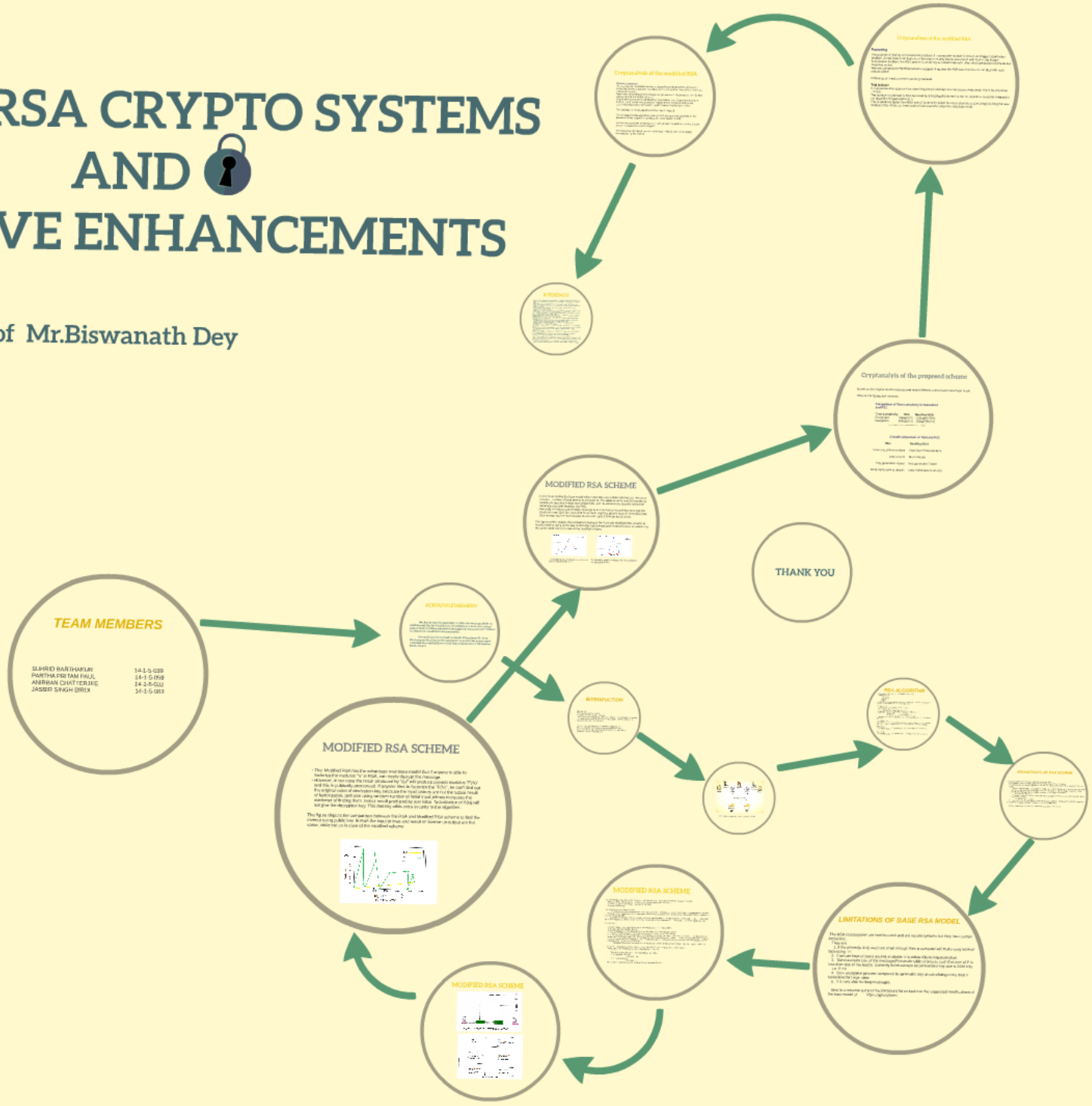
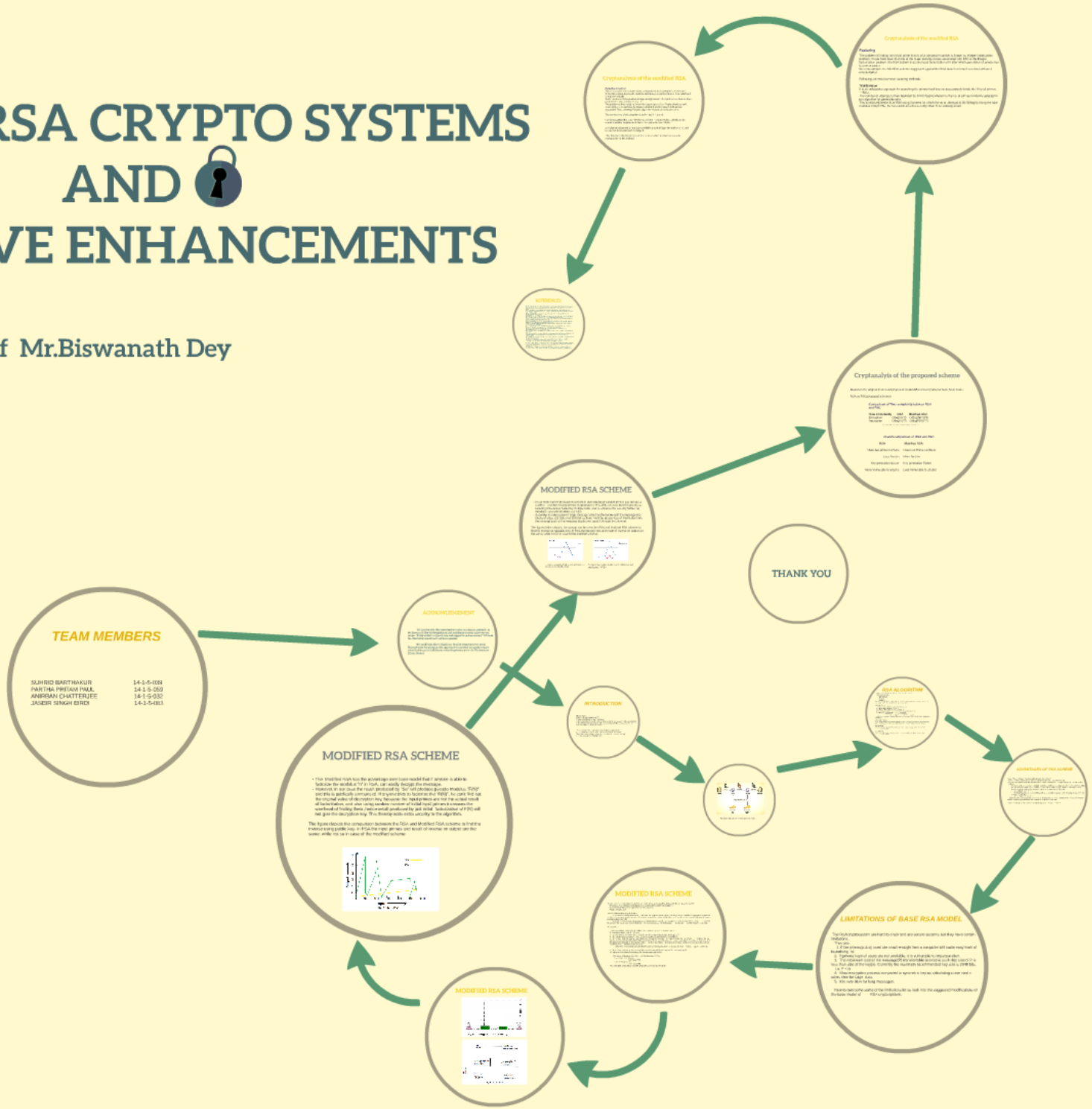
STUDY OF RSA CRYPTO SYSTEMS AND SUGGESTIVE ENHANCEMENTS

