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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Security in Patient Data Communication using Encryption Algorithm

Nikita S. Karekar, Dr. Prof. R. S. Kawitkar

M.E. Student, Dept. of Electronics, Sinhgad College of Engineering, Pune, India

Professor, Dept. of Electronics, Sinhgad College of Engineering, Pune, India

ABSTRACT: Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including healthcare applications, home patient monitoring, military. MANET has various type of routing protocols. One of them is Ad hoc On-Demand Distance Vector (AODV) routing protocol which we are considering as a base protocol in our project. In this project, we propose a practical approach to prevent the inside attacks in the healthcare applications from attackers or hackers. Here we provide the security to the network layer by using encryption and decryption standards and a cryptographic mechanisms such as Advance Encryption Standard (AES), Rivest-Shamir-Adleman Algorithm (RSA) and Secure Hash Algorithm (SHA). Simulation has been done using Network Simulator Software (NS2).

KEYWORDS: MANET, AODV, AES, RSA, SHA

I. INTRODUCTION

In recent years, wireless sensor networks have been widely used in health care applications, such as hospital and home patient monitoring. Wireless medical sensor networks are more vulnerable attacks than the wired networks[1]. If patient health data gives the bad guys or hacker more time than credit cards do. Patient data is permanent and cannot be changed. Patient health informationserves many more purposes than credit card information does. Cyber criminals use patient data for high-value purchases like fraudulent insurance claims, medical equipment, and even drugs.The available solutions can secure the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data. We can protect transmitted patient attacks but inside attacks need separate protection. To prevent inside attacks advanced cryptographic techniques are used.

From a security perspective, mobile ad hoc networks (MANETs) inherit the same problems that exist in managed, wireless networks. MANET connects mobile devices together by wireless link. Most of the time, the nodes in MANET are mobile and can request to connect or leave the network. Network topology will frequently change. If mobile nodes are in the same wireless range, they can communicate directly but, if it is not then communication will be lost. To make possible communication although wireless which is out of range, cooperation from other nodes is required.Each node in the MANET has to play two roles, i.e., as a host and as a router. As a router in a multi-hop network, each node has to control and manage the routing path. For that, they require a standard routing protocol to facilitate the communication cooperation. Routing protocol also makes MANET become attractive to network users whereby creating any network will be fast and simple. MANET routing focused on security issues, less attention has been devoted to privacy[2].Unfortunately, MANET is also vulnerable to attack like any other networks. In fact it is more vulnerable than wired network.

MANET has number of routing protocols and normally they are classified into proactive and reactive protocol one of it isAd hoc On-demand Distance Vector (AODV).This is an example of reactive routing protocol for ad hoc network.In reactive protocol nodes in the network exchange routing information only when a communication must take place and it keep this information up-to-date till the communication lasts. As there is no safety mechanism was establishedthis protocol is susceptible tothe existence of malicious attack. AODV protocols are always assumed as trusted.Whenever any node wants to send packet, it checks its routing table to search valid and active path to the receiver. If it does not

DOI: 10.15680/IJIRCCE.2017. 0505177

find any path then it advertises that packet by using route request packet (RREQ) to start the path discovery. When it finds the destination node then it sends reply by route reply packet (RREP) to transmitter node. It finds fresh and fast route by comparing destination sequence number from its routing table.

II. RELATED WORK

Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson [1] gives the information about practical approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy. Karim El Defrawy and Gene Tsudik[3] present an efficient technique i.e. PRISM protocol which supports anonymous reactive routing in suspicious location based MANET's . Durgesh Wadbude, Vineet Raichariya[4] proposed approach uses improved of security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. Pankaj Sharma and Yogendra Kumar Jain has designed and studied performance of Ad-hoc On Demand Vector (AODV) protocols has been modified by including the source route accumulation feature. Security demands that all packets be authenticated before being used.

III. PROPOSED ALGORITHM

A. Scope

Ad hoc On-Demand Distance Vector is a routing protocol for MANETs. It enables "dynamic, self-starting, multi-hop routing between mobile nodes wishing to establish and maintain an ad hoc network". AODV defines 3 types of messages: Route Requests (RREQs), Route Replies (RREPs), Route Errors (RERRs). RREQ messages are used to initiate the route searching process. To finalize the routes RREP messages are used and if any error occur in network then RERR messages are used to notify that.

