ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

A Survey on VANET Security using ECC, RSA & MD5

Rukaiya Shaikh[1], **Disha Deotale**[2]

ME Computer Engineering, G.H.R.I.E.T., Savitribai Phule University, Pune, India[1]

Professor, Dept.of Comp.Engg, , G.H.R.I.E.T., Savitribai Phule University, Pune,India[2]

Abstract: Now a day, Vehicular Ad-hoc Networks (VANET) are becoming more popular as the accident statistics increase. VANET simply provides many safety applications to save people lives while driving on road, It also eliminate accidents and damage to the vehicles and people. VANET also save our time by providing information about busy traffic on ongoing road. But on the other hand we should also consider some of the security related issues such as privacy of drivers including location and identifier information should be preserved in the network. So for preventing many of attacks and also preserving privacy of drivers, many protocols need an infrastructure for key distribution, revocation and secure exchange of the messages containing private information.

For providing secure communication here using various cryptography based methods. Some security mechanisms used for encrypting and authenticating V2V and V2I messages comes with overhead in terms of computation and communications between the vehicles. Therefore, in order to increase the feasibility and better performance of cryptographic based protocols, we should have to investigate operation of different cryptography based methods. Due to high mobility nodes in the network or high speed vehicles we need to select appropriate cryptographic method that should have a very little processing time, have a small key length, small of length of created message as much as possible and have an acceptable level of safety over the key lifetime.

In this survey paper, system described various cryptographic algorithms such as RSA, Elliptic Curve Cryptography, and Message Digest 5(MD5) with their pros and cons. They provide better security and privacy if we use combination of this algorithm. In this survey work, briefly described the comparison between the RSA and ECC.

Keywords: Elliptic Curve Cryptosystem, Elliptic Curve Integrated Encryption Scheme, MD5, RSA.

I. INTRODUCTION

A. Ron Rivest, Adi Shamir and Leonard Adelman (RSA):

- RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology.

-RSA is a cryptosystem for public-key encryption. It is widely used for securing sensitive data, particularly when the data is sending over an insecure network such as the Internet.

-Public-key cryptography, also known as Asymmetric Cryptography,. It uses two different but mathematically linked keys, i.e. public Key and Private Key. The public key can be shared with everyone, whereas the private key must be kept secret with the receiver.

- In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

- RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total factoring is considered infeasible due to the time it would take even using today's super computers.

-The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q, are generated using the Rabin-Miller primality test algorithm. A modulus n is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length.

-The public key consists of the modulus n, and a public exponent, e, which is normally set at 65537, as it's a prime number that is not too large. The e figure doesn't have to be a secretly selected prime number as the public key is shared with everyone.

- The private key consists of the modulus n and the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

B. Message Digest Algorithm 5

- MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data.

- MD5 which stands for Message Digest algorithm 5 is a widely used cryptographic hash function that was invented by Ronald Rivest in 1991.

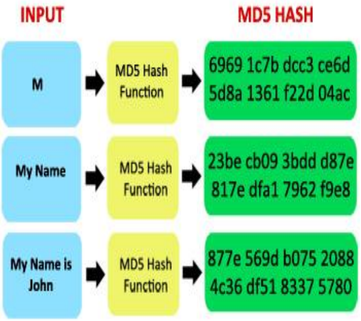
DOI 10.17148/IJARCCE.2015.4637

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

- The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size “hash value” as the output.

- The input data can be of any size or length, but the output “hash value” size is always fixed.


INPUT
MD5 HASH
M
MD5 Hash Function
6969 1c7b dcc3 ce6d 5d8a 1361 f22d 04ac
My Name
MD5 Hash Function
23be cb09 3bdd d87e 817e dfa1 7962 f9e8
My Name is John
MD5 Hash Function
877e 569d b075 2088 4c36 df51 8337 5780

• Here is an example of MD5 Hash function at work:

From the above example, whatever the input size you give, the algorithm generates a fixed size (32 digit hex) MD5 hash.

- This hash is unique for every file irrespective of its size and type. For example, two different executable files (.exe files) with the same size will not have the same MD5 hash even though they are of same type and size. So MD5 hash can be used to uniquely identify a file. The same thing applies even for messages where each message that was sent and received can be verified using the MD5 hash.

