ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Asymmetric Encryption Public Key Enhance Security in RSA Algorithms

*S.PONNARASI[#1] ,Dr.T.RAJENDRAN[*2]*
[#1]Research Scholar,Department Of Computer Science,
*[*2]Assistant Professor,Department of Computer Science,*
PERIYAR UNIVERSITY,SELAM,
*[*2]Arignar Anna Government Arts College,*
Namakkal, India.

ABSTRACT - This analysis can describe varied sorts of security problems that embrace confidentiality, integrity and accessibility of knowledge. There exists a varied threat to security problems traffic analysis, snooping, spoofing, denial of service attack etc. The uneven key secret writing techniques might give the next level of security however compared to the paralleled bilaterally symmetric biracial circulate cruciform even regular interchangeable isosceles radial satellite radically symmetrical Centrosymmetric rhombohedra trifocal parallel regular key secret writing though we've existing techniques symmetric and uneven key cryptography ways however there exists security issues. a quick description of planned framework is outlined that uses the random combination of public and personal keys. The mechanisms includes: Integrity, accessibility, Authentication, No repudiation, Confidentiality and Access management that is achieved by private-private key model because the user is restricted each at sender and receiver finish that is restricted in alternative models. Wireless sensing element networks (WSNs) have attracted a great deal of researchers because of their usage in essential applications. WSN have limitations on machine capability, battery etc that provides scope for difficult issues. The planned protocol is economical and secure in compared to alternative public key primarily based protocols in WSNs.

KEYWORDS: RSA, DH, ECC, ECDH, ElGamal secret writing, Knapsack, Digital Signature and SRNN.

I. INTRODUCTION

The uneven key cryptosystem involves the utilization of 2 distinct however connected keys particularly, the general public key and also the non-public key. Plaintext is regenerate to cipher text mistreatment the general public key. This method is understood as secret writing that is performed by the sender. On the opposite hand, deciphering of the cipher text is performed by creating use of the non-public key. This method is understood as secret writing and is performed by the receiver. solely the receiver possesses the information of the non-public key. so as to take care of the confidentiality of the non-public key, the general public key's disclosed to the general public. the general public key's used for authentication to confirm that the message is returning from the supposed sender. Public key cryptosystem conjointly ensures confidentiality. solely the receiver's non-public key will decipher the cipher text originating from the sender. Communications of messages are often worn out a secure manner since information of the general public keys not ample to decipher the cipher text.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Due to the higher than benefits, in our planned formula we tend to follow the uneven key cryptography technique. During this theme, there's a relation between the 2 keys. This truth, it's seemingly that the system could also be compromised if somebody discovers the relation between the keys and with success derives the non-public key. In RSA both the keys comprise of the big variety 'n', which may be factored into 'p' and 'q'. the general public key's familiar to any or all. it's straightforward to derive the non-public key if somebody will guess the factors of 'n' to forestallthis from happening, in our formula we have a tendency to try and eliminate the distribution of 'n' in each the keys. Instead, we have a tendency to apply a mathematical transformation over 'n' to urge a replacement for 'n' victimisation that one cannot trace back to the factors of 'n' that are 'p' and 'q'. This improves the safety of the RSA formula [7] by a larger extent.

II. PROPOSED METHOD

RSA is associate degree uneven key cryptosystem depends on the idea that it's tough to seek out the factors of enormous integers. It involves distribution of public and personal key to sender and receiver to write in code and decode the message severally. RSA may be a 3 step method that involves Key generation, Message cryptography and message decryption.

The public-key cryptography development is that the greatest and maybe the sole true revolution withinthe entire history of cryptography. The foremost wide used public-key cryptosystem is RSA. Whitfield Daffier and Martin Lillian Hellman introduced the construct of public key cryptography in 1976.the problem of confidentiality are often clearly resolved by Public key cryptography. The identification downsides are often resolved bySigning a message with a signature encrypted with ones personal key.

One key within the combine are often shared with everyone; it's known as the general public key. the opposite one key within the combine is unbroken secret, it's known as the personal key.

The encryption theme uses RSA and signature of the very fact that:

med ≡ m(mod n) (1)

for m whole number. The cryptography and coding schemes are given in algorithms one and2. The coding works as a result of cd ≡ (me)d≡ m(mod n).The safety lies within the difficultyof computing a transparent text m from a ciphertext c = American state mod n and also the public parameters n (e).

