International Journal of Cyber-Security and Digital Forensics (IJCSDF) 9(3): 139-146
The Society of Digital Information and Wireless Communications (SDIWC), 2020 ISSN: 2305-0011

Security Implementation Using RSA and Enhanced RSA

Dr.Vanitha K.[1], Varada Sandeep Kumar[2], Dara Anil Kumar Dara[3]
Assistant Professor [1], PG Scholar [2,3]
Department of Computer Applications
Madanapalle Institute of Technology and Science, Madanapalle
kvanithacse@gmail.com , drvanithak@mits.ac.in
Sandeeproyal1998@gmail.com
Daraanilkumar123@gmail.com

ABSTRACT

Today, RSA calculation is the most broadly utilized open key cryptosystem around the globe. It is utilized for security in everything from internet shopping to phones. In any case, the essential RSA isn't semantically secure, since encoding a similar message more than once consistently gives the equivalent cipher text. Consequently, the essential RSA is helpless against set of backhanded assaults, for example, known plaintext, picked plaintext, timing, basic modulus, and recurrence of squares assaults. In addition, RSA is known to be much more slow than the norms symmetric key encryption and it doesn't utilize for encoding huge information. This paper presents an altered methodology which is an improvement over conventional RSA calculation by including exponential forces, n prime numbers, numerous open keys, and K-NN calculation. Changed methodology additionally gives highlight of check at both side's sender and recipient.

KEYWORDS

Cyber Security, Authentication, Cryptography, Public key, Private Key, RSA, ERSA, Security.

1 INTRODUCTION

Cybercrime can be carried out against an individual or a gathering; it can likewise be perpetrated against government and private associations. It might be planned to hurt somebody's notoriety, physical damage, or even mental mischief. Cybercrime can make direct mischief or backhanded damage whoever the casualty is. In any case, the biggest danger of cybercrime is on the money related security of a person just as the administration.

Cybercrime causes loss of billions of USD consistently. As we know cryptography is the best approach to blocking the authorization by encrypt and decrypt data. Initially, the data which is to be transmitted is encrypted to a coded format called cipher text. This cipher text is transmitted via a channel and at the receiver end, decrypts it to get the actual data. Converting actual text to coded text is known as encryption and coded text to actual text is known as decryption. Substitution and Transposition are basic techniques available in cryptosystem. Substitution technique undergoes changing the actual letters of plaintext with coded letters or numbers to form a cipher text. As shown in (Figure 1).

A portion of the Substitution systems incorporate Caesar figure, Monoalphabetic figures, Play fair figure, Polyalphabetic figure, and so forth. Transposition cipher is the process of rearranging of the bits or characters in the data. There are many techniques in Transposition cipher one of it is Rail Fence cipher. Further, Modern cryptography was created where a key is utilized in the encryption and decoding systems. In symmetric cryptography model, a key which is classified is shared by the sender and the collector. Here key and calculations are utilized to create a coded book. Essentially, at the beneficiary side, the unscrambling calculation (same as the encryption calculation running backward) utilizes a similar key to get the genuine plaintext.

My research is based on providing best security using RSA which has some limitations where it can be overcome by implementing a new

algorithm based on the existing one which is known as Enhanced RSA which includes best security and complexity both (space and time).

Types of Cybercrime

Let us now discuss the major types of cybercrime –

- Hacking
- Unwarranted mass-surveillance
- Child pornography
- Child grooming
- Copyright infringement
- Money laundering
- Cyber-extortion
- Cyber-terrorism

2 HISTORY

Open key cryptography was observed in 1975. The main context of Diffie and Hellman who introduced public key systems is to identify the problems of symmetric cryptography. The principle issues looking in the security are Key Distribution and Digital Signatures and the responses for them were unsolved. In 1970s, Roger Needham of Cambridge University, started an authentication technique to protect computer passwords. Just approved people can get to the made sure about information that may be altered in a particular time which can be positioned away at a spot. To protect this, the images of passwords were developed using one-way function. The one-way function is helpful to protect passwords from the intruder whereas it succumbs to others who intercepts the login, as the password does not change with time. The solution of a trap-door one-way function is initiated where anyone with the secret information can compute the inverse function. These are further developed and the messages are provided with signatures, known as digital signatures. The concept of Public key cryptosystem was emerged where inverse pair of keys are used. If actual text is encrypting with one key, it can be decrypt by the other key.