- The MD5 algorithm is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

C. Elliptic Curve Cryptographic Algorithm

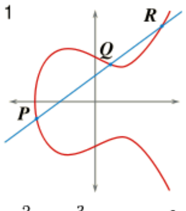
- Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

- The equation of an elliptic curve is given as,

$$\mathbf{Y^{2} = x^{3} + ax + b}$$

Where:

a and b are elements of a finite field with p^n elements, where p is a prime number which is selected as larger than 3.The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation $\mathbf{y^{2} = x^{3} + ax + b}$ defining the curve, plus an extra point that is said to be at infinity.



$y^2 = x^3 + ax + b$

1) **Key Generation**

Key generation is an important part, where user has to generate public key and private key. The senders who want to send the message, he will first encrypt the message with receiver’s public key and the receiver will decrypt that ciphertext with its private key. Now, we have to select a number‘d’ within the range of ‘n’. Using the following equation we can generate the public key

$$\mathbf{Q=d*P}$$

d = The random number that we have selected within the range of (1 to n-1).
P is the point on the curve.
‘Q’ is the public key and ‘d’ is the private key.

2) **Encryption**

Let ‘m’ be the message that we are sending. We have to represent this message on the curve.
Consider the message ‘m’ has the point ‘M’ on the curve ‘E’. Now, randomly select value of ‘k’ from [1 – (n-1)].
Two cipher texts will be generated let it be C1 and C2.

$$C1 = k*P$$
$$C2 = M + k*Q$$

Ciphertext C1 and C2 will be send to the other user.

3) **Decryption**

4) Here, in this decryption process receiver will decrypt the ciphertext message with its own private key to get original message.

$$M = C2 – d * C1$$

II. LITERATURE SURVEY

A. RSA Algorithm

1). Steps for the RSA Algorithm.

- **Key generation**

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct sufficiently large prime number say p and q. For security purposes, we must choose the integers p and q randomly, and both number should be of similar bit-length.

2. Compute n = pq.

3. Compute φ(n) = (p − 1)(q − 1) = n - (p + q -1), where φ is Euler's value and we have to keep this value as private.

4. Choose an integer e such that 1 < e < φ(n) and gcd (e, φ(n)) = 1; 1] e is released as the public key exponent. 2] e with short bit length and small Hamming weight provide more efficient encryption most commonly

2^{16} + 1 = 65,537.However, much smaller values of e (for ex.3) will not give you more secure encryption.

5. Determine d as d ≡ e^{-1} (mod φ(n));

This is more clearly stated as: solve for d given
d· e ≡ 1 (mod φ(n)) 1 and 0<d<n.

DOI 10.17148/IJARCCE.2015.4637

6. Public key is (e, n) and private key is (d, n). Where, the value of *d* is kept as the private key exponent.

- **Encryption**

User A transmits his public key (n,e) to **User B** and keeps the private key secret. If **User A** wish to send message M to **User B**. Then first he has to turns M into an integer 0 < m < n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to:

$$\mathbf{c = m^{e} mod\ n}$$

This can be done quickly using the method of exponentiation by squaring. **User A** then transmits c to **User B.**

- **Decryption**

User B can recover m from c by using his private key exponent d by the following computation:

$$\mathbf{m = c^{d} \quad mod\ n}$$

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

2). Advantages and Limitation:

There is a problem for using RSA [2] in message exchanging in VANET. Message size should be small. This means that RSA Algorithm can not be used for encrypting long messages in the network. On the other hand, many of messages that should transmit securely in vehicle to vehicle (V2V) or vehicle to roadside unit (V2R) communications are long messages. This long message usually consists of message signature or other security information in addition to the message.

While using RSA algorithm in VANET, Setting a large key is not a good idea .Because VANET is sensitive to time and if we increasing the key size, then decryption and specially encryption will take more time.

There is another way for encryption long messages. Since RSA is quite slow, the usual way to encrypt large messages is using hybrid encryption. In hybrid encryption we use a fast symmetric encryption algorithm for encrypting the data with a random key. The random key is the same secret key that encrypted with RSA and send along with the symmetric key encrypted data.