Algorithm 1: RSA Encryption

Input: RSA public key (n,e), Plain text m ∈ [0, n-1]
Output: Cipher text c
begin
1. Compute c = me mod n
2. Return c.
End

Algorithm 2: Decryption RSA

Input: Public key (n,e),Private key d, Cipher text c
Output: Plain text m
Begin
1. Compute m = cd mod n
2. Return m.
End

B. *Diffie-Hellman key exchange (D-H)*

The Diffie–Hellman key exchange theme was 1st revealed by Whitfield Diffie and Martin Lillian Hellman in[1976]. Diffie-Hellman Protocols are to permit the development of common secret key over associate unsure contact channel and to exchange keys. DH could be a methodology

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

for firmly exchanging a secret shared between 2 parties, in period of time, over associate entrusted network.

There are 2 in public known numbers they are:

A prime variety alphabetic character associated an number α that's a primitive root of alphabetic character.Suppose the users A and B would love to exchange a key. User A selects a random number XA<q and computes YA=αX mod alphabetic character. Similarly, user B severally selects a random number XB <q and computes YB=αX mod alphabetic character.

Each facet keeps the X price as non-public that's private and makes the Y price on the market as publically to the opposite side. User A computes the key as K=(YB)X mod alphabetic character and user B computes the key as K=(YA)X mod alphabetic character. These 2 calculations manufacture constant result by the principles of standard arithmetic

K=(YB)X mod alphabetic character

=(αX mod alphabetic character)A mod q

Key Exchange rule

Let us assume that A and B wish to agree upon a key that's to be used for cryptography / decrypting messages that may be changed between them. The Diffie-Hellman key exchange rule works as follows [2].

1. Firstly, A and B agree on 2 giant prime numbers n and g. These 2 integers needn't be unbroken secret. A associated B will use an insecure channel to agree on them .2. A chooses another large random number x and calculates c such that

c=g x mod n

3. A sends the number c to B

4. B independently chooses another large random integer y and calculate d such that

d=g y mod n

5. B sends number d to A

6. A now compute the secret key K1 as follows

K1= d x mod n

7. B now computes the secret key K2 as follows.

K2=c y mod n

C. Elliptic curve cryptography (ECC)

The Elliptic curves in cryptography plan was introduced by Victor Millerand N. Koblitz in 1985 as an alternate to established public-key systems like DSA and RSA. Elliptical curve cryptography (ECC) is also a (PKC) public key cryptography technique supported elliptic curve theory that may be accustomed produce quicker in speed, smaller in size, and additional economical scientific discipline keys to supply authentication theme to RFID system.

Elliptic Curve Encryption/Decryption rule may be explained by following procedure.

Assume user A would like to send message M to B.

1. 'A' chooses a random positive number 'k', a non-public key 'nA'.
2. Generates the general public key PKA = atomic number 11 × G.
3. Calculates the cipher text 'CM' consisting of combine of points CM=kilo , M + kPKB } wherever G is that the base purpose elite on the Elliptic Curve, PKB= nB × G is that the public key of B with non-public key 'nB'.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

4. To rewrite the cipher text, B multiplies the first purpose within the combine by B's secret & subtracts the result from the ordinal point:M + kPKB - nB(kG) = M + k(nB G) – nB(kG)=M.

D. Elliptic curve Diffie–Hellman (ECDH)

Elliptic curve Diffie-Hellman is associate degree anonymous key agreement protocol that allows 2 parties, every having associate degree elliptic curve public key–private key mix combine.ECDH, a variant of DH, is also a key agreement Formula. it's for generating a shared secret between A and B with ECDH, every have to be compelled to agree up on Elliptic Curve domain parameters.

We assume that Alice and Bob use the identical set of domain parameters D = (p, a, b, P, n, h) for his or her computations.

– Alice generates associate impermanent key combine (kA,QA), i.e. generates a random range Ka within the interval [1, n−1] so performs a scalar multiplicationto get the corresponding public key QA = Ka • P. She sends QA to Bob.

– Bob generates associate impermanent key combine (kB,QB) with QB = kilobyte •P within the sameway as delineate higher than and sends the final public key QB to Alice.

– Once Alice receives Bob's impermanent public key QB, she performs a scalar multiplication to urge the shared secret S = Ka • QB.

– Once Bob receives the impermanent public key QA from Alice, he obtains the shared secret through computation of S = kilobyte • QA.

E. ElGamal secret writing algorithmic program

In 1984,T.Elgamal proclaimed a public key theme supported distinct logarithms. It consists of each the secret writing and signature algorithms. The El-Gamal signature algorithmic program is comparable to the secret writing algorithmic program inthat the 2 keys public key and personal key have an equivalent form; but, secret writing isn't an equivalent as signature verification.

