International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Analysis of RSA Cryptosystem to Secure Messages in Vehicular Adhoc Network

[1]Rajesh D. Thakare, [2]Yogesh Suryawanshi, [3]Sachin Jain, [4]Arvind R. Bhagat Patil, [5] Prasheel Thakre, [6]Nitin Marotrao Chore

Submitted: 20/10/2023 **Revised**: 25/11/2023 **Accepted**: 03/12/2023

Abstract: Due to increasing rate of accidents as per World Health Organisation, it is required to provide safety in Vehicals. Even if provided safety features in vehicals such as airbags, safety belts , still rate of accidents ratio not reduced. Most of accidents occurers at intersection points. If preincident information about incident received then motorist may take decision along the path . But , difficulty is that if such messages are not secured among vehicals in network then attacker may broadcast wrong information in network for personal benefits or for just fun which may be life threatning to other users in network as other users decisions in network depends only on messages received.

Hence, Security of such Network is important. In this paper, tried to analyse the performance of RSA Cryptographic algorithms in terms of Delay. i. e. time required to generate keys , time requird for signature Generation & Signature Verification . Finally conclude wheather RSA cryptosystem is suitable for Vehicular adhoc network Communication or Not.

Keywords: *Public Key Management system, VANET .*

1. Introduction

VANET is Vehicular Adhoc Network in which each vehicle will act as node, which will transmit as well as receive message. In VANET, Roadside units also acts as Transmitter-Receiver Section. Base Station will broadcast messages in its covering Range of Vehicles Network. VANET main aim is to provide safety related messages such as traffic information , internet services shown in figure 1.

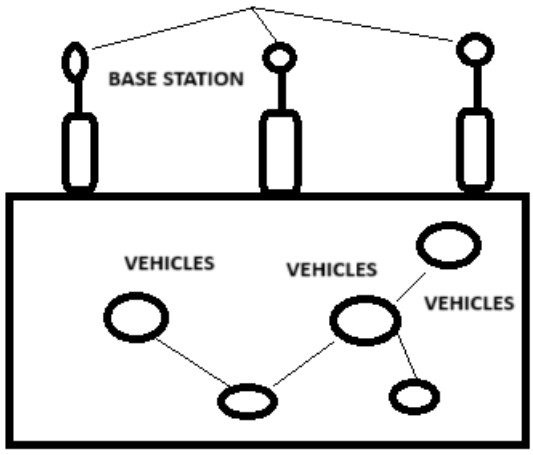


Fig 1 Vehicle Infrastructure

Safety related messages which will be broadcast in network must be secured. User decision totally depends only on received messages. If wrong information received by user which will be life threatening to user or to other nodes in network . Hence Security of such system is important. With the help of Symmetric or asymmetric key cryptosystem , security of safety related message can be provide.

Issues while Providing Security in VANET

1. As per Dedicated Short Range Communication, Each message must be process in $1X10^{-9}$ seconds as DSRC operated at 5.9 GHZ frequency

2. In Symmetric Key Cryptosystem , Sender and receiver use same key to encrypt aw well as to decrypt messages.

[1]*Professor Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering,*
Nagpur, India
rdt2909@gmail.com
[2]*Assistant Professor, Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering,*
Nagpur, India
yogesh_surya8@rediffmail.com
[3]*Assistant Professor, Department of Computer Science Oklahoma State University*
Stillwater, (United States).
[4]*Associate Professor, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India*
Nagpur, India
arbhagatpatil@gmail.com
[5]*Assistant Professor, Electronics and Communication Engineering Shri Ramdeobaba College of Engineering and Management, Nagpur*
thakrepn2@rknec.edu
[6]*Assistant Professor, Electronics and Communication Engineering Tulsiramji Gaikwad Patil College of Engineering and Technology Mohgoan Nagpur*
nitinmchore@gmail.com

If this key track by attacker then unauthorized user of system may take control of system and then may broadcast wrong information in network.

3. Routing Protocol , Speed of Vehicles , Broadcasting Range, availability of network range, are also an issues in Vehicular Adhoc Network.