B.MD5 AND RSA Algorithm to Improve Security in VANET Systems

1). Introduction

MD5, which was created by Professor Ronald L. Rivest of MIT, is basically designed for use with digital signature applications. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321.

MD5 [3] algorithm is basically used to verify integrity of the data with the help of 128-bit message digest from data input. According to the standard, sometime it is called as "Computationally Infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but it offers much more assurance of data security.

RSA used for encryption and authentication. The RSA algorithm is the mainly used in encryption and authentication algorithm it is part of the Web browsers from Microsoft and Netscape. The encryption system is based by RSA Security. Its security is based on the difficulty of factoring large integers. Presently, most implementations of the RSA algorithm employ the use of 512-bit numbers. Cracking such a system requires the ability to factor the product of two 512-bit prime numbers. Factoring a number of this size is well beyond the capability of the best current factoring algorithms.

2).Flow Diagram

The flow diagram [3] of combined MD5 and RSA algorithms describes how the security provided by the combined MD5 and Iterative RSA algorithms. The MD5 and iterative RSA algorithms are applied to input data. Both algorithms generate secure data. Secure data is divided into the encrypted data and the and create the output data .User send this output data to receiver, then on this encrypted output data receiver applied the decryption technique to get the original data.

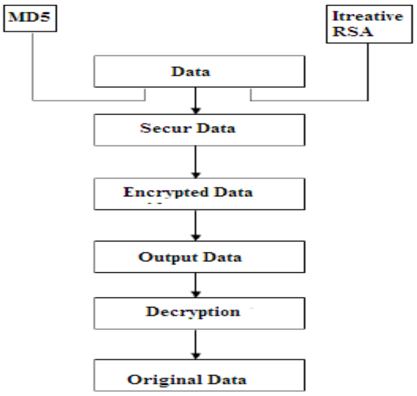


Fig 2.1: Flow Diagram for Security using MD5 and RSA

3). Advantages and Limitation

Various Securities in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. Generally MANETs suffer from various security attacks because of its features such as it provides open medium access to users. So it is very much sensitive as we consider the security issue.

Here Author [3], Implemented hybrid system using MD5 & RSA encryption algorithm to provide data security according to attacks. Any method used in order to improve the data availability with the use of multiple node-disjoint paths must consider the actual physical proximity of data transmissions on various paths. In this work the MD5 & RSA algorithms are combined, to improve the security of such network. The combined approach of both RSA and MD5 algorithms secures the data from unauthorised user as well as preserves the confidentiality of the data.

DOI 10.17148/IJARCCE.2015.4637

C. Pairing Based Elliptic Curve Cryptosystem

1). Introduction

Elliptic Curve Cryptosystem [4] is a public key encryption technique based on the theory of elliptic curves. ECC can be used to create faster and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation i.e. $\mathbf{y}^{2} = \mathbf{x}^{3} + \mathbf{ax} + \mathbf{b}$ rather than the traditional method of generation, as the product of very large prime numbers. This technology can be used in conjunction with most of the public key encryption methods such as RSA and Diffie-Hellman key exchange algorithm. ECC can yield a level of security with a 224-bit keys compared with other systems that require a 2,048-bit keys. ECC provides features such as security and computational efficiency. The security of ECC depends on the difficulty of solving the elliptic curve logarithm problem.

2). System Architecture

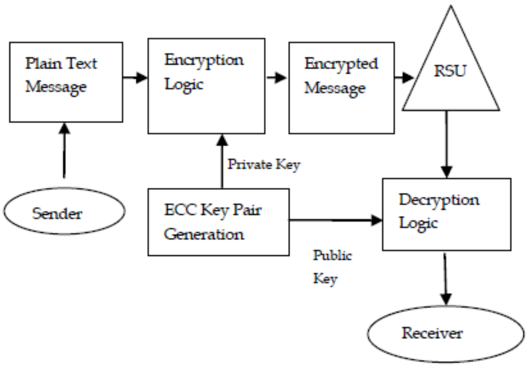


Fig2.2: System Architecture of Pairing Based Elliptic Curve Cryptosystem

- **Elliptic Curve Cryptosystem**

The system based on the elliptic curve is called Elliptic curve cryptosystem. To form a cryptosystem, generally we required a set of following three algorithms:

1. Key-generation Algorithm: An algorithm which is used for generating an encryption/decryption key.

2. Encryption: An algorithm for encrypting plain texts. This algorithm takes original message and converts it into other message called Ciphertext. This generated ciphertext will send to the other user.