ElGamal Key secret writing

The secret writing algorithmic program works as follows: To encipher a message m to A below the general public key ,(G,q,g.h).

1. B chooses a random y from then calculates c1 =gy
2. B calculates the shared secret s=hy
3. B converts the key message m into m' a part of G
4. B calculates. c2=m'.s
5. B sends the ciphertext (c1, c2)= (gy ,m'.hy) =(gy ,m'.(gx)y) to A.

Notethat one will notice easily if one is aware of m'. Therefore,to improve security a replacement y are often generated for each message. For this reason, y is additionally known as associate impermanent key.

ElGamalDecryption

The coding algorithmic program works as follows:

to rewrite a ciphertext (c1,c2) with the personal key x,

1. A calculates the shared secret s=c1x
2. Then A computes m'=c2.s-1 is regenerate into the plaintext message m , wherever inverse of s within the cluster is s-1.(E.g. standard inverse if G could be a subgroups of a increasing cluster of integers modulo n).

The coding algorithmic program produces the meant message, since c2.s-1=m'.hy.(gxy)-1=m'.gxy .g-xy =m'

F. backpack algorithmic program

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

The Merkle–Hellman backpack cryptosystem was fabricated by Ralph Merkle and Martin Hellman in 1978.It was one amongst the earliest public key cryptosystems.Knapsack downside contemplates associate best answer 0-1.
knapsack downside can't be resolved by greedy methodology as a results of it's not fill the capability of backpack and empty amount lower the effective worth per pound of the load, we tend to and that we} ought to estimate the solution to the sub downside with within which the item is exclude before we area unit ready to build the dainty.
Let G be a finitely generated cluster, and let A be a finite generating set for G. Then, parts of G are often portrayed by finite words over the alphabet A±1 = A [A−1]. An*exponent equation* over *G* is an equation of the form

$$h0gx11\ h1gx22\ h2 \cdot \cdot \cdot gxkkhk = 1$$

where *g*1, *g*2, . . . , *gk*, *h*0, *h*1, . . . , *hk*2 *G* are group elements that are given by finite wordsover the alphabet *A*±1 and x1, x2, . . . , x*k*are not necessarily distinct variables. Such anexponent equation is *solvable* if there exists a mapping _ : {x1, . . . , x*k*} ! N such that$h0g_(x1)1\ h1g_(x2)1\ h2 \cdot \cdot g_(xk)$ *k hk*= 1 in the group *G*. The *size* of an equation is P*k*
P *i*=0 |*hi*| + *ki*=1 |*gi*|, where |*g*| denotes the length of the shortest word *w* 2 (*A*±1)_ representing *g*.
Solvability of exponent equations over G is the following computational problem:
Input: An exponent equation *E* over *G* (with elements of *G* specified by words over *A*±1).
Now calculate the sequence
β = (β1, β2... β*n*) where β*i*= *rwi*mod*q*.
The public key is β, while the private key is (*w*, *q*, *and r*).
(ii) Encryption:
To encrypt an *n*-bit message
α = (α1, α2... α*n*),
Where
Is the *i*-th bit of the message and {0, 1}, calculate
The cryptogram then is *c*.
(iii) Decryption:
In order to decrypt a cipher text *c* thena receiver has to find the message bits α*i* such that they satisfy.

G.Digital Signature Algorithm

The Digital signatures and hand-written signatures each accept the fact that it isvery onerous to seek out twoWith constant signature. Individuals used public-key cryptography to reckon digital signatures by associating one thing distinctive with everyone.
The DSA makes use of the subsequent parameters:
1. p = a first-rate modulus, wherever ever 2L-1 < p < 2L for 512 £ L£ 1024 and L a multiple of sixty four.
2. Q = a first-rate divisor of p - one, wherever ever 2159 < Q < 2160.
3. g = h(p-1)/q mod p, wherever ever h is any number with one < h <p - one such h(p-1)/q mod p > 1(g has order Q mod p).
4. x = a arbitrarily or pseudo arbitrarily generated integerwith zero < x < Q.
5. y = gx mod p.
6. k = a arbitrarily generated integerwith zero < k < Q.