The AODV protocol doesn't have security considerations. (Refer fig.2 & 3), therefore it will be more vulnerable to many threats. It is assumed every node is truthful. Once a node claims that it has the shortest path to the destination, other nodes may trust it. The adversary node in the network responds any received RREQ by false RREP which it claims having the freshest and shortest path to the destination. Malicious nodes can attract all network traffics by falsely claiming to have a fresh and the shortest path to the destination. When a RREQ packet is received by a fake node, it sends back a RREP packet with a large sequence number and less hop count, which gives a fresh and shortest path to the destination.Once the source node receives the RREP packet it will send all packets to this adversary node as the next hop. When an adversary node is positioned near the source node then the ratio of packet dropping by malicious node will be increased. To overcome these problems we can use SHA & AES cryptographic algorithms. In route request and route reply message formats security field is not provided in AODV.

a. AES Algorithm

In AES encryption algorithm block length and the key length can be specified to be 128, 192, or 256 bitsindependently. AES parameters built upon the key length.

The input to the encryption and decryption algorithms is a single 128-bit block[6]. Fig.1 shows the flow of AES encryption algorithm. In this project we are using 5678 as a public key which will be known to everyone and the private key used is 01234567891234560123456789123456

DOI: 10.15680/IJIRCCE.2017. 0505177

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

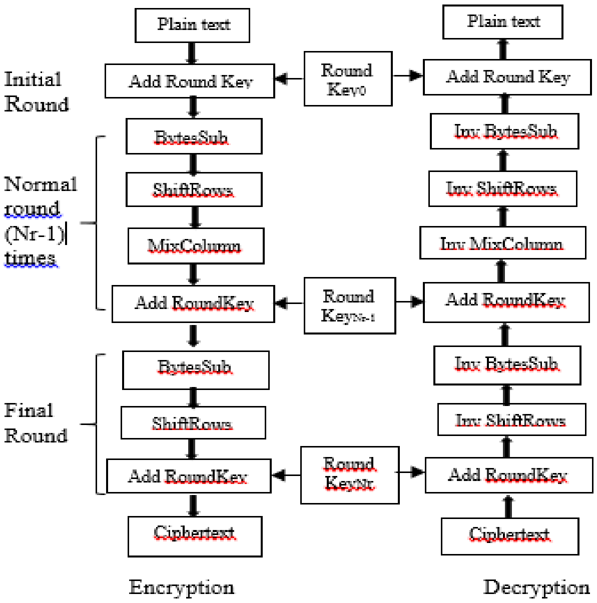


Fig.1 AES Algorithm

b. *RSA Algorithm:*

Rivest, Shamir, and Adleman have developed this scheme makes use of an expression with exponentials. Plaintext is enciphered in blocks.Individual block has a binary value which is not more than some number *n*. The block size must be beneath or equal to log2(*n*) where 2*i* <*n* 2*i*+1, the block size is *i* bits[6]. For some plaintext block *M* and ciphertext block *C*Encryption and decryption are of the following form:

$C = Me \bmod n$ (1)

$M = Cd \bmod n = (Me)d \bmod n = Med \bmod n$ (2)

The value of *n*must be known to both sender and receiver. The senderhave the value of *e*, and only the receiver knows the value of *d*. So that it is called as a public-key encryption algorithm with a public key of *PU* ={*e*, *n*} and a private key of *PU* = {*d*, *n*}. RSA Encryption is faster than other algorithms.RSA encrypted message is difficult to decrypt than any other algorithms.

c. *SHA Algorithm*

SHA stands for Secure Hash Algorithm. This algorithm is most widely used for the security applications and protocols. Hash value is generated of AES encrypted data.Following algorithm structure used for SHA-1

i. Padding bits
ii. Appending length as 64 bit unsigned
iii. Buffer initiation
iv. Processing of message
v. Output

B. *Block Diagram*

The proposed mechanism shows a secure communication between the mobile nodes using hybrid1 cryptography. Data transmission between the two mobile nodes has been assumed whenever source is active itguaranteed that the source is interacting with real node. The Fig.2 explains process of Encryption & authentication. [8]

