STUDY OF RSA CRYPTOSYSTEMS AND SUGGESTIVE ENHANCEMENTS

*Research conducted under the supervision of Mr. B.Dey. (*Dept. of CSE, NIT Silchar*)*

Anirban Chatterjee (*Author*)
Dept. of CSE, NIT Silchar.
7th Sem, B. Tech
email : reachanirban95@gmail.com

Jasbir Singh Birdi (*Author*)
Dept. of CSE, NIT Silchar.
7th Sem, B. Tech
email : jappy95jasbir@gmail.com

Partha Pritam Paul (*Author*)
Dept. of CSE, NIT Silchar.
7th Sem, B. Tech
email : parthap177@gmail.com

Suhrid Barthakur (*Author*)
Dept. of CSE, NIT Silchar.
7th Sem, B. Tech
email : suhrid53@gmail.com

***Abstract*—Rivest–Shamir–Adleman algorithm is widely used in the popular implementation of public-key infrastructures. In this research work, we present a drawbacks and suggestive enhancements on the algorithm including their cryptanalysis. (*Abstract*)**

Keywords— Encryption, Decryption , RSA , Cryptography, Computer Security.

I. Introduction

This project, under the guidance of Mr. Biswanath Dey aims at providing a layer of extra security to the very well known RSA algorithm for encryption. RSA is a cryptosystem for public-key encryption also known as asymmetric cryptographic named after its inventors Rivest, Shamir and Adleman.

II. THEORY

How RSA works ?

RSA is based on the simple yet strong mathematical philosophy that it is very difficult to factorise a very large number. RSA involves the following 4 steps :

1.Key generation.

2. Key distribution.

3. Encryption.

4. Decryption.

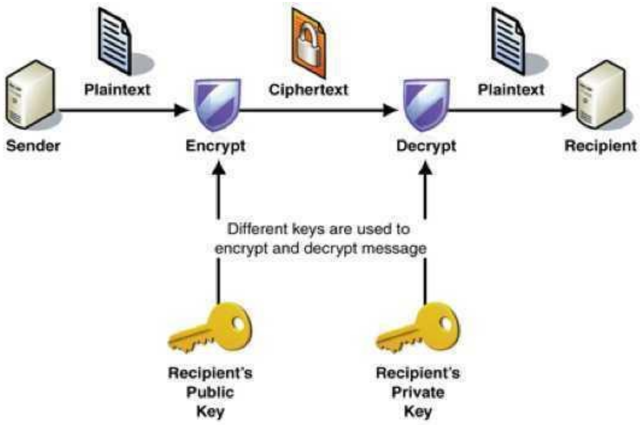

Figure 1: The principle mechanism of RSA.

Working of the algorithm.

The mathematics behind RSA algorithm is based on Integer factorisation, Prime Generation, Modular exponentiation and its roots[12]. The basic objective being, making the RSA easier to implement but harder to crack.

a)**Prime Generation** : The process of generating large random prime numbers is an easy task ,and there exists algorithms for generation in O(ln(n)) complexity.

b)**Integer Factorisation** : Given a (n = p * q), it is always quite difficult to recover the prime factors p and q.

Despite hundreds of years of study of the problem, finding the factors of a large number still takes a long time. The fastest current methods are much faster than the simple approach of trying all possible factors one at a time.

For example, , it has recently been recorded that recovering the prime factors of a 1024-bit number would take a year on a machine that costs US $10 million. A 2048-bit number would require several billion times more work.

c)**Modular Exponentiation** : The operation of modular exponentiation calculates the remainder when an integer P raised to the eth power, is divided by a positive integer m (the modulus). In symbols, given base P, exponent e, and modulus m, the modular exponentiation C is: C ≡ Pe (mod m).

Two **optimisations** facilitate the problem :

a) Multiplying by an appropriate sequence of previous intermediate values, instead of just
P, reduces the number of multiplications to nothing more than twice the size of e in binary.
b) Dividing and take the remainder after each multiplication keeps the intermediate results of the same size as n.