In the RSA algorithm, the sender can either private key or public key or sometimes both depending on the application. After all the public key cryptosystems can be classified as Encryption/Decryption, Digital Signature, and Key Exchange. After the creation of open key cryptography, Diffie and Hellman distributed the principal open key calculation alluded as Diffie-Hellman Key Exchange. This calculation, empowers a protected trade of key for encryption between the sender and the collector. It requires to process discrete logarithms. Consider a sender A and the recipient B. A prime number q and a whole number α (crude base of q) are shared openly.

This calculation is infeasible when huge primes are considered. Diffie-Hellman Key trade is viewed as uncertain against a man-in-the-center assault. A gatecrasher can plan to assault by figuring two irregular private keys X1 and X2 and compute two open keys Y1 and Y2. Thus, this convention is powerless against this sort of assaults where confirmation is the primary disadvantage. Further, numerous well known lopsided calculations, for example, RSA, ElGamal, Elliptic Curve Cryptography (ECC), and so forth, were presented which incorporate computerized marks and testaments to give validation and secure transmission. In the following area, we will talk about the most well-known open key cryptosystem, RSA.

3 CYBER SECURITY

Cyber security is a potential movement by which data and other correspondence frameworks are shielded from and additionally protected against the unapproved use or alteration or misuse or even robbery.

Moreover, digital security is an all-around structured procedure to ensure PCs, systems, various projects, individual information, and so on., from unapproved get to.

Cyber Security, a wide range of information whether it is government, corporate, or individual need high security; be that as it may, a portion of the information, which has a place with the administration safeguard framework, banks, protection innovative work association, and so on are profoundly private and even limited quantity of carelessness to this information may make extraordinary harm the entire country. In this way, such information need security at an extremely elevated level.

4 SERVICES AND MECHANISMS

ITU-T gives some security administrations and a few components to actualize those administrations. Security administrations and components are firmly related in light of the fact that an instrument or blend of systems are utilized to offer an assistance.

4.1 Types of Security Services

- Authentication:

assures recipient that the message is from the source that it claims to be from.

- Availability:

Available to authorized entities for 24/7.

- Confidentiality:

Information is not made available to unauthorized individual

- Integrity:

Assurance that the message is unaltered

- Non-Repudiation:

Protection against denial of sending or receiving in the communication.

4.2 Types Security Mechanisms

- Encipherment:

  This is stowing away or covering of information which gives privacy. It is additionally used to supplement different components to offer different types of assistance. Cryptography and Steganography are utilized for enciphering

- Digital Integrity:

The information trustworthiness system annexes to the information a short check esteem that has been made by a particular procedure from the information itself. Information uprightness is saved by contrasting check esteem got with the check esteem created.

- Digital Signature:

An advanced mark is a method by which the sender can electronically sign the information and the collector can electronically confirm the mark. Open and private keys can be utilized.

- Authentication Exchange:

In this two entities exchange some messages to prove their identity to each other.

- Traffic Padding:

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

- Routing Control:

Directing control implies choosing and constantly changing distinctive accessible courses among sender and collector to keep the rival from listening stealthily on a specific course.

- Notarization:

Legally approbation implies choosing a third confided in gathering to control the correspondence between two elements. The collector can include a believed outsider to store the sender demand so as to keep the sender from later denying that she has made a solicitation.