Under the Guidance of Mr.Biswanath Dey



STUDY OF RSA CRYPTO SYSTEMS AND SUGGESTIVE ENHANCEMENTS

Under the Guidance of Mr.Biswanath Dey



TEAM MEMBERS

SUHRID BARTHAKUR	14-1-5-039
PARTHA PRITAM PAUL	14-1-5-059
ANIRBAN CHATTERJEE	14-1-5-032
JASBIR SINGH BIRDI	14-1-5-083

ACKNOWLEDGEMENT

We ,hereby take this opportunity to offer our sincere gratitude to Mr.Biswanath Dey for his guidance and confidence on us to carry out our project "Study on RSA cryptosystem and suggestive enhancements" .Without his efforts this would have not been possible.

We would also like to thank our Head of Department Dr. Arup Bhattacharjee for giving us this opportunity to present our project report submitted in partial fulfillment of the Requirements for the 7th Semester B.Tech. Project.

INTRODUCTION

What is RSA?
RSA was first described in 1977.
It Stands for Rivest - Shamir - Adleman.
It is a cryptosystem for public-key encryption also known as asymmetric cryptography,
It is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

What is Public Key Encryption or Asymmetric Cryptography?
It is a cryptographic system that uses two keys public and private.
These keys are just large numbers but not identical (i.e; asymmetric).
It is used to encrypt and decrypt data.

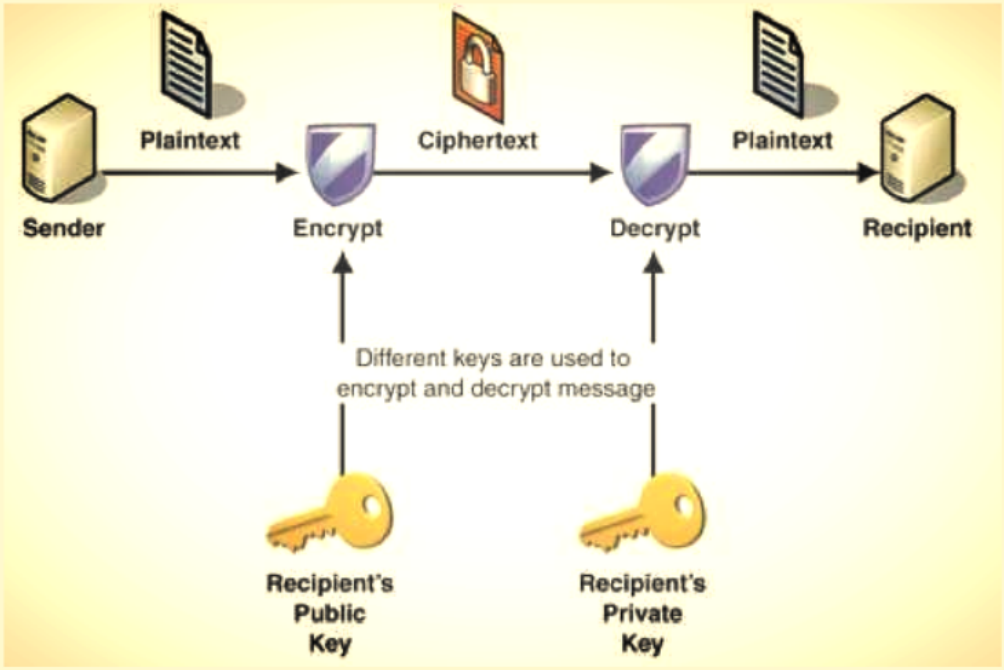


Fig: Sender sending a secure message to the recipient

RSA ALGORITHM

RSA is based on the fact that it is difficult to factorize a large integer.
RSA involves four steps:-

- Key generation
- Key distribution
- Encryption
- Decryption

RSA uses two pairs of related keys (Public key) uk{ e, n} for encryption and (Private key) vk{d, p,q} for decryption. So, lets see how these four steps are implemented:-