III. Limitations of the RSA.

The RSA cryptosystem is hard to crack and is secure but surely it has certain limitations . They are:

1. if the primes(p & q) used are small enough then a computer will make easily factor 'n'.

2. If private keys of users are unavailable, it is very much vulnerable to impersonation.

3. The maximum size of the message(P) that can be transferred at once is such that size of P must be less than the size of the key(n). Currently the maximum recommended key size is 2048 bits.i.e; P < n

4. A slow encryption process compared to symmetric key as calculating c=me mod n takes time for large data.

5. It is very slow for long messages.

Now to overcome some of the limitations, let us ponder over the suggested modifications of the base model of
RSA cryptosystem.

A) Modifications to the base RSA

To overcome the certain limitations in the base model .We present a modified RSA model which is based on mainly :

a) Protecting the private key in case the attacker successfully factorizes the modulus n .
b) Increase the ability to send larger messages through RSA.
c) Faster key generation.

The modifications suggested are listed below :

a) In our model unlike the base model which uses two large random primes p,q we use a random number of large primes to generate N. This adds an extra level of security as factoring N becomes harder by multiple folds.
b) To further enhance the security further we introduce a pseudo Modulus say F(N).
c) In order to permit large message to be transferred we split the message into blocks of sizes 1024 bits
We then encrypt each of the message blocks and send it through the channel.

B) The modified algorithm is depicted below :

The Algorithm:

1. Select a random number(say 4) of large prime numbers p , q , r , s.

2. Compute φ(N)=(p-1)*(q-1)*(r-1)*(s-1)

3. Now we compute a variable P_e (consists all possible values of E) such that gcd[E ,φ(N)]=1.

4. In next step select a value of variable e from P_e and calculate "d" such that [e*d mod φ(N)] = 1

5. In this step, finds the desired "Se" where "Se" are special value over the range of values "Pe " ,which are multiplied by N to produce pseudo modulus F(N)=N*S_e. The new modulus "F(N)" is used in place of actual modulus "N" as shown in figure 2 and do the process of encryption and decryption. If the results of decryption and plaintext are matched, then the selected value that was considered "S_e" will be the desired value.Otherwise if the plaintext and decryption results are not matched then the selected number must be again set for S_e .

6. If "S_e " has not found go back to step 4 change the value of "e" and compute "d" then repeat step 5.

Finally after S_e has been found we get our fake modulus F(N)=N*S_e .This gives us the public key :(F(N), e) and private key:(F(N),d).The encryption is done as C=M^e mod F(N)And the decryption as

$P=C^d$ mod F(N).The encryption can be made faster by using Chinese Remainder Theorem[6].

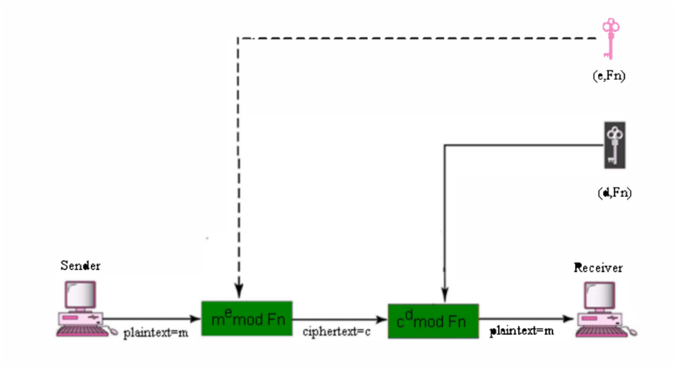

Figure 2: encryption & decryption using"***Fn***"

C) Observations pertaining to this model

The Modified RSA has the advantage over base model that if anyone is able to factorize the modulus "n" in RSA, can easily decrypt the message.