- **Decryption**

An algorithm for decrypting cipher texts. In traditional symmetric or private-key cryptography, the generated key is used for both encryption and decryption, with the consequence that anybody that possesses the key is able to en- and decrypt messages. To ensure confidentiality, the key has to be kept secret between communication partners.

- **Key Sizes**

ECC achieves the security level with smaller keys. Key length is most important feature in Elliptic Curve Cryptography. We can get better security level with the smaller key size.

- **Asymmetric Data Encryption**

Here, First Group manager has to distributes and allocates the public keys to each user and authenticate each user by using the ECC authentication mechanism. In order to provide the confidentiality to this transformation of data simply we have to use the cryptography formula named called ECC .For cryptographic process we have used the ECC algorithm for the encryption and decryption process.

- **Asymmetric Data Decryption**

By using the ECC algorithm original file is converted as crypto files. In order to get the original content of the files, the encrypted files must be decrypted with receivers private key. Each and every encrypted file should be decrypted. Using Respective Private keys, files are decrypted using the ECC Key Generator Decryption process is done by ECC Algorithm, Since ECC has 166 key lengths it executes faster and more secured algorithm than RSA.

- **Pairing**

Pairing-based cryptography [4] is used to pair two cryptographic groups to a third group to construct cryptographic systems. If the same group is used for the first two groups, the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group. In this way, pairings can be used to reduce a hard problem in one group to a different, usually an easier problem in another group.

3). Advantages and Limitation

The pairing on elliptic curves is applied for secure id based cryptography technique. Pairing Based Elliptic Curve Cryptosystem [4] is used to reduce the number of computations of the pairing for the verification of the id based signature and also which is used to decode the id based public key cryptosystems with authentication by factor of 2.

Elliptic Curve Cryptography (ECC) will be applied in the Vehicular Ad hoc Network (VANET).Hash function is used to verify the messages exchanged with the VANET environment. This will be helpful to achieve message authentication.

ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

Because ECC helps to establish equivalent security with lower computing power and battery resource usage, now ECC have been widely used for mobile applications.

E. Security Using RSA and Hash.

1).System Architecture

The proposed frame work [6] uses the algorithm for secure communication of messages, the algorithm are hash and RSA.

The hash key technique is used because the framework does not need a specific range. Why because the key length is fixed and larger which is defined in the RSU. The nodes are ordinary vehicles on the road that can communicate with each other and RSU's though radio. In

DOI 10.17148/IJARCCE.2015.4637

a highway scenario RSU are normally away from each other.

The following figure clearly illustrates the flow of message authentication in proposed Shared key management framework. The management framework is the intermediate between the system information and the groups, system information gives the necessary information above the three aspects which are covered in this key management framework. The group is set of 7 RSU and 150 nodes. This technology of connection is done by RSA and hashing technology. Thus the authentication process is done by the flow as shown. In Following figure and further the group is connected for the performance evolution.

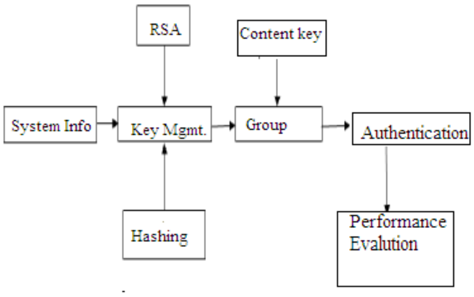


Fig: RSA and Hash

2). Advantages and Limitation

1. The key components of this proposed Shared key management framework [6] is to connect the RSU by group key distribution and cooperative message authentication for the safe communication.

2. This framework uses the data encryption and also client authentication for which the centralized server may not be required. Since the keys are distributed each key can communicated among them by cooperative message authentication and does not required the group authentication.

3. There is no necessity for extra protocol for the authentication beyond the range because here in this approach every participating key is given priority message authentication.

4. The centralized server is not required, since the keys are shared group authentication is not necessary for transferring the information because the key them self will shared the information separate protocols is not needed to send and receive message out of the range because each vehicle can spread the message.

