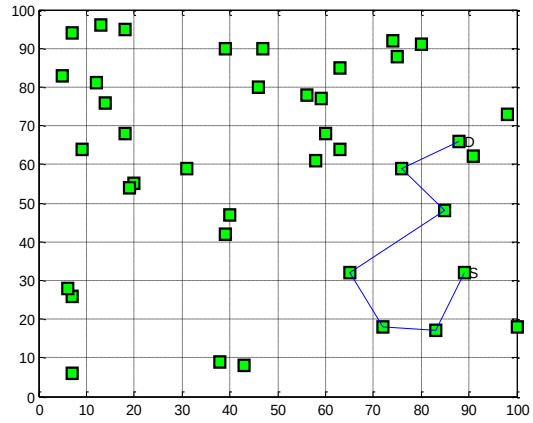
(b)



(c)

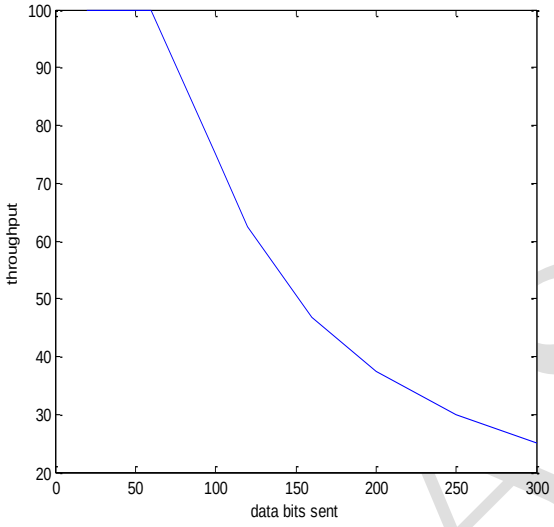


(d)

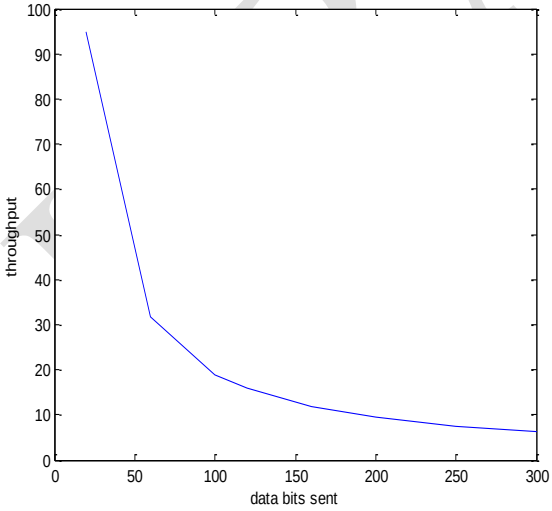


(e)

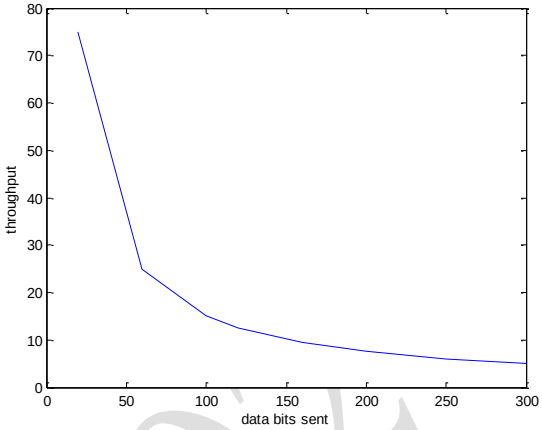
Fig 2: AODV routing for 40 nodes network at 5 different node distributions using RC4.