- Access Control:

Access control used methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

5 RSA ALGORITHM

RSA is the primary uneven key calculation created by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA is a square figure framework, which depends on the number hypothesis. It utilizes two prime numbers to create open and private keys which are utilized for encryption and decoding. RSA includes encrypting, decrypting and key trade.

5.1 Steps Involved in RSA Algorithm

RSA Algorithm involve 3 major steps

- Key generation
- Encryption
- Decryption

Key generation

1: Choose two large unique prime numbers p, q

2: Compute

$$n=p * q \quad (1)$$

3: Compute

$$\varphi(n) = (p-1)(q-1) \quad (2)$$

4: Select an integer e for encryption such that gcd ((φ (n), e) =1 and 1<e< φ (n).

5: Compute

$$d \equiv e^{-1} (\text{mod } \varphi(n)). \quad (3)$$

6: (e, n) is public key and (d, n) is private key.

Encryption:

Compute Cipher text

$$C = M^{e} \text{mod } n \quad (4)$$

Decryption:

Compute plaintext

$$M = C^{d} \text{ mod } n \quad (5)$$

5.2 Program for RSA in C

```
#include<stdio.h>

#include<math.h>

intgcd(int a, int h)

{

    int temp;

    while(1)

    {

        temp = a%h;

        if(temp==0)

        return h;

        a = h;

        h = temp;

    }

}

int main()

{

    double p = 17;

    double q = 11;

    double n=p*q;

    double count;

    double s= (p-1)*(q-1);

    double e=7;

while(e<s)

    {

    count = gcd(e,s);

    if(count==1)
```

```
        break;
    else
        e++;
    }
    double d;
    double k = 2;
    d = (1 + (k*s))/e;
    doublemsg = 88;
    double c = pow(msg,e);
    double m = pow(c,d);
    c=fmod(c,n);
    m=fmod(m,n);
    printf("Messagedata=%lf",msg);
    printf("\np = %lf",p);
    printf("\nq = %lf",q);
    printf("\nn = pq = %lf",n);
    printf("\ntotient = %lf",s);
    printf("\ne = %lf",e);
    printf("\nd = %lf",d);
    printf("\nEncrypted data = %lf",c);
    printf("\nOriginal Message Sent =
%lf",m);
    return 0;
}
```

5.3 Example of RSA

- Key Generation

    1. Select 2 prime numbers let p=17 and q=11
    2. Calculate n = p×q =17 ×11=187
    3. Calculate φ(n)=(p-1) (q-1) = 16 × 10= 160
    4. Select 'e' such that e is relatively prime such that gcd ((φ (n), e) =1 and 1<e< φ(n)

       gcd ((160, e) =1

       ⇨ e=7
    5. Determine d such that:

       de =1 mod (n)

       d × 7 = 1 mod 160d=23

       ⇨ d=23
    6. Then the resulting keys are:

       pu = {7, 187} pr = {23, 187}

    Let M=88

- For encryption

  $C= M^e \bmod n$

  $C=88^7 \bmod (187) = 11$

- For Decryption

  $M = C^d \bmod n$

  $M=11^{23} \bmod (187) =88$

As shown in Figure 2

6 USES OF RSA

RSA is one of the most famous calculation utilized in transmitting information safely where it follows open key cryptosystem. Computerized Signature is worked alongside RSA to upgrade the security level. The idea of Digital Signature in RSA calculation is created utilizing hash capacities. Hash work is accessible on the two sides of the information. In the wake of applying the hash work, scarcely any lines of information are gotten, known as message digest. The message digest is scrambled with the private key to deliver an advanced mark. These can be utilized in budgetary exchanges, and electronic documents, for example, email, electronic

records, and so on. This aid in distinguishing altering and fabrication of information.

