Upgrade of GSM Security Using Elliptic Curve Cryptography Algorithm

M. S. N. G. K. Mounika, Arvind Yadav, S. Lokesh Anand, P. Satyannarayana

Abstract**: *As of late, the versatile business has practiced an outrageous rise in the total of its users. The Global system for mobile organize with the best overall number of users capitulates to a large number of safety susceptibilities. Safekeeping is a consuming and clever problem. It will dependably stay constant for what it's worth imperative in an extremely wide range of uses. Global system for mobile Security defects have been distinguished quite a long while back. A portion of these blemishes have been fixed however others are left to discourse. The vast majority of the RSA– kind equipment and program writing items furthermore, models require enormous key size for higher safekeeping level. In this research work we will concentrate about the inspection of functioning practice on RSA's algorithm and ECC calculation in system of Global System for Mobile to how it's a higher promise for a quicker and progressively protected technique for encryption in correlation to the present benchmarks in the open key cryptographic calculations of RSA cryptographic technique.***

Index Terms**: *Cryptography, ECC, Public- Key, Global System for Mobile.***

I. INTRODUCTION

Cell phones are utilized once a day by many a large number of clients, over different connections like radio. Fixed telephones offer only some dimension of security for example physical access is expected to the telephone line for tuning in. Not at all like a stable telephone, with a radio connection, anybody with a collector which can inactively screen the wireless transmissions. In this way it is exceedingly critical that sensible innovative safety efforts are taken to surety the protection of client's telephone calls and instant messages too to avoid unapproved use of the administration. Global system mobile is the nine hundred MHz radio framework utilizing a typical overall standard. The framework use by PCN (DCS eighteen hundred) is in fact indistinguishable, with the exception of the recurrence. GSM was intended to develop and meet the necessities of new innovations. GSM is as of now made out of various newly developed and updated technologies. Every individual from the family is intended to tackle a specific need. Enhanced data rates of GSM evolution is an upper level part utilized for cutting edge versatile administrations such as downloading music cuts, video clasps, and sight and sound messages. General packet radio services is intended for "dependably on" frameworks that are required for web-perusing. 3GSM is the Global system for mobile running on third era norms for sight and sound administrations. It permits full wandering from administrator to administrator if common reciprocal understandings are set up. Be that as it may, being the web an exposed and undependable system, some anxiety has been brought up in communicating touchy data. The arrangement works by utilizing the cryptography technique and various authentication conventions that ensure the secrecy, authentication and uprightness of interchanges. Such conventions, as secure socket layer and secure electronic transaction, as of now occur and they are broadly utilized in current internet business applications. A large portion of them are situated in RSA open key cryptography. A convention is created which depends solely on ECC a lopsided cryptography that performs well in asset bound stages and keep up the most safekeeping range which one can accomplish with the agreements being used today.

This research paper emphases on the downsides of calculation of R.L. Rivest, A. Shamir and L. Adleman and why ECC calculation is wanted instead of RSA.

II. LITERATURE SURVEY

GSM is a versatile correspondence modem, it is represents worldwide framework for portable correspondence (GSM). The possibility of GSM was created at Bell Laboratories in 1970. It is generally utilized portable correspondence framework on the planet. GSM is an open and advanced cell innovation utilized for transmitting versatile voice and information administrations works at the 850MHz, 900MHz, 1800MHz and 1900MHz recurrence groups.

General System for Mobile Communications, GSM, is a propelled cell phone framework utilized far and wide. Global system for mobile has numerous advantages over its forerunners as far as security, limit, lucidity, and region inclusion. Global system for mobile expects to give a safe association with correspondence. Since its coming in the middle of nineteen eighties it has established into a group of organizations to give everything from transportable voice to multipurpose material. The most ideal approach to recognize safekeeping is by taking a glimpse at how tumultuous and perilous a portable interchanges assembly would be without safekeeping. At some random minute, anyone could listen in into your discussion. Your financial balance data, day by day plan, and some other data you may unveil on the telephone would be in danger. Other than tuning in, at some random minute, a programmer could imitate your client data to make calls that would later add up to a great many dollars in administration charges. The rundown continues endlessly. Global system mobile was intended to address security issues like those recorded previously. The security techniques institutionalized for the Global system mobile (GSM) System make it the most secure cell media communications standard as of now accessible. In spite of the fact

Revised Manuscript Received on May 06, 2019

M. S. N. G. K. Mounika, Electronics and Computer Science, Koneru Lakshmaiah University, Vaddeswaram, India.

Arvind Yadav, Assistant Professor, Electronics and Computer Science, Koneru Lakshmaiah University, Vaddeswaram, India.