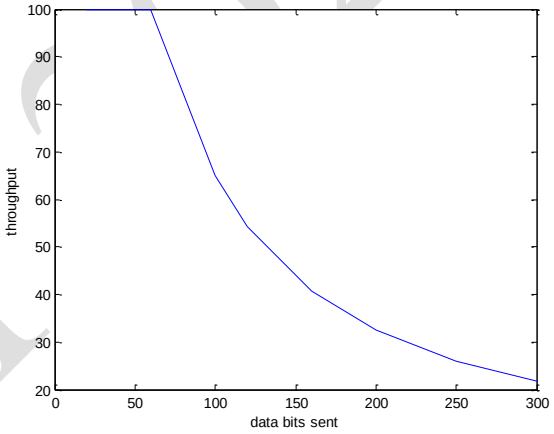
(a)



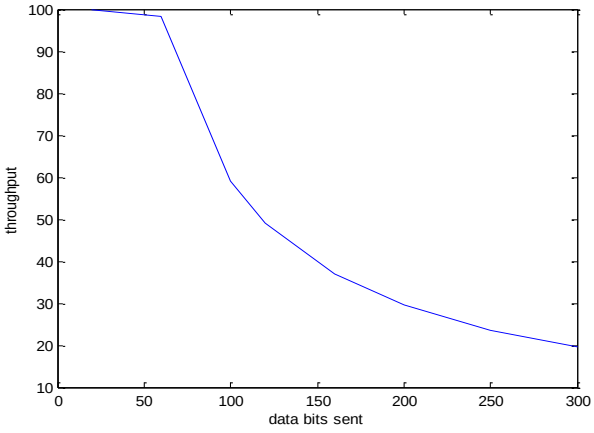
(b)



(c)



(d)



(e)

Fig 3: Through values for figure 4.1 shown networks at packet size of 500 using RC4.

The above fig 2 shows the routes developed by AODV routing for all the 5 different 40 node networks. By these routes data is transferred at a packet size of 500. The throughput is shown in fig 3 during the data transmission through above routes for RSA encryption

5. Conclusion:

This work demonstrates one of the aspects of WSN network called as data security. We have focused on ciphering techniques performance over the transmission delay. For this purpose different WSN networks with variety of sensor node distribution at different nodes are observed in terms of time consumed in transmission mode with AODV routing time prior to RC4 and RSA ciphering. It has been observed that for all the cases RC4 ciphering consumes less time as compared to RSA ciphering. Hence it proves that for WSN networks RC4 ciphering provides higher transmission rate due to small time consumtion in ciphering diciphering. In future we can also check performance for routing technique other than AODV. We may also consider composite routing mechanism that involves artificial intelligence tools for determining the shortest possible route in minimum time. It can also helps in minimizing time delay in data transmission in WSN network with high security concerns.

References:

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Hand- book of Applied Cryptography. CRC Press, August 2011 edition, 1996. Fifth Printing.

[2] Douglas R. Stinson. Cryptography: Theory and Practice. CRC Press, third November 2005) edition, 1995.

[3] Thomsan D. Bruce D. Arjen L. and Mark M.,"On the Factoring of RSA-120", (169), pp.166-174, 1994

[4] Cavallar S, Dodson B, Lenstra A, Leyland P,Lioen W, Montgemery P, Murphy B, and Zimmermann P, "Factoring of RSA-140 using the number field sieve", 1999

[5] Eric W "Prime Factorization Algorithm", Mathworld.woiframe.com/news/ 2003

[6] Bahr F, Boehm M, Franke J and Kleinjung T, "For the Successful Factorization of RSA-200" www.rsasecurity.com

[7] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc On- Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[8] Diffie W and Hellman M, "New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[9] Rivest R, Shamir A and Adelman L, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communications of the ACM, 21, pp. 120-126, 1978

[10] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000.

[11] Priteshkumar Prajapati et. al., " Comparative Analysis of DES, AES, RSA Encryption Algorithms", International Journal of Engineering and Management Research, Volume-4, Issue-1, February-2014.

[12] Sourav Sen Gupta and Subhamoy Maitra, "(Non-)Random Sequences from (Non-) Random Permutations—Analysis of RC4 Stream Cipher" J. Cryptol. (2014) 27: 67–108.

[13] Avala Ramesh et. al., " Analysis On Biometric Encryption using RSA Algorithm", International Journal Of Multidisciplinary Educational Research, Volume 2, Issue 11(2), October 2013.