7 RSA SECURITY

RSA gives private and secure correspondences. The primary quality of RSA is that the open encryption key doesn't uncover the comparing decoding key. As of late, RSA is utilized in programs and web servers for secure correspondences. The security of RSA, relies upon the trouble of considering huge prime numbers. For the little estimations of p and q, the encryption procedure is excessively frail and interloper can unscramble the message by utilizing techniques for likelihood hypothesis. Besides, for enormous estimations of p and q, the encryption procedure turns out to be excessively unpredictable and expends additional time. In any case, every one of these assaults, relies upon the abuse of RSA. They may cause vulnerabilities, yet on the off chance that all the qualities are taken significantly, these sort of assaults can be forestalled effectively as they rely upon the structure of RSA. These incorporate some arbitrary blames, for example, the recipient figures the marks independently with p and q to accelerate the calculation. This sort of figuring's accelerates the general mark time and along these lines improves the exhibition of the framework. However, in case a little error in check of p or q, can impact the whole imprint. This kind of shortcomings is dangerous to cryptographic frameworks. In general, the assaults of RSA are principally centered on the numerical counts. Whenever executed appropriately, RSA gives greater security in the present applications.

8 LIMITATIONS IN RSA

The confinement of utilizing open key cryptography for encryption and decoding is speed. Its calculation sets aside some effort to register the numerical activity of RSA calculation. Open key utilized for encryption ought to be verified. In the event that programmer know the variables of an enormous prime number, by then this break the security of computation, considering the way that the estimations of open key and private keys are known with the help of parts. Loss of private key may release the data in the correspondence arrange.

9 ENHANCED RSA ALGORITHM

9.1 About ERSA

Cryptography is a way to deal with oversee secure data from software engineers. Not only it gives assures, but also provides authenticity. This paper presents a modified approach RSA which is used to give more secured algorithm by including exponential powers, n prime numbers, multiple public keys, and K-NN algorithm. Modified approach also gives feature of verification at both side's sender and receiver. Modified approach is an enhancement form of RSA cryptosystem.

Here we utilize 4 prime numbers in process.

Algorithm

Key Generation

- Select the random values A, B, C and D
- Calculate

$$S=A*B*C*D \quad (1)$$

- Calculate

$$Ø\ (S) =(A-1)\ (B-1)\ (C-1)(D-1) \quad (2)$$

- Compute e:

  lg S <e< S (e must be co-prime to S)

- A general formula to find d

$$d * e =1 \bmod (S) \quad (3)$$

Encryption:

$$C = P^e \bmod (S) \quad (4)$$

Decryption:

$$P = C^e \bmod (S) \quad (5)$$

9.2 Example of ERSA

- Key Generation

1. Let A=3, B=11, C=17 and D=5
2. Calculate

S=3*11*17*5=2805 and A*B=3*11 =33

3. Calculate

ϕ (S) = (A-1) * (B-1) * (C-1) * (D-1)

= 2*10*16*4 =1280

4. Select e, such that gcd (e, ϕ (S)) = 1

gcd ((e, 1280) =1

⇨ e=61

5. Determine d such that

d * e =1 mod (S)

d * 61 = 1 mod 1280

⇨ d=21

6. Then the resulting keys are :

pu = {61, 2805 }

pr = {21, 2805 }

Let P=88

- For encryption

C= P^emod S

C=88^{61}mod(2805) = 913

- For Decryption

P = C^d mod S

P=913^{21}mod (2805) =88

As shown in Figure 3

9.3 Pros of Enhanced RSA

- The strength of large prime four variables A, B, C, D. However, it is hard to people to break the into four prime numbers.
- Having separate variable for encryption and decryption gives more security for data.
- Here the Security is more for having many complexities in key.