- However, in our case the result produced by "Se" will produce pseudo modulus "F(N)" and this is publically announced. If anyone tries to factorize the "F(N)", he can't find out the original value of decryption key, because the input primes are not the actual result of factorization, and also using random number of initial input primes increases the overhead of finding them ,hence result produced by just initial factorization of F(N) will not give the decryption key. This thereby adds extra security to the algorithm.
- The figures below depicts the comparison between the RSA and Modified RSA scheme to find the inverse using public key. In RSA the input primes and result of inverse on output are the same, while not so in case of the modified scheme.

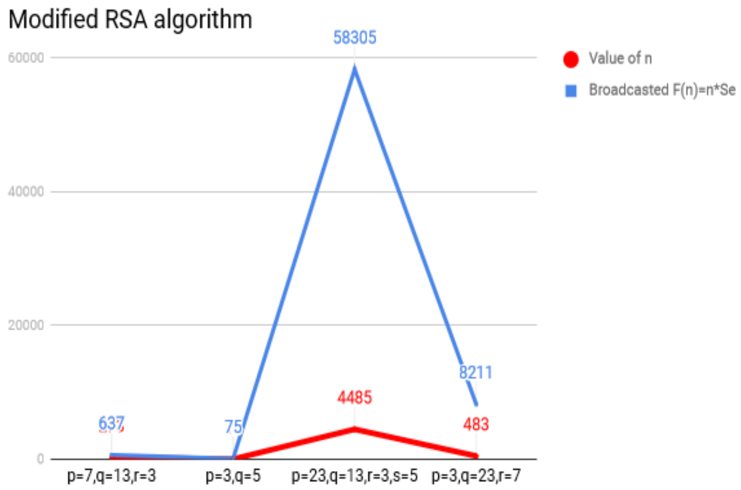

FIGURE 3: COMPARATIVE GRAPHS OF VALUES OF N CALCULATED AND BROADCASTED IN MODIFIED RSA

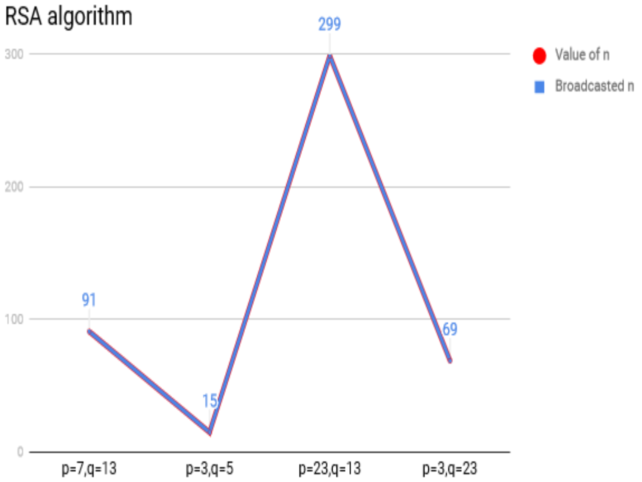

FIGURE 4: COMPARATIVE GRAPHS OF VALUES OF N CALCULATED AND BROADCASTED IN RSA

IV. CRYPTANALYSIS OF THE MODIFIED RSA

A) Factoring

The problem of finding non trivial prime factors of a composite number is known as Integer factorization problem. As we have seen that one of the major security issues associated with RSA is the Integer factorization problem, the RSA system is as strong as factorization of n after which generation of private key becomes easier.

We now compare the Modified scheme suggested against the RSA based on how it can deal with such attacks better.

Following are most common factoring methods:

1) Trial Division

It is an exhaustive approach for searching the private key.Here we successively divide the N by all primes <=$N_{1\backslash 2}$.

The number of attempts is then bounded by (k$N_{1/2)}$/log(N),where k is the no. of primes randomly selected in our algorithm for generation of n.

This is relatively better than RSA using 2 primes for which the no of attempts is (2$n_{1/2}$/log(n)).Using the fake modulus F(N)=N*Sp_e ,Sp_e here adds an extra security when N is relatively small.

2) Pollard p-1 method

This is a special factorization technique depending on the properties of divisor of N.Now say if q is a prime factor of N for which p-1 is B-power smooth.

If we make M the product of large enough powers of all primes less than B, then we have that M is a multiple of p – 1.