From above issues, it is conclude that the VANET is vast area of research in which need to work on each aspect like routing protocol, Range of Node and also cryptosystem to secure messages in network.

In this Paper, Cryptographic Algorithm is taken as challenging task and with the help of this algorithm , tried to provide Solution.

2. Objectives

To Make Key management system flexible

To increase the throughput of the system

To reduce overheads

These objectives can be achieved by using appropriate algorithms and routing protocols

3. Related Work

After key management techniques have been employed there is considerable improvement in the data communication between the nodes [1]

The related protocol and the proposed security architecture has shown to what extent and how it protects privacy[2]

Both security concerns and the requirement of the potential VANET application are taken into account in a proposed secured and application oriented network design framework [3].

Presented Temporary Anonymous Certified Keys (tacks) as an efficient way to fulfill the Security and Privacy Properties Necessary for Key Management in Vehicular Ad Hoc Networks (vanets). [4]

Proposed a Practical Ways of Defending Against Sybil Attack in a VANET Environment, Which Require Neither a Dedicated Vehicular Public Key Infrastructure for Individual Vehicles, nor Additional Setup, but only Basic Roadside units. [5]

For defending against sybil attack in a VANET enviornment prcatical ways are proposed which neither requires an additional setup nor dedicated vehicular public key infrastructure for individual vehicles, but only basic roadside units.

Proposed an Applicable Method for Securing Safety Message and Solve Problems Facing During Implementation [6]

Applicable methods are proposed for securing safety message and solve problems facing during implementation.

Role of Routing Protocol in VANET

If node A wish to send Message to Node B then initially Node A will broadcast “Hellow” kind of message in network .This “Hellow” message contains Node ID’s. So that , other nodes in network can get idea about their surrounding nodes in network . After reception of this message any node in network can establish communication with other nodes in network. Node A will send Request to Node B as node A wish to send Message to Node B. This request message will contains node id, sequence number , hope count etc. After received, request from Node A , node B will check whether request is for himself or for other nodes based on parameters mentioned in request message. After received request , if node B wish to establish communication with node A then node B will send reply to Node A. After received Reply from Node B , Node A will start to send messages to node B in network as shown in figure 2.

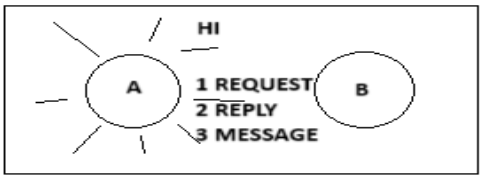


Fig 2 Communication Establishment in Adhoc Network

If Attacker is listening their communication then may easily hack such system that I am active member of network and have shortest path and fresh route to destination.

With the help of Cryptosystem , tried to provide solution. How Symmetric and Assymetric Key Cryptographic algorithms will works that have explained with the help of following figures.

Symmetric Key Cryptography Algorithm :

If Node A wish to send message to Node B in network. First Node A will Encrypt Hello message with the help of Symmetric Key Cryptographic based Algorithm by using Secrete key. Node B will decrypt this Hello message using the same secrete key . Node B will confirm that the message received from authorized source . Only authorized nodes in network will have this secured key provided by key management system . Hence , only authorized nodes in network can read messages. But, Difficulty in this mechanism is that Attacker may easily get this secrete key which have explained with figure 3 .

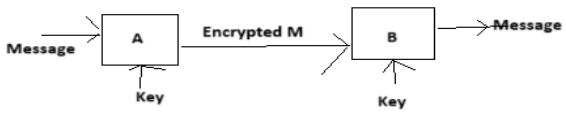


Fig 3. Assymetric Key Algorithm

After received number of messages , attacker can use currently available Symmetric Cryptographic based algorithms like AES or DES and will try to apply different keys to decrypt message and at which key Attacker will get meaningful message, attacker will get that secrete key . once attacker get the key then attacker can easily control the system.