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

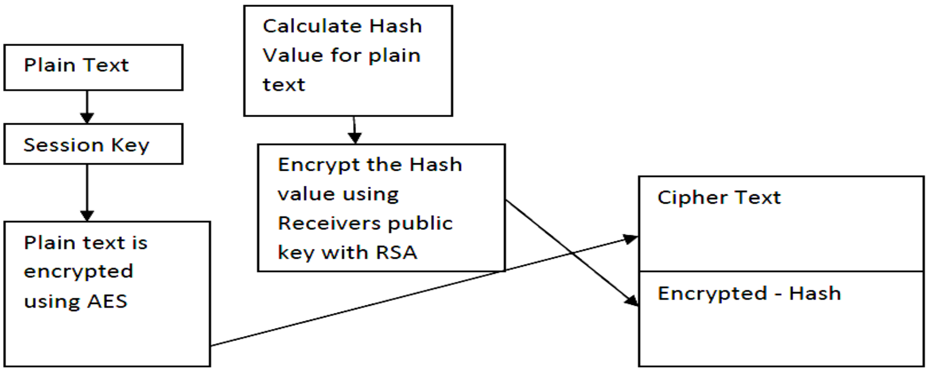

Plain Text
Session Key
Plain text is encrypted using AES
Calculate Hash Value for plain text
Encrypt the Hash value using Receivers public key with RSA
Cipher Text
Encrypted - Hash

Fig.2 Encryption Process & authentication.

Fig.3 Explains process of Decryption & authentication.[8]

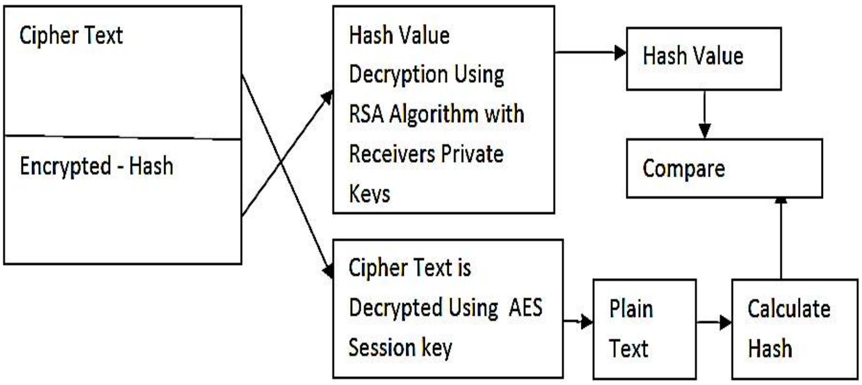

Cipher Text
Encrypted - Hash
Hash Value Decryption Using RSA Algorithm with Receivers Private Keys
Hash Value
Compare
Cipher Text is Decrypted Using AES Session key
Plain Text
Calculate Hash

Fig.3 Decryption Process & Authentication.

The service uses a key management to get back the extended public key it is ensured by the third party for recognition of the destination. The destination also uses same methodology to corroborate the source. A shared key is generated after execution of the key management module which is used by both source and destination.Like this all messages are transmitted to the destination. In this hybrid encryption approach, sender side using 128-bit session key value with AES to encrypt the message.The hash value of message was encrypted using RSA algorithm with 1028 bit Extended Public key of the receiver. In the receiver side the decryption done for the encrypted message using AES with 128-bit session key value.Using RSA with 1028 bit extended private key of the receiver to decrypt the encrypted hash value. To ensure the integrity the comparison is carried out between calculated and decrypted hash values. The simulation results can be seen by using network simulator.

Figures 4 & 5 are the frame formats for SAODV which shows extended Digital Signature fields provided for security, this shows the modifications which are carried out in RREQ and RREP.

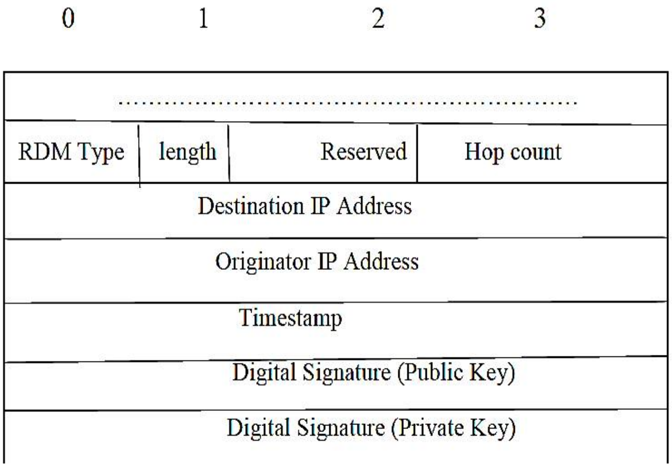
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