F. ECIES -Elliptic Curve Integrated Encryption Scheme

1). Introduction

The most extended encryption and decryption scheme based on ECC is called the Elliptic Curve Integrated Encryption Scheme (ECIES) [7]. This scheme is a variant of the ElGamal scheme proposed by Abdalla, Bellare, and Rogaway. The different versions of ECIES can be found at ANSI X9.63, IEEE 1363a, ISO/IEC 18033-2 and SEC 1 standards. ECIES is an integrated encryption scheme which uses the following functions:

1. Key Agreement (KA): This Function is used for the generation of a shared secret key by two parties.

2. Key Derivation Function (KDF): This is the Mechanism which is used to produces a set of keys from keying material and some optional parameters.

3. Encryption (ENC): Symmetric encryption algorithm.

4. Message Authentication Code (MAC): Data used in order to authenticate messages.

5. Hash (HASH): Digest function, used within the KDF and the MAC functions.

Here, we assume that **User A** want to send some message to **User B** over the network. In this case first, we assume that private and public keys of User **A'** is represented as u and U, respectively. Similarly, we will refer to **User B**'s private and public keys as v and V, respectively.
In ECC, private keys are elements of the finite field, either GF(p) or GF(2m), on the other hand public keys are points belonging to the elliptic curve and calculated as the product of the private key and the generator G of the elliptic curve.

- **Steps to be followed for Encryption by User A:**

1) **User A** must create key pair consisting in the finite field element u and the elliptic curve point U=u·G. That key pair should be generated pseudo-randomly exclusively for the current process.

2) After the keys u and U are generated, **User A** will use the Key Agreement function, KA, in order to create a shared secret value, which is the result of the escalar multiplication u·V,.

3) Then, **User A** must take the shared secret value u·V and optionally other parameters such as the binary representation of public key U, as input data for the Key Derivation Function, KDF. This function gives us the concatenation of the symmetric encryption key, kENC, and the MAC key, kMAC.

4) Now with the element kENC and the clear message, m, **User A** will use the symmetric encryption algorithm, ENC, in order to produce the encrypted message, c i.e Ciphertext.

5) Taking the encrypted message c, kMAC and optionally other parameters, such as a text string previously agreed by both parties, **User A** must use the selected MAC function in order to produce a tag.

6) Finally, **User A** will take the temporary public key U, the tag, and the encrypted message c, and will send the cryptogram (U||tag||c) consisting of those three concatenated elements to **User B**.

- **Steps to be followed for Encryption by User B:**

1) After receiving the cryptogram (U||tag||c) from **User A, User B** must retrieve the public key U, the tag, and the encrypted message c, so he can deal with those elements separately.

2) Using the retrieved public key, U, and his own private key, v, **User B** will multiply both elements in order to produce the shared secret value v·U, as the result of this computation is the same that the product u·V.

DOI 10.17148/IJARCCE.2015.4637

3) Taking as input the shared secret value v·U and the same optional parameters that **User A** used, **User B** must produce the same encryption and MAC keys by means of the KDF procedure.

4) With the MAC key kMAC, the encrypted message c, and the same optional parameters used by **User A**, **User B** will first compute the element tag*, and then he will compare its value with the tag that he received as part of the cryptogram.
If the values are different, **User B** must reject the cryptogram due to a failure in MAC verification procedure.

5) If the tag value generated by **User B** is the correct one, then he will continue the process by deciphering the encrypted message c using the symmetric ENC algorithm and kENC. At the end of the decryption process, **User B** will be able to access the plaintext that **User A** intended to send to **User B.**

2). Advantages and Limitation

ECIES [7] is the best known encryption scheme in the scope of ECC, which is one of the most interesting current cryptographic trends. Even though ECIES provides some valuable advantages over other cryptosystems as RSA, the number of slightly different versions of ECIES included in the standards may obstruct the adoption of ECIES.
It is not possible to implement a software version compatible with all those standards, regarding both the specific operations and the list of allowed functions and algorithms.
Implementations may face another important problem, which is the limitation in the functions available to the developer in the application programming interface of the target device such as PCs, smart cards, mobile phones, etc.