Solution to Existing System

With the help of Asymmetric Key Cryptography Algorithm ,have tried to provide solution. Here, have considerd Asymmetric Key Cryptography Algorithm i .e. RSA Cryptographic Algorithm. How RSA cryptosystem will work in vehicular adhoc network that have explained.

If Node A wish to send messages to node B then node A will first broadcast hello message in network by encrypting with the help of Private key provided to node A. After received hello message , node B will decrypt the message with the help of public key available to node B. Only authorized nodes in network will have these two keys Public key and Private Key. By using Private Key , any node in network can encrypt messages and by using Public Key any nodes in network can decrypt messages. Using Assymetric key Cryptographic Algorithm, its becomes difficult for attacker to get that private key as each nodes in network will have different private keys .Hence, in this paper have studied Assymetric key Cryptographic Algorithm i.e. RSA Algorithm and have analyzed its performance in terms of time require for Key Generation, time require for Signature Generation and Verification.

RSA Algorithm

RSA (Rivest- Shamir-Adleman) is an algorithm used to encrypt and decrypt messages. This Algorithm developed by three authors Rivest- Shamir-Adleman . That's why name of this algorithm is RSA. It is Asymmetric Cryptographic algorithm. In Asymmetric Cryptographic algorithm , we use public key and Private Key for encryption and decryption. So, both sender and receiver use private key and public key for encryption and decryption.

Encryption

$X = Y^e \bmod n$, where Y is original message and X is encrypted message. e is public key and n is product of two large prime numbers.

Decryption

$Y = X^d \bmod n$ where Y is original message and X is encrypted message. e is public key and n is product of two large prime numbers.

Key Generation Algorithm in RSA Cryptosystem

First will select two large prime numbers a and b.

Secondly will calculate n= a X b and then will calculate Eulers Function i.e. $\theta(n)= (a-1) X (b-1)$.

In Next step, will choose a small number e, coprime to $\theta(n)$ with $GCD(\theta(n), e) = 1$ and $1 < e < \theta(n)$.

In last step , will find d , such that $d \times e \bmod \theta(n) =1$.

Let us see example for key Generation Algorithm.

First consider two prime numbers p=3 , q=5

Then calculate n = p X q therefore n = 3 X 5 =15.

$\theta(n) = (p-1) (q-1)$

$\theta(n)= (3-1) (5-1)$

$\theta(n) =8$

Assume e such that $gcd (e,\theta(n)) =1$ and $GCD(\theta(n), e) = 1$ and $1 < e < \theta(n)$.

gcd (3,8) =1

gcd (5,8) =1

gcd (7,8) =1

Out of these three , can select any one value which will satisfy the condition $GCD(\theta(n), e) = 1$ and $1 < e < \theta(n)$.

Therefore e =3 is selected.

Now, in last step calculated d.

$d \times e \bmod \theta(n) =1$

$d \times e \bmod 8 = 1$

Consider d =3

Therefore

$3 \times 3 \bmod 8 = 1$

$9 \bmod 8 = 1$

Therefore

d = 3

Now we have public key = {e,n} = {3,15}

Private Key = {d,n} = {3,15}

After Calculated Public and Private Key , tried to encrypt and decrypt messages.

Encryption

$X = Y^e \bmod n$

Suppose Y = 8 (original message)

$X = 83 \bmod 15$

X= 2 (Encrypted Message)