S. Lokesh Anand, Electronics and Computer Science, Koneru Lakshmaiah University, Vaddeswaram, India.

Dr. Penke Satyannarayana, Professor, Electronics and Computer Science, Koneru Lakshmaiah University, Vaddeswaram, India.

that the secrecy of a call and obscurity of the Global System Mobile - GSM supporter is just ensured on the radio set channel, this is a noteworthy advance in achieving start to finish safekeeping. The supporter's anonymity is guaranteed using impermanent recognizable proof numbers. The classification of the correspondence itself on the radio set connection is performed by the utilization of encryption calculations and recurrence bouncing which must be accredited utilizing high-tech outlines and flagging. The security engineering of Global system mobile was initially planned to give security administrations, for example, secrecy, validation and classification of client information and flagging data.

The security objectives of Global system mobile are as per the following:

- Validation of portable clients for the system,
- Secrecy of client information and flagging data,
- Inconspicuousness of supporter's character,
- Manipulating 'Subscriber Identity Module' as a safekeeping module.
- Every key is securely put away.

A. Present works on Global system mobile on security with RSA algorithm.

"R.L. Rivest, A. Shamir and L. Adleman" which in short known as RSA is invented in nineteen seventy eight. As it is an open key we need to give more protection to our system. As it is in public the attackers automatically increase in the number as it is open to them. The maker keeps that learning mystery which is the isolated key and distributes the riddle which is general society key. Generally open key comprises of the 'mod n' and encryption or open exponential 'e'. The isolated key comprises of the 'mod n' and the decoding or private exponential 'd' which must and should be kept as a secret. Encryption and decoding are implemented by indistinguishable secluded exponential activities utilizing an open and secluded key match. The info Y is spoken to as a grouping of whole numbers in the collection of (0) to (A – 1) and afterward we have to increase it to the E^{th} control mod A. This is a task can be processed by repeated particular increases and squares utilizing the r-l double practice. It is improved for speed by enabling augmentations and squares to be performed in corresponding. The information sources are at first changed over to the Montgomery space. Each piece of the example is then filtered from directly to left and an augmentation performed if the bit is one. A squaring is performed on each progression of the emphasis. Toward the finish of every exponentiation, the yield J is charted back to typical portrayal.

$$[J = (Y)*(E \ (\mathrm{mod}\ A))]$$

Every element makes a RSA open Key and comparing isolated Key. Every element needs to choose two huge prime digits also, will make open key and isolated or private key. The chosen two prime digits ought to be substantial and of same magnitude. At that point we will compute their item and pick an irregular digit. This irregular digit and the item will be the open key. Process a one of a kind digit utilizing Extended Euclidean Algorithm. This digit and the irregular number ought to be harmonious to modulo result of prime digits. This special digit will be the private key.

- **Encryption of a message using RSA**

X communicates its open key (a and b) to Y and keeps the private key mystery. K at that point wishes to send message 'Msg' to L. K first transforms 'Msg' into a number g < a by utilizing a settled upon reversible convention known as a cushioning conspire. K at that point registers the figure content r relating to:

$$r = g*b \bmod a*r$$

This should be possible rapidly utilizing the technique for exponentiation by squaring. K at that point transmits c to L.

- **Decryption of a message**

L can recuperate m from c by utilizing its secluded key d in the accompanying system

$$g = r{}^\wedge d \bmod a$$

Given m, L can recoup the first message 'Msg'. The unscrambling system fills in as:

$$r{}^\wedge d \equiv (gb){}^\wedge d \equiv g{}^\wedge(bd) \pmod a .$$

RSA algorithm isn't anchor if a similar message is encoded to a few collectors, to totally break it, one needs to locate the prime elements. Practically speaking, It has ended up being very moderate, particularly for key age calculation. Moreover, it isn't appropriate for restricted conditions like cell phones and brilliant cards without its co-processors since it is difficult to actualize widespread whole digit component of math on such situations. This type of algorithm calculation encryption utilized in document of security for little records, any document with unbalanced key encryption into its content can be increasingly advantageous to impart and oversee, and it has expansive improvement prospects.