Key generation:

In dynamic cluster signature schemes the key generation algorithmic rule GKgis wont to generate the cluster public key and therefore the cluster manager secret keys.group manager generate these keys.
Join procedure:
It is for admitting a replacement valid member to the cluster each dynamic cluster executes the be part of procedure. This procedure is dead between the cluster manager and therefore the member that's United Nations agency want to affix the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

cluster.Upon successful admission for linguistic communication the new member receives the key and therefore the cluster manager gathers the key info needed so as to open the signature generated by the new member.

H. Short vary Natural Numbers algorithmic rule (SRNN)

SRNN algorithmic rule is analogous to RSA algorithmic rule with some modifications.In addition to the current we've used 2 naturalnumbers in try of keys (public, private).These natural numbers will increase the safety of cryptosystem.so its name is "modified as RSA public key cryptosystem victimisation short vary number algorithm "Difference between SRNN and RSA with modulus length 1024 bits are approximately 5080 milliseconds (SRNN 1024 bits > RSA 1024 bits) whereas difference of RSA 2048 bits and SRNN 1024 bits are 5338 milliseconds (RSA 2048 bits > SRNN 1024 bits). Hence SRNN with modulus length 1024 bits are in good balance between speed and security.

III. EXPERIMENTAL RESULTS

(i) Key generation:

1. Generate 2 massive random prime p, q.
2. reckon n=p*q
3. Reckon phi= (p-1) (q-1)
4. opt for Associate in Nursing whole number e, 1<e<phi, specified gcd (e, phi) =1 reckon the specified (e*d) mod phi=1
5.Pick short vary number u haphazardly specified u<phi-1
6. Pick another Short vary number a haphazardly specified phi>a>u and reckon ua
7.Find d specified,
e*d mod ((p-1) (q-1)) =1
8. Public key's (n, e, ua)
9. Personal key's (d, a, u) P, q, alphabetic character ought to even be unbroken secret.

(ii) Encoding method:

Sender will the following:- Obtains the recipient's public key (n,e,ua)

- Represents the plaintext message as a positive whole number m.
- Computes the cipher text c = (m ua) e mod n.
- Sends the cipher text c to recipient.

(iii)Decryption process:

Recipients will the following:-

- Uses his personal key (d, a, u) to reckon m = (v e c) d mod n wherever v= u phi-a mod n. Extracts the plaintext from the whole number representative m.

The following table analyses the assorted Public Key Cryptography Algorithms and its benefits and downsides.

Table 1.comparison for algorithms

S.NO	Algorithms	Advantages	Disadvantages
1	RSA Only intended user can read the message using their private key.	Several secret key secret writing ways that's considerably quicker than any current accessible public-key secret writing.	Diffie-HellmanNo secret sharing necessary. Slower or computationally intensive.
2	ECC Short secret's faster and requires less computing power. it'scostlier	ECDH Very secure means of exchanging keys between two parties Little difficulty in	Elgamal The advantages of a similar plaintext gives a special cipher text when, it's

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

	and it shortens the lifetime of batteries.	exchanging keys.	called encryption.
3	the most disadvantage of El-Gamal is that the	Need for randomness, and its slower speed(especially for signing).	Knapsack A perfect protocol for distribution of secret keys deciphering keys are easy
4	sequences, they're breakable		
5	RSA Only intended user can read the message using their private key.	Several secret key secret writing ways that's considerably quicker than any current accessible public-key secret writing.	Diffie-Hellman No secret sharing necessary. Slower or computationally intensive.
6	ECC Short secret's faster and requires less computing power. it's costlier and it shortens the lifetime of batteries.	ECDH Very secure means of exchanging keys between two parties Little difficulty in exchanging keys.	ElgamalThe advantages of a similar plaintext gives a special cipher text when, it's called encryption.
7	DSA	It is employed in several crypto product for	DSA isn't used for cryptography except for digital
		authentication.	signature.
8	SRNN	SRNN formula is best in security	SRNN formula is slower in speed

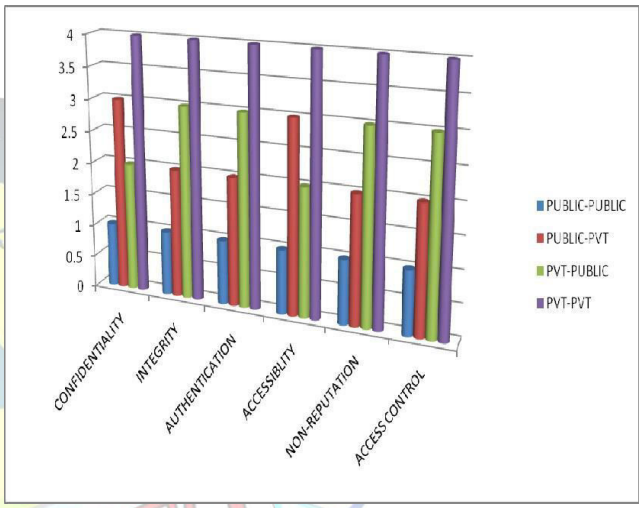

Fig.1 Comparison of Attributes of Information Security.