KEY GENERATION:

1. Receiver chooses two very large prime numbers p & q.
2. Calculating the modulus as: $n = p * q$.
3. Calculate Euler's value as $\varphi(p. q) = (p - 1)*(q - 1)$.
4. Now, Choose an integer 'e' such that $1 < e < \varphi(p. q)$ and $gcd[e, \varphi(p. q)] = 1$
5. Calculate 'd' from the equation: $d * e \equiv 1 \bmod(\varphi(n))$.
   which implies:- $(d * e) \bmod(\varphi(n)) = 1$.
   $d * e = k * \varphi(n) + 1$,where k is quotient.
6. After the key generation Receiver announces uk{ e, n} as public Key and vk{d, p,q} is kept secret as private key.

KEY DISTRIBUTION:
Now if Sender wants to send a secret message to Receiver using RSA then the sender must know the public key to encrypt the message and the receiver uses it's private key to decrypt the message.

ENCRYPTION:
The message or the plaintext(P) that the sender wants to send is encrypted to Cipher text(C) as:

$C = Pe \bmod(n)$

DECRYPTION:
After receiving the cipher text the receiver uses its private key(d,p,q) to decrypt the message as:

$P = Cd \bmod(n)$

ADVANTAGES OF RSA SCHEME

Some of the advantages of the RSA cryptosystems are as follows:

- RSA is used for secure communications over public channels which are unsecured.
- RSA scheme also uses Digital Signatures which avoids repudiation and masquerading. It can be achieved as follows:
  - The fact that the encryption and decryption operations are inverses and operate on the same set of the entries also means that operations can be used in reverse order to obtain a digital signature. A message can be digitally signed by applying the decryption operation, i.e. exposing it to dth power:
  - C = SIGN (P) = Pd mod n.
  - The digital signature can be verified by applying the encryption operation and comparing the result with the message or retrieving it:
  - P = VERIFY (C) = Ce mod n

In practice, clear m text is generally a function of the message, such as a unidirectional formatted message hash. This allows you to sign a message of any length with only one exponential.

- RSA can also be used to share the symmetric key on an unsecured channel.

LIMITATIONS OF BASE RSA MODEL

The RSA cryptosystem are hard to crack and are secure systems but they have certain limitations .

They are:

1. if the primes(p & q) used are small enough then a computer will make easy work of factorising 'n'.
2. If private keys of users are not available, it is vulnerable to impersonation.
3. The maximum size of the message(P) transferrable at once is such that size of P is less than size of the key(n). Currently the maximum recommended key size is 2048 bits. i.e; $P < n$
4. Slow encryption process compared to symmetric key as calculating $c = m^e \bmod n$ takes time for large data.
5. It is very slow for long messages.

Now to overcome some of the limitations let us look into the suggested modifications of the base model of RSA cryptosystem.

MODIFIED RSA SCHEME

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

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

Let us look understand these in details:

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 . and to enhance the security further we introduce a pseudo Modulus say F(N).

Secondly, in order to permit large message to be transferred we split the message into blocks of sizes 1024 bits (not 2048 bit as there might be greater loss of information).We then encrypt each of the message blocks and send it through the channel.

The Algorithm:

1. Select a random number(say 4) of large prime numbers p , q , r , s. and N=p*q*r*s.
2. Compute φ(N)=(p-1)*(q-1)*(r-1)*(s-1)
3. Now we compute a variable Pe (consists all possible values of e) such that gcd[e ,φ(N)]=1.
4. In next step select a value of e from Pe 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*Se. 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 "Se" will be the desired value.

   Otherwise if the plaintext and decryption results are not matched then the selected number must be again set for Se .

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

Finally after Se has been found we get our fake modulus F(N)=N*Se .

This gives us the public key :(F(N) , e) and private key:(F(N),d).