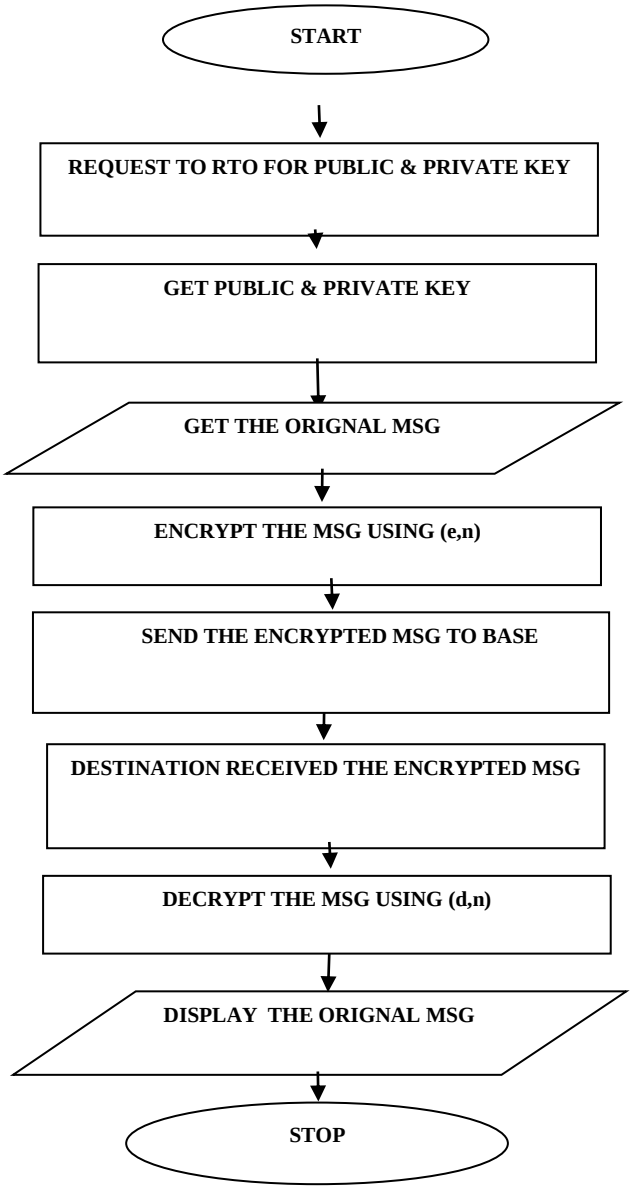
Decryption

$Y= X^d \bmod n$

$Y= 23 \bmod 15$

Y = 8 (original Message)

Use of RSA Cryptography Algorithm in VANET



4. Result Analysis

In tabular form have represented some simulated results of RSA cryptography Algorithm for 1028 ,2048 and 4096 key length and Calculated time required for key generation , Signature generation and Signature Verification in 10^{-9} seconds.

RSA 1024 Key Length

256R p4 2.8Ghz	1024
e	3
p	65380725939414761705852595117 33365414213441424081803846910 3932472260901245076191 89673752276652886189517360257 78723053906837161677149470805 02491432169079
q	69753739842748268836081639629 16622088282533527946320278776 120949407422174183 1547 13626263564383759643597152476 42579709509100138110367838583 2861559015126527
phi	45605501479079607014653245970 98219011085876191320989817220 119565798521307749 0239 11026314001067015676419267439 81730995741236168446416507087 6715133853325682640291 94228914561398898825190925937 99434021928489911301501622761 6260004360217380362767 41946923226645166862708469212 09071177090791613560843860847 94763028
m	12345678909876543210123456789 09876543210123456789098765432 101234567890 9876543210 12345678909876543210123456789 09876543210123456789098765432 101234567890 9876543210 12345678909876543210123456789 09876543210123456789098765432 101234567890 9876543210
Message encrypted	15273916995936178735607493695 00840113194490207488208458480 74517473635179471 47238 37059996706625074978379753261 68015793532920611142322008288 403981423273847561 4454 79816232671772886897269860379 48085009129877732178415953633 129822967585758022 4043 06841908113837719807655685163 29006859291413238470160713273 8386243
signature generation time	0
decrypted msg	12345678909876543210123456789 09876543210123456789098765432 101234567890 9876543210 12345678909876543210123456789 09876543210123456789098765432 101234567890 9876543210