III. METHDOLOGY

A. ECC

A way to deal with open cryptography dependent on mathematical structures of elliptic curves over limited fields is ECC. Elliptic curves are characterized over a limited field given a gathering structure that is utilized to actualize the cryptographic plans. The components of the gathering normally focuses on the elliptic curve, together with an extraordinary point R. The scientific tasks of ECC is characterized over the elliptic curve**.**

$$Y^2 = X^3 + iX + j, \text{ when}$$
$$4i^3 + 27j^2 \neq 0$$

Each estimation of the 'i' and 'j' gives an alternate curve which is elliptic. All focuses [X, Y] which full-fills the above condition in addition a point at unendingness lies on the curve. The open key is a point in the curve and the secluded key is an arbitrary digit. The open key is acquired by increasing the secluded key with the generator point C in the curve. The generator point C, the curve parameters 'i' furthermore, 'j', together with couple of more constants creates the area parameter of ECC. We can utilize ECC to develop another cryptosystem. In the event that Kin needs to send a message to Liv. Initial, Kin picks an elliptic curve and a point C on it, note that both Kin and Liv should know C. At that point Kin encodes message to the point P_v on the curve. Liv pick an arbitrary number a (Liv's isolated or private key), and process a*C (L's open key), and report it. At that point Kin picks another arbitrary number k, what's more, process

$$P_v + k*(i*C) \text{ and } k*C,$$

And send

$$C= (k*C, P_v + k*i*C) \text{ to L.}$$

When Liv receives R, he can compute

$$P_v=P_v - k*i*C - i*k*Q$$

what's more, get Pm, at that point unravel Pm to the message. On account of the Elliptic curve discrete logarithm problem, it is extremely hard for aggressors to get P_v. ECC gives more elevated amount of security because of its complex numerical activity. Science utilized for ECC is extensively more troublesome and more profound than arithmetic utilized for ordinary cryptography. Actually this is the fundamental reason, why curves of curves of elliptic are so useful for cryptographic purposes, however it additionally implies that so as to execute ECC more comprehension of science is required. Given beneath is a short prologue to science behind elliptic curve cryptosystems.

B. Arithmetic behind Elliptic Curve Cryptography - ECC

Cryptographer saw that curves of elliptic acted helpfully when activities were performed with prime modulus. That implies cryptographer elliptic curve is in the structure

$$Y^2 \bmod p=(X^3+iX+j) \bmod p$$
$$\text{Where, } 4i_3+27j_2 \neq 0$$

what's more, p is a prime digit and a, b is the parameter of the curve. Here factors and coefficient are altogether confined to components of a limited field. There are two groups of elliptic bend are utilized in cryptography application:

1. Prime Curves over H_p
2. Paired Curves over CF (2^v).

In Binary curve characterized over CF (2^v), the factors and co-proficient all interpretation of qualities in CF (2^v) and in computation performed over CF (2^v).

In Prime Curve over H_p we utilize a cubic condition in which the influences and co-proficient all interpretation of qualities in the set of whole digits from 0 through [p-1] and in which computations are performed modulo p.

IV. MATH

A. Math Operation in Elliptic Curve Cryptography

The standard of scientific activity on elliptic curve is not quite the same as the standard traditional scientific tasks. In the event that we need to include two points of elliptic curve at that point we need to utilize are a few tenets which are as per the following

Principles of Addition:

Guideline 1. infinite + Infinite = infinite.
Guideline 2. (X_1, Y_1) + Infinity = (X_1, Y_1).
Guideline 3. $(X_1 , Y_1) + (X_1, - Y_1)$ = Infinity.
Guideline 4. In the event that $X_1 \neq X_2$, at that point
$(X_1 , Y_1) + (X_2 , Y_2) = (X_3 , Y_3)$.
Where
$X_3 =(\lambda_2 - X_1 - X_2) \bmod p$,
Guideline 5. (Multiplying 2 times):
On the off chance that $Y_1 \neq 0$, at that point
$(X_1 ,Y_1) + (X_1 ,Y_1) = 2(X_1 ,Y_1) = (X_3 ,Y_3)$.
Where
$X_3 = (\lambda^2 – 2X_1) \bmod p$
$Y_3 = (\lambda (X_1 - X_3) - Y_1) \bmod p$
What's more,
$\lambda = ((3X_1^2 + ai) / 2Y_1) \bmod p$.