The encryption is done as

$$C=Pe \bmod F(N)$$

And the decryption as

$$P=Cd \bmod F(N)$$

The encryption can be made faster by using Chinese Remainder Theorem.

MODIFIED RSA SCHEME

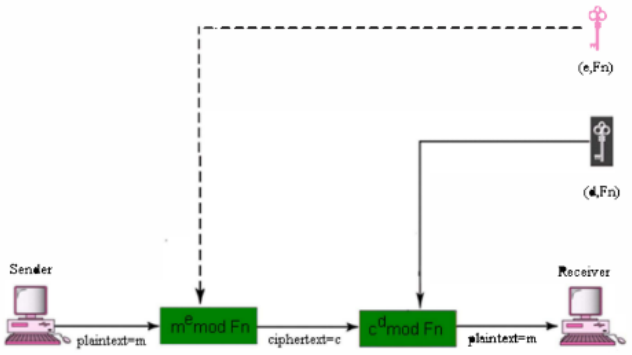


Figure 2: encryption & decryption using"***Fn***"

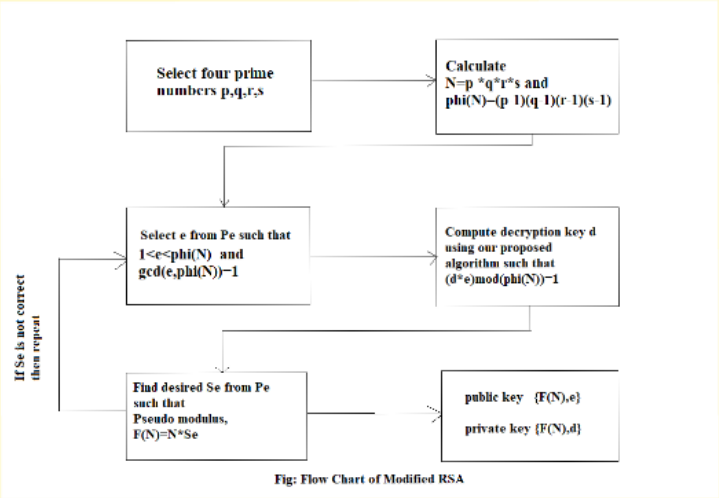


Fig: Flow Chart of Modified RSA

MODIFIED RSA SCHEME

- 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 figure 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

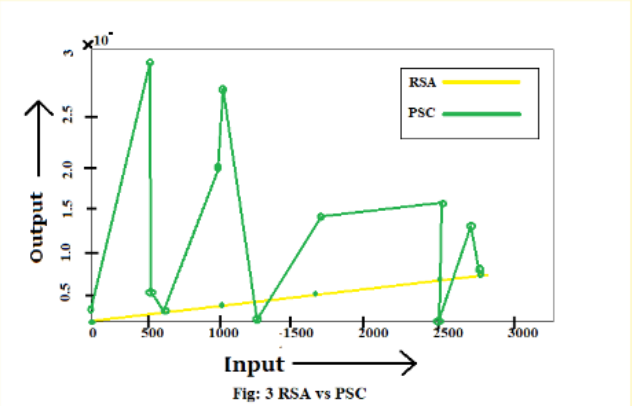
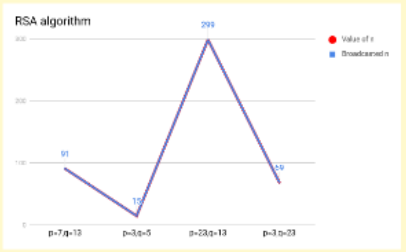


Fig: 3 RSA vs PSC

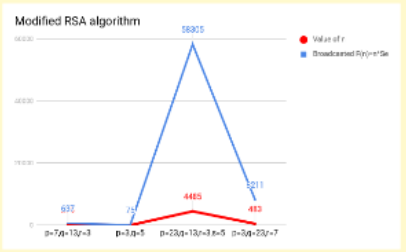
MODIFIED RSA SCHEME

- 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 .and to enhance the security further we introduce a pseudo Modulus say F(N).
- Secondly, in order to permit large message to be transferred we split the message into blocks of sizes 1024 bits (not 2048 bit as there might be greater loss of information).We then encrypt each of the message blocks and send it through the channel.