	123456789098765432101234567890 0987654321012345678909876543210 1012345678909876543210
signature verification time	47
Message signed	152739169959361787356074936950 0840113194490207488208458480 745174736351794714723 8 37059996706625074978379753261 68015793532920611142322008288 4039814232738475614454 79816232671772886897269860379 48085009129877732178415953633 1298229675857580224043 06841908113837719807655685163 29006859291413238470160713273 8386243
sign time	47
verify time	0
Original message back, verified:	12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210 12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210 12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210
Message signed and encrypted,	14367793390310734815712597946 28738203321905078300220039460 0108636941711485518628 86710028936661006188019597423 79891551785970635730521918752 5788728433112277685336 82255467600709353550748484737 65886920538139017116511383488 9324853508230893824428 06067004339471877900751263242 74747628109009426909660571994 9918958058
sign and encypt time	46

Original message back, verified and decrypted,	12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210 12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210 12345678909876543210123456789 09876543210123456789098765432 1012345678909876543210
decrypt and verify time	47

Table 1 RSA 1024 256R P4 2.8Ghz

512 P4 2.8Ghz	1024
e	3
p	2117721817371107221459918814 8657408835062452971855259293 083427605161166018310137 8591532058161068643583008885 1141550252373703161486052104 509087534977339278061
q	3262368513127156944741311916 4836396711818489776216520691 905034150122521298405532 3206122018355210301554178849 2072841697332047144073358988 2821092828248583
phi	6908788976553919671346685560 3460357365438837401560752277 634297638986247206190455 2732762333253976150192503075 35222773791318642603151353113 211812197766417568044971 9107551866764256538735409214 3842065147429274280770076571 613100641889453808994064 5550824546617034993012566406 5075235389840103171010277500 706098710920
m	1234567890987654321012345678 9098765432101234567890987654 321012345678909876543210 1234567890987654321012345678 9098765432101234567890987654 321012345678909876543210 1234567890987654321012345678 9098765432101234567890987654

	321012345678909876543210
Message encrypted	445835960344509253764761564946244262877331313805447419091855610101795817574060593886682778481004304563341102690831509692937201046421305240990206911286515029248379073272544557563893390479266960654429765914751423032438340610742929940896857173115748876858671579927944678659336591415664513025447804251666702724405183596034450925376476156494624426287733131380544741909185561010179581757406059388668277848100430456334110269083150969293720104642130524099020691128651502924837907327254455756389339047926696065442976591475142303243834061074292994089685717311574887685867157992794467865933659141566451302544780425166670272440
signature generation time	0
decrypted msg	123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210
signature verification time	47
Message signed	445835960344509253764761564946244262877331313805447419091855610101795817574060593886682778481004304563341102690831509692937201046421305240990206911286515029248379073272544557563893390479266960654429765914751423032438340610742929940896857173115748876858671579927944678659336591415664513025447804251666702724405183596034450925376476156494624426287733131380544741909185561010179581757406059388668277848100430456334110269083150969293720104642130524099020691128651502924837907327254455756389339047926696065442976591475142303243834061074292994089685717311574887685867157992794467865933659141566451302544780425166670272440
sign time	47
verify time	0
Original message back, verified:	123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210

	123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210
Message signed and encrypted,	393064363077073694620193280473545453175363281659276379522661515548282581520603659776174601621637418515750828560679502222055418718324549826681652592715767364342681856130560534226424848158880266930740932256269117169799476655926157331527485557746526685546202352809091987495821272165766151666109692553377886219504717
sign and encypt time	47
Original message back, verified and decrypted,	123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210
decrypt and verify time	47