The problem is that we do not know the factorization of p – 1 beforehand , so we have to choose a bound B and increase it until we are successful.

The running time of this algorithm is O(B × log B × log2 n).
For the suggested the algorithm the bound of B is increase multiplicatively as the pseudo-modulus and ,k no. Of initial primes requires us to find all the prime factors of F(N) ,i.e. k+1.
This becomes effective in case of smaller keys which in RSA can be easily decrypted using this method.
Also to increase the security we take initial primes p such that p-1 are not B-power smooth.

B) Other attacks

1) Low Private Exponent attacks

As shown by M. Wiener in his study small value of d can lead to total break of system.hence if F(N) is the modulus and d is the private exponent, with d < 1/3(F(N))1/4 , then given the public key (e, N), an attacker can efficiently recover d.

Hence d needs to be selected accordingly.

2) Partial Key Exposure Attack

As per study by Boneh, Durfee and Frankel shows the importance of protection of the entire private exponent d.

They have shown that, if the modulus N is k bits long, given the (k/4) least significant bits of d, an attacker can recreate all of d in time linear O(e log(e)), where e is the public exponent. This means that if e is small, the exposure of a quarter of bits of d can lead to the recovery of the whole private key d.

Hence it is necessary for safe storage of the private key from attacker.

Conclusion

Here thereby we have seen that the modified scheme can provide more security against the system by preventing integer factorization from occurring easily with conventional methods ,and also helps to increase the size of the message limit.However it’s effectiveness against modern advanced factoring techniques like Elliptic Curve Factorization have not been verified against.

Future Scope

Although RSA is an extensively researched topic there hasn’t been much developments which aren’t an alteration/tweak for optimization.Even our algorithm although promises better security has more time complexity than the original,so it is mostly a trade off between security and time.Hence there exist the scope for the modified scheme to know how good it is implementation wise and also suggesting better algorithms for it.

References

• [1]Ming-Der Shieh, Chien-Hsing Wu , Ming-Hwa Sheu, Jia-Lin Sheu and Che-Han Wu,” Asynchronous implementation of modular exponentiation for rsa cryptography” , 30-30 Aug. 2000, Cheju, South Korea.

• [2]Taek- Won Kwon, Chang-Seok You, Won-Seok Heo, Yong-Kyuk ang, and Jzin-Rim Choi,” Two implementation methods of a 1024-bit rsa cryptoprocessor based on modified montgomery algorithm”, pp: 650 - 653 vol. 4,2001

•[4]Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek.” Dual RSA and Its Security Analysis”,pp. 2922 – 2933.vol:53,2007.

•[5]K.Gomathi and Dr.Meera Gandhi,”Weight based Clustered Key Management scheme using RSA for Wireless Mobile Ad hoc Networks”,pp. 359 – 364, 14-16 Dec. 2011, Chennai, India

•[6] H. C. Williams, “A Modification of the RSA Public-Key Encryption Procedure”, IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.

•[7] Ravi Shankar Dhakar,Amit Kumar Gupta, Prashant Sharma,” Modified RSA Encryption Algorithm (MREA)”,pp. 426 – 429, 7-8 Jan. 2012, Rohtak, Haryana, India.

•[8]Gaurav R. Patel, Prof. Krunal Panchal and Sarthak R. Patel “ A Comprehensive Study on Various Modifications in RSA Algorithm”.

•[9]Aarushi Rai, Shitanshu Jain, ” Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem”, volume 4 Issue 7 – July 2017, Jabalpur, India.

•[10]Prabhat K. Panda and Sudipta Chattopadhyay, ” A Hybrid Security Algorithm for RSA Cryptosystem”, Jan. 06 – 07, 2017, Coimbatore, India.

•[11]R. Minni, K. Sultania and S.Mishra, “An algorithm to enhance security in RSA” , 4th ICCCNT, IEEE , pp.1-4, 2013.

•[12]Burt Kaliski ,”The Mathematics of the RSA public key cryptosystem”,RSA Laboratories.