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.



Comparative graphs of values of n calculated and broadcasted in Modified RSA



Comparative graphs of values of n calculated and broadcasted in RSA

Cryptanalyis of the proposed scheme

Based on the original model and proposed model different comparisons have been made.

RSA vs PSC(proposed scheme)

Comparison of Time-complexity between RSA and PSC.

Time Complexity	RSA	Modified RSA
Encryption	O(log(n)^3)	O((log(N)^3)*k)
Decryption	O(log(n)^2)	O(log(F(N))^2)

k=no.of iterations after which correct Se is found. k<=sizeOf(Pe)

Overall comparison of RSA and PSC.

RSA	Modified RSA
Uses two prime numbers	Uses four Prime numbers
Less Secure	More Secure
Key generation slower	Key generation Faster
More Vulnerable to attacks	Less Vulnerable to attacks

Cryptanalysis of the modified RSA

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:

Trial Division
It is an exhaustive approach for searching the private key.Here we successively divide the N by all primes <=N1\2 .
The number of attempts is then bounded by (kN/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 (2n/2)/log(n).Using the fake modulus F(N)=N*Se ,Se here adds an extra security when N is relatively small.

Cryptanalysis of the modified RSA

Pollard p-1 method

This is a special factorization technique depending on the properties of divisor of N.For this division to prevail it must be such that q is a prime factor of N for which q-1 is B-power smooth.

Now 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 q – 1.

The problem is that we do not know the factorization of q – 1 beforehand as don't know q initially, so we have to choose a bound B and increase it until we are successful.Thus ,following Pollard's algorithm we predict the factor q of n.

The running time of this algorithm is O(B × log B × log2 n).

For the suggested the algorithm the bound of B increase multiplicatively as the pseudo-modulus requires us to find all the prime factors of F(N) .

And also we select two primes say r,s initially at start of algorithm such that r-1 and s-1 are not B-powersmooth for large B.

This becomes effective in case of smaller keys which in RSA can be easily decrypted using this method.

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-Kyu Kang, and Jzin-Rim Choi," Two implementation methods of a 1024-bit rsa cryptoprocessor based on modified montgomery algorithm", pp: 650 - 653 vol. 4,2001.

[3] 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.

[4] 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

[5] 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.

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

[7] Gaurav R. Patel, Prof. Krunal Panchal and Sarthak R. Patel " A Comprehensive Study on Various Modifications in RSA Algorithm".

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

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

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

[11] Manoj Agrawal , B. L. Pal , Rohit Maheshwari," Improvement Over Public Key Cryptosystem RSA by Implementing New Decryption Key Generation Algorithm" ,pp 300-304,Volume-5, Issue-6, December-2015

[12] A. Joseph Amalraj, Dr. J. John Raybin Jose," a survey paper on cryptographic techniques", pp. 55 – 59 Vol. 5, Issue. 8, August 2016.