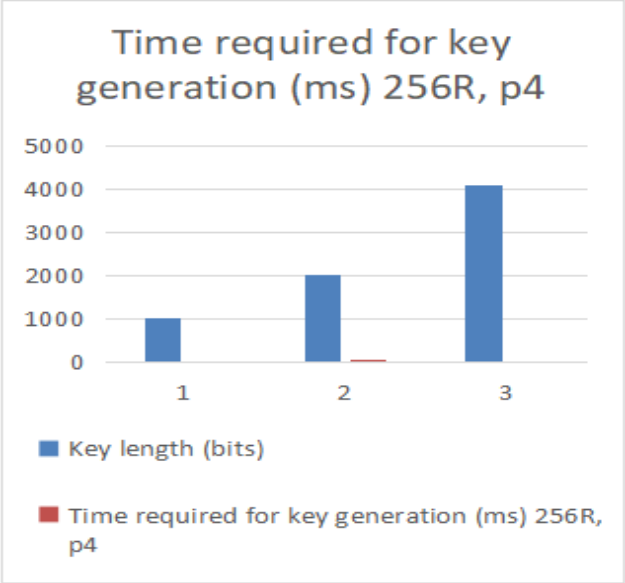
Table 2 RSA 1024 for 512R p4 2.8 Ghz

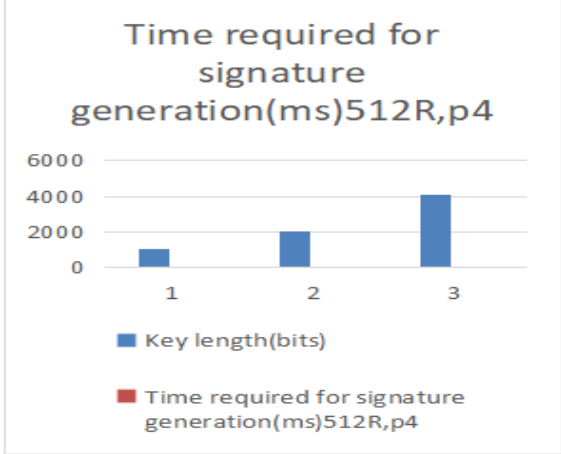
Verification and Testing of Algorithms

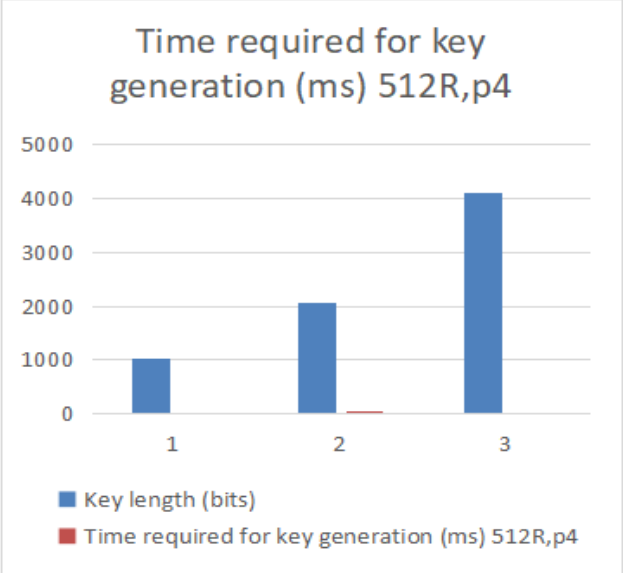
TABLE 3 RSA ALGORITHM ANALYSIS

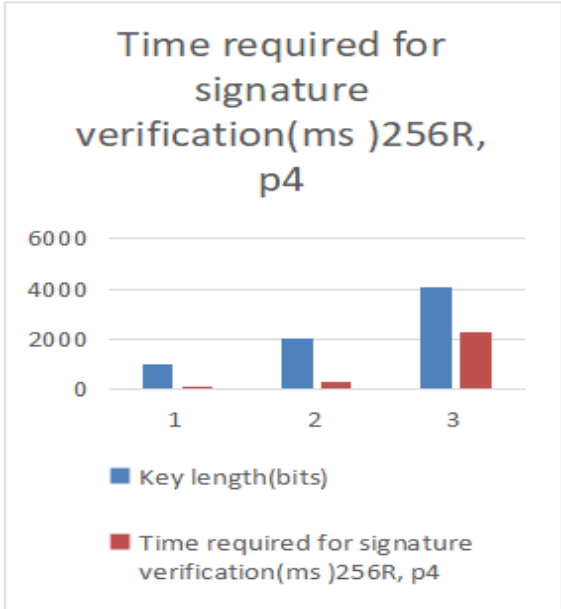
S.N	Key length (bits)	Time required for key generation (ms)		Time required for signature generation (ms))		Time required for signature verification (ms)	
		256R, p4	512R,p4	256R, p4	512R,p4	256R, p4	512R,p4
1	1024	0	32	0	0	47	47
2	2048	16	16	0	16	297	297
3	4096	47	32	0	0	2297	2297