G. Comparison between Elliptical Curve cryptography and RSA

In RSA, encryption and decryption time is dependent on the key length. If we increasing the key length, the it strongly affects the decoding time. Therefore RSA is not sufficient for encrypting long messages.
On the other hand, ECC provides similar functionality to RSA. ECC requires less computing power and memory and it has smaller keys (better performance) compared with RSA for longer messages.
The sizes of selected key pairs are shorter for the ECC than RSA. RSA have a long length and it consumes a lot of time, which is not applicable and sufficient for VANETs. Each public key method can either encrypt session key, or it is used for signing a short message such as message digest (signature application). For public key encryption and signature generation, we can use both ECC and RSA methods. ECIES-224 and RSA-2048 they have the same security levels. Increasing the keys length in RSA method has a huge effect than ECIES, on decryption time. It means for short messages that need to keys less than 1024 bits in RSA, using RSA is effective for processing time and for longer messages we should use ECIES method for increasing performance and scalability in the VANET-.

III.CONCLUSION

Vehicular networks such as VANET provide many useful applications for avoiding dangerous crashes; it gives warning message to the driver about weather conditions, road congestion, traffic, and other hazardous driving conditions. With VANET we can efficiently perform traffic management and increase the safety while driving. In order to take full advantage of this network, the communications must be secured with all of security requirements. Many attacks in this network can be prevented or detected using cryptography methods. Due to the high speed of vehicles, they have limited opportunities to communicate with each other. So the response time for selected encryption method must be minimal and the security level must be acceptable considering the key lifetime.
This paper describes various asymmetric encryption algorithms such as RSA, ECC in details with their advantages and limitation. From the comparison between RSA and ECC we can say that if messages are too short, RSA at 1024 bits, consumes less time with a high security level, otherwise ECIES is the best choice.

REFERENCES

[1]. T.W. Chim, S.M. Yiu, Lucas C.K. Hui, " VSPN: VANET-Based Secure and Privacy-Preserving Navigation " IEEE Transactions On Computers, Vol. 63, No. 2, February 2014.
[2]. M. Alimohammadi, and A. A. Pouyan, "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET", International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014.
[3]. Karamjeet Singh, Chakshu Goel , "Using MD5 AND RSA Algorithm Improve Security in MANETs Systems ", International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue 2 (June 2014)
[4]. T.Punitha1,M.Sindhu , "Pairing Based Elliptic Curve Cryptosystem for Message Authentication ",International Journal For Trends In Engineering & Technology Volume 3 Issue 3 – March 2015 ,pages-87-90.
[5]. V.Vijayalakshmi, S.Saranya, M.Sathya, C.Selvaroopini, "A Novel Mechanism for Secure and Efficient VANET Communication ",International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 3– Mar 2014
[6]. G.Sasikala K.S. Dhanalakshmi ,"Key Management Techniques for VANETs ", Special Issue of International Journal of Computer Applications (0975 – 8887) on International Conference on Electronics, Communication and Information Systems (ICECI 12) pages 13-16 .
[7]. V. G. Martínez, L. H. Encinas, and C. S. Ávila,"A Survey of the Elliptic Curve Integrated Encryption Scheme", Journal Computer Science & Engineering, vol. 2, no. 2, August 2010.
[8]. N. Jansma and B. Arredondo, "Performance Comparison of Elliptic Curve and RSA Digital Signatures" Technical Report, University of Michigan College of Engineering, 2004 .
[9]. L. Delgrossi, & T. Zhang, Cryptographic Mechanisms. Vehicle Safety Communications: Protocols, Security, and Privacy, John Wiley & Sons, Inc., Hoboken, NJ, USA, pp. 167-208, 2012.
[10]. Kristin Lauter, Microsoft Corporation "The Advantages Of Elliptic Curve Cryptography For Wireless Security ",IEEE Wireless Communications February 2004,pages-62-67.
[11]. Prachi B. Danak Prof. M. D. Sabir, "Security & Content Distribution of Vehicular Ad-Hoc Network ", International Journal of Engineering Research & Technology (IJERT) ,Vol. 3 Issue 5, May – 2014 ,pages-131-135.

DOI 10.17148/IJARCCE.2015.4637