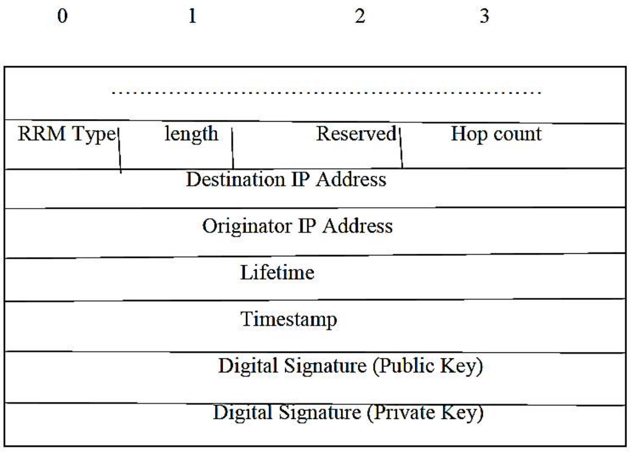
Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



0	1	2	3
……………………………………………………			
RDM Type	length	Reserved	Hop count
Destination IP Address			
Originator IP Address			
Timestamp			
Digital Signature (Public Key)			
Digital Signature (Private Key)			

Fig.4 Route Discovery Message Format (RDM)



0	1	2	3
……………………………………………………			
RRM Type	length	Reserved	Hop count
Destination IP Address			
Originator IP Address			
Lifetime			
Timestamp			
Digital Signature (Public Key)			
Digital Signature (Private Key)			

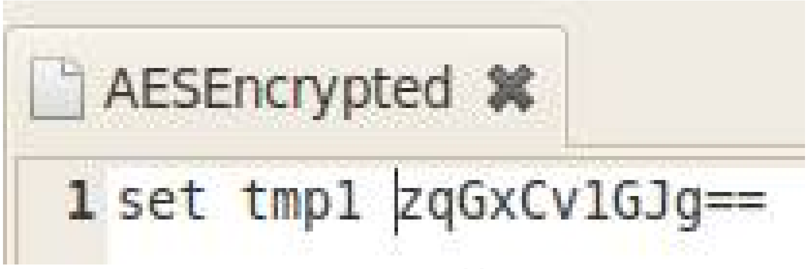
Fig.5 Route Reply Message Format (RRM)

C. *Methodology*

The system is proposed to provide security for data communication. The security can be provided by using three algorithms namely Advanced Encryption Standard (AES), Rivest-Shamir-Adleman Algorithm (RSA), SecureHash Algorithm (SHA). These algorithms are used for encryption and decryption purpose. Two level security is provided by using these security algorithms. A private 32 byte key is given to the data which we want to transmit for the sender and then the data is transferred at the receiver side. The person at the receiver side will get the encrypted data and that particular person should know the private key which is attached with the data after typing that known key the data will be decrypted. End-to-end encryption is carried out here, as the private key which is a secret key only known to sender person and receiver person. The network scenario is carried out in NS-2 software where we will take the some random wireless nodes.

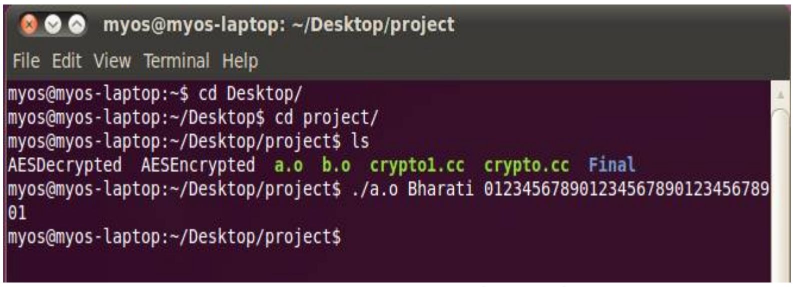
IV. **RESULT**

Figures 6 to 13 showthe encryption and decryption process which is carried out in NS2 software. Fig.7 shows the commands for encryption of data and the result is shown in fig. 6



```
set tmp1 zqGxCv1GJg==
```