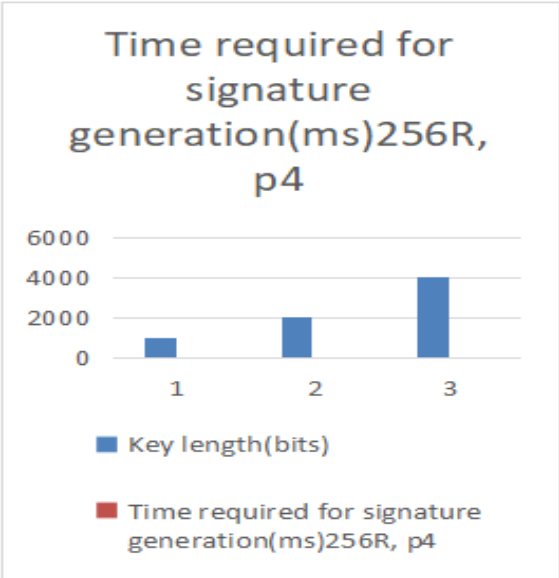
Graphical Analysis

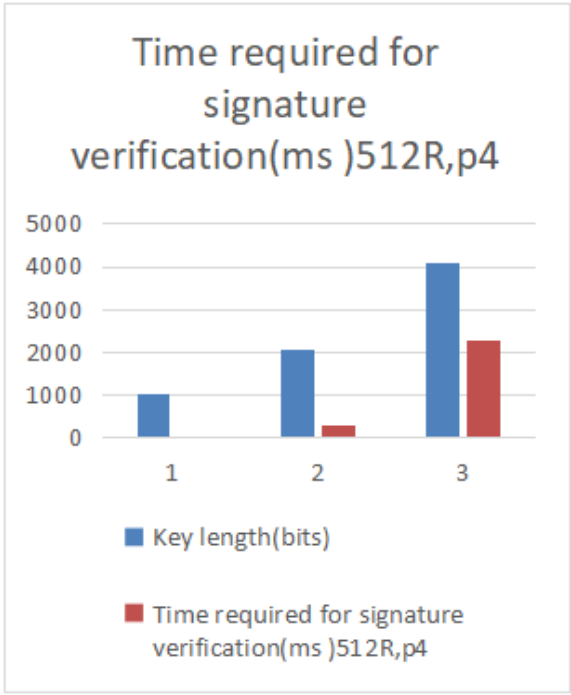












5. Conclusion

After implementing RSA algorithm , it has been observed that the time required for signature verification for 1024, 2048, 4096 bits respectively is on higher side

References

[1] Sasikumar p , Vivek c , Jayakrishnan p.,"Key-Management Systems in Vehicular Ad-hoc Networks", in international journal of computer applications (0975 – 8887) volume 10– no.1, november 2010.

[2] Yogesh A. Suryawanshi , Avichal Kapur,"Security and Privacy Preservation in Vanet", international journal of information technology and knowledge management january-june 2011, volume 4, no. 1, pp. 125-128

[3] Yi Qian , and Nader Moayeri, "Design Secure and Application-Oriented Vanet" , National Institute of Standards and Technology 100 bureau drive, stop 8920 gaithersburg, md 20899-8920, USA

[4] Ahren Studer, Elaine Shi, Fan Bai, & Adrian Perrig, "Tacking Together Efficient Authentication, Revocation, and Privacy in Vanets", carnegie Mellon university general motors

[5] Soyoung Park, Baber Aslam, Damla Turgut, Cliff C. Zou, "Defense Against Sybil Attack in Vehicular Ad hoc Network Based on Roadside Unit Support",School of Electrical Engineering and Computer Science University of Central Florida 4000 Central Florida Blvd. Orlando, FL 32816-2362

