***Abstract* —** *This should contain the abstract of the mini project. It is a brief summary of your project and the concept involved in it such that it will be useful to help the reader quickly ascertain the project’s purpose. Length of abstract should be between 12 to 15 lines in a single paragraph without any sketches or drawings. Please follow the instructions given for every topic below. The titles shown in BLACK are mandatory whereas titles in RED are optional. Ask your Guide about this. The write up must in black Times New Roman 12 font. All titles should be in black Times New Roman 12 font bold and Italics.*

***Keywords*** *— RSA, Encryption, Decryption, Cyber Security, Asymmetric cryptography, public key cryptography.*

# INTRODUCTION

Cryptography is the practice of securing information by converting it into an unreadable format, known as ciphertext, using various mathematical algorithms and techniques. It ensures that only authorized individuals can access and understand the original information, referred to as plaintext. The primary goals of cryptography include confidentiality, integrity, authentication, and non-repudiation. Confidentiality ensures that information remains hidden from unauthorized individuals, integrity guarantees that the information remains unaltered, authentication verifies the identity of the sender or receiver, and non-repudiation prevents individuals from denying their involvement in a transaction or communication. Cryptography relies on two main types of algorithms: symmetric-key algorithms and asymmetric-key algorithms. Symmetric-key algorithms use a single key to both encrypt and decrypt data. The same key is used by both the sender and receiver, which requires secure key exchange methods. Examples of symmetric-key algorithms include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). Asymmetric-key algorithms, also known as public-key algorithms, employ a pair of mathematically related keys: a public key and a private key. The public key is freely available to anyone, while the private key is kept secret. Messages encrypted with the public key can only be decrypted with the corresponding private key. Asymmetric-key algorithms provide a secure method for key exchange and digital signatures. One of the most widely used asymmetric-key algorithms is the RSA algorithm.

# Literature Review

R.L. Rivest, A. Shamir, and L. Adleman[1] proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. If the security of our method proves to be adequate, it permits secure communications to be established without the use of couriers to carry keys, and it also permits one to “sign” digitized documents. The reader is urged to and a way to “break” the system. Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of condense. The encryption function is the only candidate for a “trap-door one-way permutation” known to the authors. The large volume of personal and sensitive information currently held in computerized data banks and transmitted over telephone lines makes encryption increasingly important. In recognition of the fact that efficient, high quality encryption techniques are very much needed but are in short supply, the National Bureau of Standards has recently adopted a “Data Encryption Standard”, developed at IBM. The new standard does not have property (c), needed to implement a public-key cryptosystem.

In the paper “Modified RSA Encryption Algorithm using Four Keys” by Nivetha et al, Preethy et al and Santosh et al[2]. The proposed paper enhances the RSA algorithm through the use of four prime number in combination of public and private key. Hence by using this, factoring complexity of variable is increased, this makes the analysis process with the development of equipment and tools become much easier. The use of four prime number will give the ability to the modified encryption technique to provide more security in accessing, and also increased speed. This was developed from the original RSA algorithm the additional two prime numbers are going to provide secrecy. Many experiments have been done under this proving Modified RSA encryption Algorithm using four keys to be faster and efficient than the original encryption and decryption process. This thesis presents the implementation of successive subtraction operation instead of division operation. By applying this approach we can achieve the high computational speed and reduce the complexity of the mathematical steps.

“A Modified and Secured RSA Public Key Cryptosystem Based on ‘n’ Prime Numbers”[3] by Muhammad Ariful Islam et al, Md. Ashraful Islam et al, Nazrul Islam, Boishakhi Shabnam et al proposed an enhanced and modified approach of RSA cryptosystem based on “n” distinct prime number. This  existence of “n” prime number increases the difficulty of the factoring of the variable “AN” which increases the complexity of the algorithm. In this approach, two different public key and private key generated from the large factor of the variable “A” and perform a double encryption-decryption operation which affords more security. Experiment on a set of a random number provided that the key generation time, analysis of variable “N’, encryption and decryption will take a long time compared to traditional RSA. Thus, this approach is more efficient, highly secured and not easily breakable. “Matrix Modification of RSA Public Key Cryptosystem and its Variant”[4] by Gupta et al and sanghi et al. In this paper, modification of RSA public key cryptosystem using square matrices of order h x h is proposed. Also, a variant of RSA using modulus of the form p'q is proposed along with its matrix modification.

# Methodology/Experimental

1. *Traditional RSA Algorithm*

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is one of the most popular asymmetric-key algorithms used for secure communication and digital signatures. RSA is based on the mathematical difficulty of factoring large composite numbers.