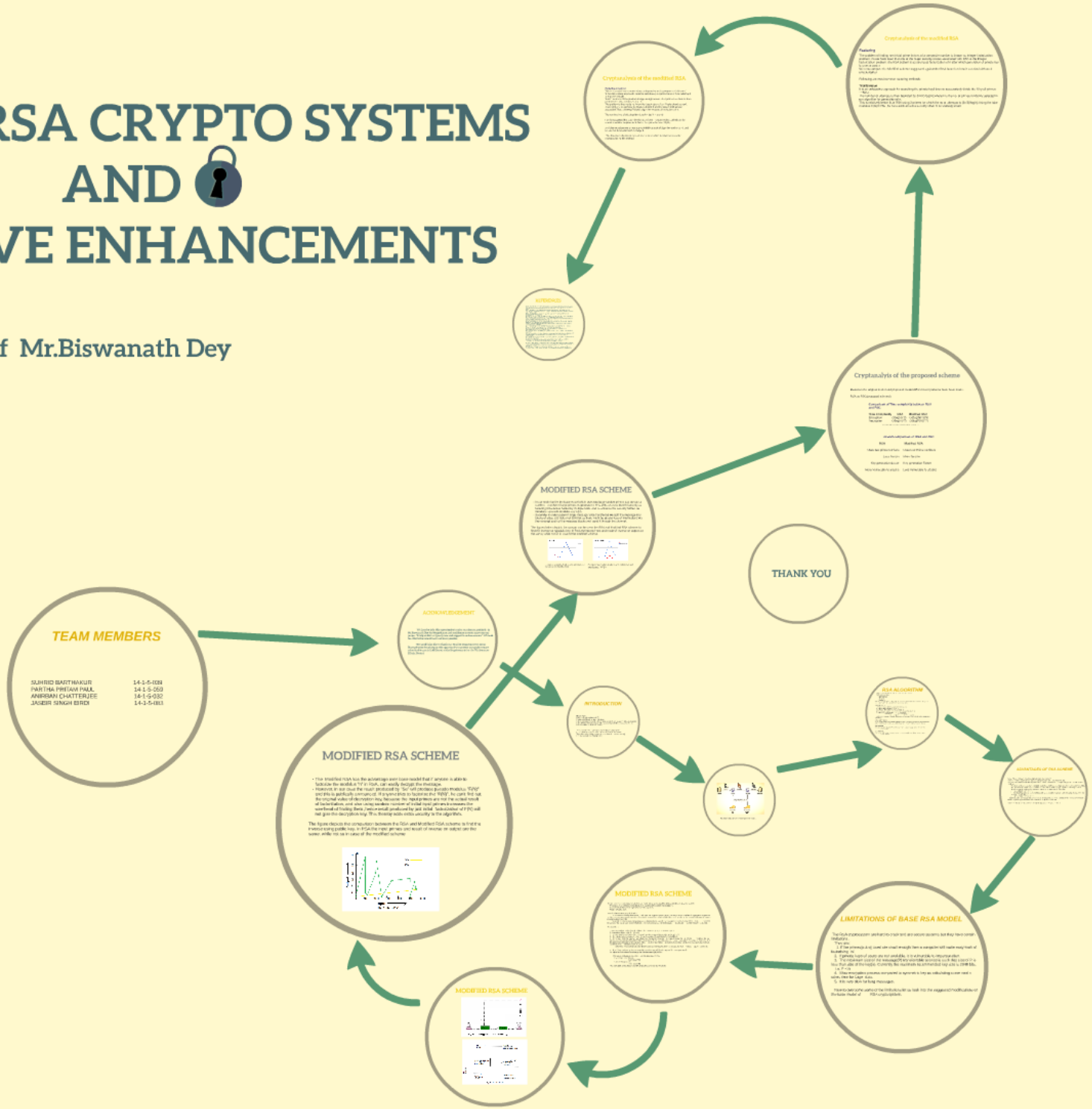
[13] S. Mangard, M. Aigner and S. Dominikus, "A Highly Regular and Scalable AES Hardware Architecture", IEEE Transactions on Computers, Vol. 52, No. 4, pp. 483- 491, 2003.

[14] M. Y. Wang, C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, "Single and Multi Core Configurable AES Architectures for Flexible Security", IEEE Transactions on Very Large Scale Integration Systems, Vol. 18, No. 4, pp. 541-552, 2010.

[15] M.Thangavel, P. Varalakshmi, M. Murrali and K.Nithya, "An enhanced and secured RSA key generation scheme" Journal of Information Security and applications, Elsevier, vol 20, pp.3-10, 2015.

STUDY OF RSA CRYPTO SYSTEMS AND SUGGESTIVE ENHANCEMENTS

Under the Guidance of Mr.Biswanath Dey



THANK YOU