[6] Nasser Mozayani, Maryam Barzegar, Hoda madani, "Strategies for Securing Safety Messages with Fixed Key Infrastructure in Vehicular Network" , world academy of science, engineering and technology 48 2008

[7] M. Raya and j.-p. Hubaux, "Securing Vehicular Ad hoc Networks", j. Computer security, special issue on security, ad hoc and sensor networks, vol. 15, no. 1, 2007

[8] X. lin, r. lu, c. zhang, h. zhu, p.h. ho, and x. shen,"Security in Vehicular Ad hoc Networks", ieee communications magazine, vol. 46, no. 4, 88-95, 2008

[9] A Stampoulis and Z chai, "a survey of security in vehicular networks" yale university

[10] Abedi, o, Fathy, m, and Taghiloo, j "Enhancing Aodv Routing Protocol Using Mobility Parameters in Vanet", computer systems and applications, 2008

[11] S. D. Ram churn, D. Huynh, and N. R. Jennings, "Trust in Multi-agent Systems", the knowledge engineering review, vol. 19, no. 1, pp. 1–25, 2004.

[12] Behrouz A. Forouzan, "Data Communications and Networking", Tata McGraw Hill Education Private Limited, 4th Edition.

[13] Coron Jean-Sebastien and Weger Benne de, "Hardness of the Main Computational Problems Used in Cryptography", Information Society, 2007.

[14] Dan Calloway, "Introduction to Cryptography and its role in Network Security Principles and Practices", 2009, available at http://www.dancalloway.com/.

[15] David M. Burton, "Elementary Number Theory", University of Hampshire, Universal Book Stall, New Delhi, 2nd Edition.

[16] Hinek M. J., "Another look at small RSA exponents", Springer, New York, 2006, pp. 82–98.

[17] Hinek M. Jason., "On the Security of Some Variants of RSA", Waterloo, Ontario, Canada : s.n., 2007.

[18] Kaliski Burt, "The Mathematics of the RSA Public-Key Cryptosystem", RSA , Laborataries.

[19] Ou Huayin and Wei Baodian, "Multi-factor Rebalanced RSA-CRT Encryption Schemes", IEEE, 2009.

[20] Peng Jiezhao and Wu Qi, Research and Implementation of RSA Algorithm in Java", IEEE, 2008.

[21] RSA Laboratories, "Why RSA?", available at http://www.rsa.com/rsalabs/node.asp?id= 2222 and http://www.rsa.com/rsalabs/node.asp?id=2223.

[22] Shen Guicheng, Liu, Bingwu and Zheng, Xuefeng, "Research on Fast Implementation of RSA with Java", International Symposium on Web Information Systems and Applications (WISA'09), Acadaemy Publisher,Nanchang, China, 2009, pp. 186-189.

[23] Shoup Victor, "Why Chosen Ciphertext Security Matters", IBM Research Division, 2005.

[24] Stallings William, "Cryptography and Network Security - Principles and Practices". India : Pearson Prentice Hall, 4th Edition.

[25] Sun H., "Dual RSA and its Security Analysis", IEEE Transactions on Information Theory, 2007, pp. 2922-2933.

[26] Sun H.-M. and C.-T. Yang, “RSA with balanced short exponents and its application to entity authentication in Public Key Cryptology”, Springer, NewYork, 2005, pp. 199–215.

[27] Sun H.-M. and Wu M.-E., “An approach towards Rebalanced RSA-CRT with short public exponent Cryptology”, s.l. : ePrint Archive, 2005.

[28] Xie Jianquan, “A practical method for generating big primes quickly”, Information Security and Communication Secrecy, 2006, pp. 56-58.

[29] Yang Shuqun, “An algorithm for generating strong primes”, Science and Technology Square, 2006, pp. 74-75.

[30] Yingxiong Xiao and Shaohua Zhang, “The Determination and Generation of a kind of Strong Primes”, Science and Technology Square, 2006, pp. 74-75.

[31] Zheng Ziwei and Li Cuihua, “Realization of Class-Based RSA System”, Journal of Huaqiao University (Natural Science), 2003.