Principle of Subtraction:

$$(X_1 , Y_1) - (X_2 ,Y_2) = (X_1 , Y_1) + (X_2 , -Y_2).$$

Principle of Multiplication:

Assume W is a point on elliptic curve W=(X , Y) .
In this manner 8*W =W+W+W+W+W+W+W+W
=2W+2W+2W+2W
=4W+4W

B. ECC - Elliptic Curve Cryptography calculation

- At first we will take a curve in the structure
$$Y^2=X^3+iX+j$$
Where i and j are curve parameters**.**
- We at that point pick a prime digit.
- Utilizing point by multiplying it with itself it would create the curve.
- Choose a creating call attention to those which focuses whose request ought to be huge.
- At that point take an arbitrary number not as much as requested for creating a an isolated digit which will be our isolated or private key.
- The element produced will create its open key by duplicating the producing number with the isolated digit and will distribute the point.

C. Algorithm for ECC

At first we will take a curve in the structure

$$D^2 = E^3 + sE + t$$

Where s and t are bend parameters.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- We at that point pick a prime digit.
- Utilizing point including and point multiplying we process the focuses on the curve of the elliptic.
- Select a creating bring up of those focuses whose request ought to be vast.
- At that point take an arbitrary number not as much as request of creating point as a private number for each element. This will be a mystery key.

This will at that point create its open key by duplicating the producing number with the mystery number and will distribute the point.

V. CORRELATION OF RSA AND ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

As examined previously, in the remote condition, the hardware's plan of action, control and process limit all are constrained. So the encryption context in it must be short power what's more, RAM utilization. In any case, current the most mainstream calculation RSA does not full-fill it.

ECC key size	163	285	411	573
RSA key size	1024	3074	7682	15362
Ratio of the key size	1:6	1:11	1:19	1:27

Table 1: Ratio of the key sizes

Compared to RSA, ECC is more powerful and secure. There are a few examinations between elliptic curve cryptography ECC and RSA.

From the table overhead, we can see the ECC needs little key size however can accomplish a similar security level as a major key size of RSA. A run of the mill precedent is that a hundred and sixty three bit ECC key can do just as, in a similar condition, 1024-bit RSA key.

Calculation	**Values of Signature**		**Size of the key**	
	Authentication	**Value**	**Admin**	**End user**
1024RSA	11.90	304.0	304.0	15.40
160ECDSA	45.09	22.820	22.30	22.30
2048RSA	53.70	2302.70	2302.70	57.20
224ECDSA	121.980	61.540	60.40	60.40

Table 2: Vitality cost of computerized signature and key trade calculations [mJ].

The table above demonstrates to us the vitality cost of RSA and Elliptic curve digital signature algorithm. From here we can plainly observe that ECC has much preferred execution over RSA. The ECC can give an all-out answer for the security issues in the remote correspondence, for example, validation, mark, and key trade. The digital signature algorithm of Elliptic curve is the curve of elliptic simple of digital signature algorithms. It is a very imperative one of ECC. The security of 322-piece Elliptic curve digital signature algorithm is equivalent to the 1024-piece key size of RSA value, also, the length of ECDSA accreditation is 62 bytes, while that of RSA is 256 bytes, Elliptic curve digital signature algorithm is 168 bytes. There is gigantic significance of shorter key lengths particularly in applications having controlled memory assets in light of the fact that shorter key length requires less memory for key stockpiling reason. The cryptosystems of elliptic curve additionally require less equipment assets than traditional open key cryptography. Presently at the security level of ECC curve cryptography is more than that of RSA. RSA can be split effectively, utilizes five hundred and twelve bits and for ECC the quantity of bits is ninety seven, separately. It has been dissected that the calculation control required for splitting ECC is around double the power required for splitting RSA. ECC gives more elevated amount of security because of its complex scientific task. Science utilized for ECC is extensively increasingly troublesome furthermore, more profound than science utilized for ordinary cryptography. Indeed this is the principle reason, why elliptic curves are so useful for cryptographic purposes, yet it too implies that so as to actualize ECC additionally comprehension of arithmetic is needed. The converse task of ECC which known as the Elliptic Curve Discrete Logarithm problem (ECDLP) gets more enthusiastically, quicker, against expanding key length than do the opposite tasks in Diffie Hellman and RSA. As security prerequisites progress toward becoming increasingly stringent and as preparing power get less expensive and progressively accessible, elliptic curve cryptography turns into the progressively functional framework for use. What's more, as security necessities turn out to be all the more requesting, and processors turn out to be all the more dominant. This keeps ECC executions littler and progressively proficient than different executions, ECC can utilize a significantly shorter key and offer the equivalent dimension of security as other topsy-turvy calculations utilizing a lot bigger ones. Also, the distinction between ECC and its rivals as far as key size required for a given dimension of security progresses toward becoming significantly increasingly articulated, at more elevated amounts of security.