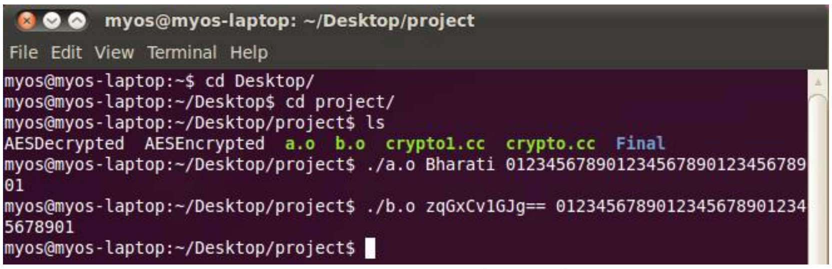
Fig.6AES Encrypted data


myos@myos-laptop: ~/Desktop/project
File Edit View Terminal Help

```
myos@myos-laptop:~$ cd Desktop/
myos@myos-laptop:~/Desktop$ cd project/
myos@myos-laptop:~/Desktop/project$ ls
AESDecrypted  AESEncrypted  a.o  b.o  crypto1.cc  crypto.cc  Final
myos@myos-laptop:~/Desktop/project$ ./a.o Bharati 0123456789012345678901234567890
01
myos@myos-laptop:~/Desktop/project$
```

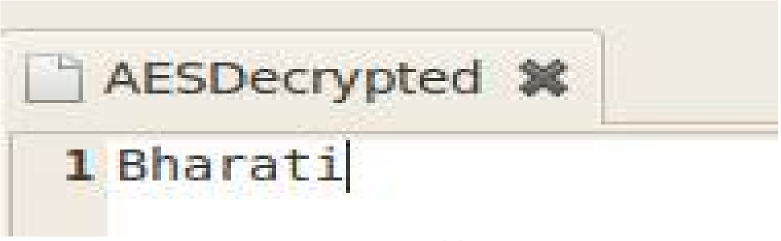
Fig.7AES Encryption in NS2 with private key

For the decryption same private key is used following with decrypted data as in fig. 8 and its result window is as in fig.9.


myos@myos-laptop: ~/Desktop/project
File Edit View Terminal Help

```
myos@myos-laptop:~$ cd Desktop/
myos@myos-laptop:~/Desktop$ cd project/
myos@myos-laptop:~/Desktop/project$ ls
AESDecrypted  AESEncrypted  a.o  b.o  crypto1.cc  crypto.cc  Final
myos@myos-laptop:~/Desktop/project$ ./a.o Bharati 0123456789012345678901234567890
01
myos@myos-laptop:~/Desktop/project$ ./b.o zqGxCv1GJg== 0123456789012345678901234
5678901
myos@myos-laptop:~/Desktop/project$ 
```

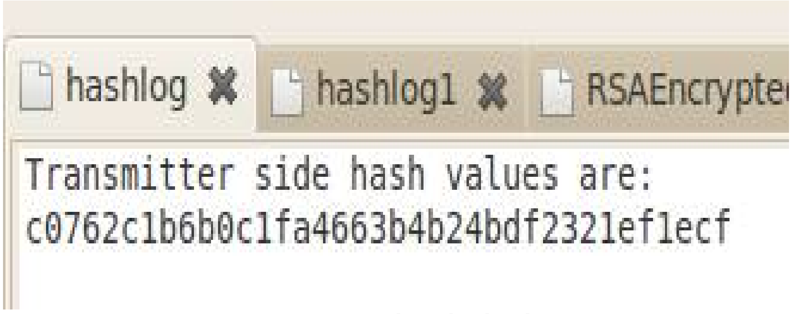
Fig.8AES Decryption in NS2 with private key



```
Bharati
```

Fig.9AES Decrypted data

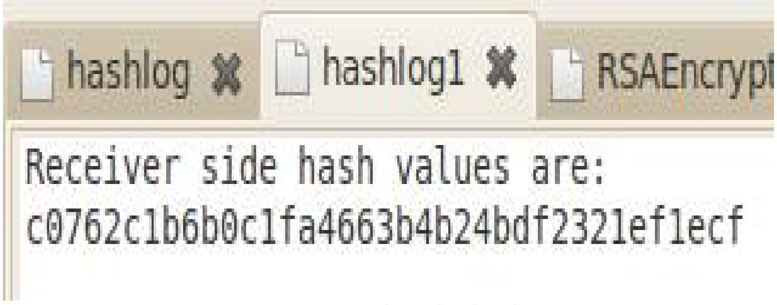
For more security purpose the AES encrypted data followed through the SHA-1 cryptographic algorithm which is shown in fig. 10 at the transmitter side.



```
Transmitter side hash values are:
c0762c1b6b0c1fa4663b4b24bdf2321ef1ecf
```

Fig.10Transmitter side Hash values log

Fig. 11 shows the receiver side hash value. Further RSA technique is carried out correctly if and only if both transmitter and receiver hash values are same.