10 FIGURES

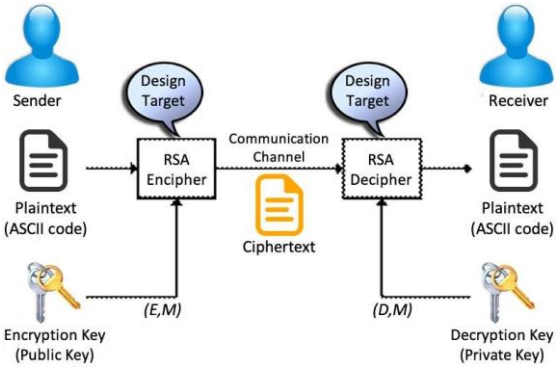

Figure 1 Network Model of Public Key Cryptography

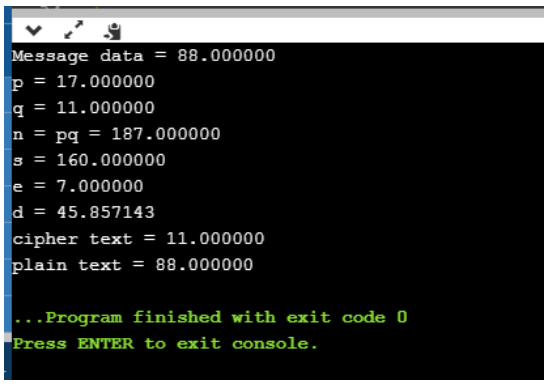

Figure 2 Implementation of RSA

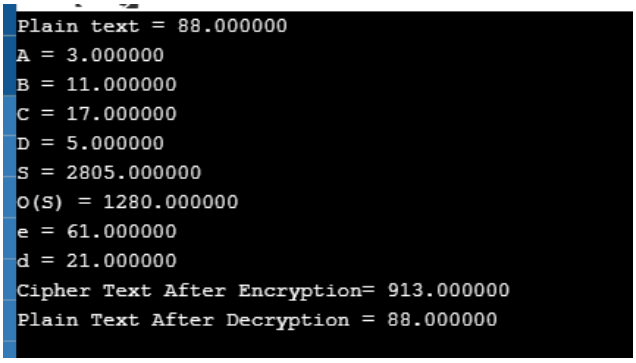

Figure 3 Implementation of Enhanced RSA

11 CONCLUSION

This study shows us the importance of securing the information from unlicensed users. This study states the important aspects of cybercrime and cyber security, ways to overcome the problem. For securing the data for unauthorized user RSA algorithm is the best approach through which you can encrypt and decrypt data. Although RSA plays a major role in security, for better security we use Enhanced RSA Algorithm where the unauthorized person cannot decode a number into 4 large prime numbers. This offer extra safety and dependable use in network

REFERENCES

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Vol. 21, pp.120-126, 1978.

[2] http://sdiwc.net/ijcsdf/files/IJCSDF_Vol6No1.pdf

[3] K. Vanitha, Dr.A.M.J.Md Zubair Rahman and K.Anitha," An Analysis of Issues in Security and Routing Protocol in MANET", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 1, pp.1594-1599 January – 2014.

[4] https://www.geeksforgeeks.org/rsa-algorithm cryptography

[5] https://binaryterms.com/rsa-algorithm-in cryptography.html

[6] K. Vanitha, K. Anitha, Dr.A.M.J. Md Zubair Rahaman, Dr.M. Mohamed Musthafa," Analysis of Cryptographic Techniques in Network Security", Journal of Applied Science and Computations, Volume 5, Issue 8,pp:155-163, 2018.

[7] Stallings, William, "Cryptography and Network Security: Principles and Practice," Prentice Hall Press Upper Saddle River, NJ, 2010.

[8] https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

[9] Vanitha, K., Zubair Rahaman, A.M.J. Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol. Cluster Computing22,13453–13461(2019). doi.org/10.1007/s10586-0181958-9.

[10] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[11] A. Sharaieh, A. Edinat and S. AlFarraji, "An Enhanced Polyalphabetic Algorithm on Vigenerecipher with DNA-Based Cryptography," 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, 2018, pp. 1-6, doi: 10.1109/AICCSA.2018.8612860