VI. CONCLUSION

This paper presents, the advantage of using Elliptic Curve Cryptography in GSM. ECC proves to be better compared to RSA. Elliptic curve cryptography can be utilized in resource asset constrained cell phones with sensible execution compared to RSA. It tells the importance of using ECC in GSM and also gives a brief similar point between elliptic curve cryptography and RSA. The elliptic curve cryptosystem has a superior execution than conventional cryptosystem with high speed, low calculation, and asset utilization. we can provide more security by giving less key size . So it is entirely reasonable for the remote condition. But since of not all the remote correspondence convention have presented elliptic curve cryptography. Additionally, elliptic curve cryptography's quick equipment execution is being looked into, the utilization of ECC in remote correspondence is increasing in scholastic than in industry now.

REFERENCES

1. “ActionTriggered Public-Key cryptography for GSM systems Using RSA with Phone- Dependent end-to-end encryption”, Rehab El Nemr et.al, Journal of Computer Networks and Internet Research, Vol (5), Issue (2), 123–135,June2006. 2. “Fast Algorithm in ECC for WSN”, Xu Huang et.al, International Multi-conference of Engineers and Computer Sci., Vol(2), March 17-19, 2010.
3. “File encryption and decryption system based on RSA algorithm”, Wang Suli, Liu Ganlai, International Conference on Computational and Information Sciences, 797- 800, Issue Date: 21-23 Oct. 2011.
4. “Implementation of Elliptic-Curve Cryptography on Mobile Healthcare Devices”, Malhotra.K et.al, International Conference on Networking ,Sensing and Control, 15-17, April 2007.
5. “Elliptic curve cryptography for Real Time Embedded Systems in IOT Networks”, P Kaur, Sheetal Kalra, International Conference on Wireless Networks and Embedded Systems,2016.
6. “Elliptic Curve Cryptography And Its Applications”, M Amara, Amar S, International Workshop on Systems, Signal Processing and their Applications, 2011.
7. “Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm”, Goswami S et.al, Third International Conference on Intelligent Systems Modelling and Simulation, 2012.
8. “Efficient implementation of EC based key management scheme on FPGA for WSN”, P. Mathew et.al, International Conference on Telecommunication Systems Services and Applications, 2015.
9. “Performance analysis of point multiplication algorithms in ECDH for an end-to-end VoIP network”, G. Vennila et.al, INDICON, 2015.
10. “Embedded systems security: Threats, vulnerabilities, and attack taxonomy,” D. Papp et.al, 13th Annual Conference on Privacy, Security and Trust , 2015.
12. “Secure authentication scheme for IoT and cloud servers”, S. Kalra and S. K. Sood, Pervasive and Mobile Computing, Vol (24), 210–223, 2015.
14. “Embedded Systems Security Challenges,” K. Fysarakis et.al, 4th International Conference on Pervasive and Embedded Computing and Communication Systems, 255-266, 2014.
15. “Emerging Frontiers in Embedded Security”, M. Kermani et.al, 2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems, 203-208, 2013.
16. “Tiny ECC: A Configurable Library for ECC in WSN”, A. Liu and P. Ning, International Conference on Info. Processing in Sensor Networks, 2008.
17. “Lightweight Cryptography for Embedded Systems – A Comparative Analysis,” C. Manifavas et.al, Data Privacy Management and Autonomous Spontaneous Security Lecture Notes in Computer Science, Vol(8247), 333–349, 2014.

AUTHORS PROFILE

Author-1
Photo

M. S. N. G. K. Mounika, I am a student of KL University studying in final year of B-Tech. I have done my specification in cyber security and IOT technologies. I have done my certifications on cyber security, android app development and IOT. I have worked on elliptic curve cryptography as my minor project.

Arvind Yadav. Assistant Professor, KL university Bijayawada. I have completed Ph.D. from National Institute of technology Rourkela. I have published the “Prediction of suspended sediment yield by artificial neural network and traditional mathematical model in Mahanadi river, India in Springer. Recently, I have also published SCI paper impact factor 2.3 in Taylor & Francis. Many papers are under review in SCI journals. I have qualified GATE exam.

Author-3
Photo

S. Lokesh Anand, I am a student of KL University perusing my B-Tech degree and I’m in my final year . I have done my specification in web technologies and cyber security technology. I have done my certificate courses on python and cyber security and IOT applications.

Author-3
Photo

Dr. Penke Satyannarayana, Professor, Electronics and Computer Science, Koneru Lakshmaiah University, Vaddeswaram, India.Ph.D JNTU. AP, India