Private -Private key technique uses a private key at sender site and a private key at receiver,both are different and secret .Data is more securely transmitted from sender to receiver.Based on the comparison of security mechanisms all the parameters are achieved in private - private technique.Therefore it is considered as secure model.

IV.CONCLUSION

This analysis gift varied key algorithms of uneven like RSA,ECC,ECDH, Elgamal, knapsack, DSA and SRNN.RSA is one in all the foremost effective secret writing rule in terms of security and plausibility. ElGamal rule is a lot of secured as compared

to RSA rule as a result of it generates a a lot of advanced cipher textand it had been additionally slow as a result of after we write and rewrite it, it generates over one public keys. Elliptic Curve Cryptosystem is safer. Elliptic curve replaces ElGamal additionally and use distinct index drawback. the safety feature here is that the elimination of n from the initial RSA rule. Instead, the freshly generated replacement for n will be employed in each the keys. The RSA rule is liable to mathematical resolution attacks. The rule that we tend to given during this research eliminates this issue creating the rule safer with a small increase of your time complexness.

REFERENCES

[1]Caregia Mellon Software Engineering institute "*Public Key Cryptography"*.

[2] William Stallings, "Cryptography and Network Security Principal and Practice", Fourth Edition, Pearson 2005.

[3]Gustavo da Silva Quirino and Edward David Moreno,"architectural evaluation of algorithms RSA, ECCand MQQ in arm processors", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.

[4]Gustavo S.Quirino,Edward David Moreno,and Leila B.C.Matos,"PerformanceEvalution of Asymmetric Encryption Algorithms in embedded platforms used in WSN,Further information:www.nist.gov.

[5] S Nithya, Dr E. George Dharma Prakash Raj, "Survey on Asymmetric key Cryptography Algorithms", Journal of Advanced Computing Technologies (ISSN: 2347-2804) Volume NO. 2 Issue No. 1,Febuary 2014.

[6]PrashantkumarArya,DrMahendra Singh Aswal,DrVinodKumar,"Comparative Study of Asymmetric Key Cryptographic Algorithms",ISSN:2249-5789 Prashant Kumar Arya et al , International Journal of Computer Science & Communication Networks,Vol 5(1),17-21.

[7]GauravYadav,Mrs.AparnaMajare,"A Comparative Study of Performance Analysis of Various Encryption Algorithms", (ICEMTE-2017)Volume:5 Issue:3,ISSN:2321-8169,70-73.March 2017.

[8] E. George Dharma Prakash Raj, k. Sheela, "Survey on public key cryptography algorithms", IJSRCSMS July 2013.

[9]David A. Carts," A Review of the Diffie-Hellman Algorithmand its Use in Secure Internet Protocols",SANS Institute of InfoSec Reading Room,November 5, 2001.

[10]Monika Nayak,Deepak Rajput, "Cryptography Algorithms-The Science of Information Security:Review Paper", IJIRCCE,Vol.5,Issue 3,March 2017.

[11]HimjaAgarwal,Prof.B.R.BadadaPure, "A Survey Paper On Elliptic Curve Cryptography",(IRJET)Volume: 03 Issue: 04 | Apr-2016.

[12]H T Loriya,A.Kulshreshta,D.R. Keraliya,"Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network",IJARCCE,Vol. 6, Issue 2, February 2017.

[13]AnnapoornaShetty, ShravyaShetty K, Krithika K,"A Review on Asymmetric Cryptography –RSA and ElGamalAlgorithm", IJIRCCE,Vol.2, Special Issue 5, October 2014.

[14]VeenuYadav,Ms.ShikhaSingh,"A Review Paper on Solving 0-1 knapsack Problemwith Genetic Algorithms",VeenuYadav et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (2) , 2016, 830-832.

[15]Markus Lohrey and Georg Zetzsche,"The Complexity of Knapsack in Graph Groups",(STACS 2017).

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

[16]VenkateswaraRaoPallipamu,Thammi Reddy K, Suresh Varma P,"A survey on digital signatures",IJARCCE*Vol. 3, Issue 6, June 2014.*