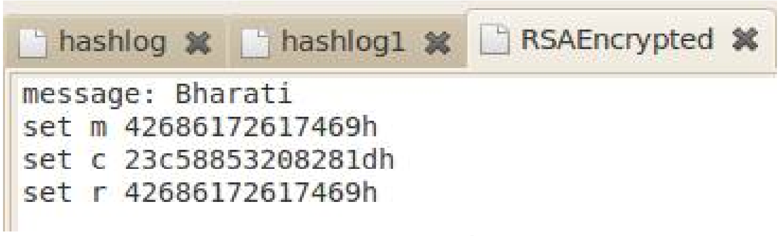


```
Receiver side hash values are:
c0762c1b6b0c1fa4663b4b24bdf2321ef1ecf
```

Fig.11Receiver side Hash values log

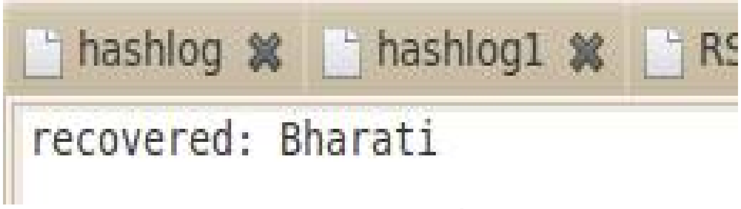
Fig. 12 shows the recovered data with the RSA calculated values which are namely m represents the value of plain text and c represents the value of cipher i.e. encrypted text.

Finally, fig. 13 shows the output at the receiver side i.e. decrypted data.



```
message: Bharati
set m 42686172617469h
set c 23c58853208281dh
set r 42686172617469h
```

Fig.12 RSA encryption log



```
recovered: Bharati
```

Fig.13 RSA Decryption log

V. CONCLUSION

In this methodology Security issues for AODV will be implemented. It focuses on authentication security architecture. It will provide secure data transmission between the source and destination using cryptographic algorithms. Thus by using hybrid cryptography we provide security to the AODV algorithm.The proposed mechanism will authenticate the node and ensure the security of important routing information in AODV protocol. The Simulation Results can be seen using network simulator like NS-2.

REFERENCES

[1] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson, “Privacy Protection for Wireless Medical Sensor Data”, DOI 10.1109/TDSC.2015.2406699, IEEE Transactions on Dependable and Secure Computing

[2] Kamarularifin Abd Jalil, Zaid Ahmad Jamalul- Lail Ab Manan2011, “Securing Routing Table Update in AODV Routing Protocol” IEEE Conferece on Open systems (ICOS2011),SEPTEMBER 25-28,2011,Langkawi,Malasia

[3] Karim El Defrawy, Member, and Gene Tsudik, “Privacy-Preserving Location-Based On-Demand Routing in MANETs”, IEEE Journal On Selected Areas In Communications, VOL. 29, NO. 10, DECEMBER 2011

[4] Durgesh Wadbude, Vineet Richariya An Efficient Secure AODV Routing Protocol in MANET, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012 274

[5] Cerri and Alessandro Ghioni, Securing AODV:The A-SAODV Secure Routing Prototyped vide

[6] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition

[7] USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks IEEE Transactions On Wireless Communications, VOL. 11, NO. 5, MAY 2012

[8] Satyendra Sing, Vinod Kumar Yadav, Ganesh Chandra, Rahul Kumar Gangwar, An Efficient and Improving The Secrity Of AODV Routing Protocol.

BIOGRAPHY

Nikita Karekar is an M.E. student in the Sinhgad College of Engineering, Pune

Dr. Prof. Rameshwar Kawitkar is a Professor in E&TC Engg Dept in Sinhgad College of Engineering, Pune. He completedPh.D.(ElectronicsEngg).