The security of RSA is based on the difficulty of factoring large numbers. Breaking RSA encryption requires factoring the modulus, which becomes increasingly difficult as the size of the prime numbers used in the key generation process increases.

RSA is widely used for secure communication, digital signatures, and key exchange protocols. It provides a secure method for transmitting information over insecure networks while maintaining confidentiality, integrity, and authentication.

Here's a simplified overview of the RSA algorithm:

1. Key Generation:
   1. Select two large prime numbers, p and q.
   2. Compute the modulus, n, by multiplying p and q: n = p \* q.
   3. Compute Euler's totient function, φ(n), where   
       φ(n) = (p - 1) \* (q - 1) (1)
   4. Choose an integer e, such that 1 < e < φ(n) and e is coprime to φ(n).
   5. Calculate the private key, d, which is the modular multiplicative inverse of e modulo   
       φ(n): d ≡ e^(-1) mod φ(n). (2)
   6. The public key is (n, e), and the private key is (n, d).
2. Encryption:
   1. Convert the plaintext message into a numerical value, m.
   2. Compute the ciphertext, c, by raising m to the power of e and taking the modulus n:   
       c ≡ m^e mod n (3)
   3. The ciphertext c is the encrypted message.
3. Decryption:
   1. Obtain the ciphertext, c.
   2. Compute the plaintext, m, by raising c to the power of d and taking the modulus n:  
       m ≡ c^d mod n. (4)
   3. The plaintext m is the decrypted message.

1. *Our Proposed RSA Algorithm*

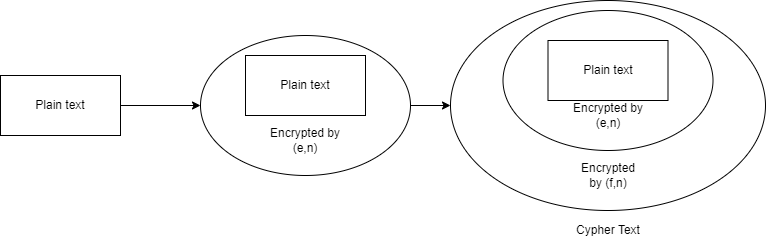
Our proposed algorithm uses 3 input variables and based on that we calculate and instead of the Euler's totient function φ(n) we use exponentiation modulo.

1. Key Generation
   1. first select 3 random prime numbers which are not equal to each other p,q and r.
   2. n = p\*q\*r.
   3. Calculate the exponentiation modulo by the given formula :   
       N(n)=(p^2-1)\*(q^2-1) (5)
   4. choose two integers e and f such that 1<e<N(n) and 1<e<N(n). e and f are coprime to N(n).
   5. calculate d and f such that:  
       d\*e=1 mod N(n) and g\*f=1 mod N(n) where d is the modulo inverse
   6. public keys are (n,e) and (n,f) and private key is (n,d) and (n,g).
2. Encryption
   1. convert the plaintext into numerical value by replacing the letters by their index number
   2. Divide the whole number into 4 parts and place them in row major form in a 2x2 matrix M
   3. compute the cipher text c by the following formula:

Cm=(M^e mod n)^f mod n (5)

* 1. Cm is a 2x2 matrix, by taking the row major form of this matrix we will get a number and by replacing the number by the index of corresponding letters we will get the ciphertext c.

1. Decryption
   1. Obtain the ciphertext c.
   2. decrypt the ciphertext by the following formula:
   3. M=(Cm^g mod n)^d mod n
   4. now write down M in row major form and convert it into plaintext by replacing the numbers with corresponding letter



# Results and Discussions

References

1. A method for obtaining digital signatures and public-key cryptosystems, R. L. Rivest, A. Shamir, L. Adleman Authors Info & Claims, Communications of the ACMVolume 21Issue 201 February 1978pp 120–126https://doi.org/10.1145/359340.359342
2. Modified RSA Encryption Algorithm using four keys, Nivetha A, Preethy Mary S, Santosh kumar J, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCICN-2015 Conference Proceedings
3. Islam, M. , Islam, M. , Islam, N. and Shabnam, B. (2018) A Modified and Secured RSA Public Key Cryptosystem Based on “n” Prime Numbers. *Journal of Computer and Communications*, **6**, 78-90. doi: [10.4236/jcc.2018.63006](https://doi.org/10.4236/jcc.2018.63006).
4. Matrix Modification of RSA Public Key Cryptosystem and its Variant, S.C Gupta and Manju Sanghi, International Journal on Emerging Technologies 12(1): 76-79(2021), ISSN No. (Print): 0975-8364, ISSN No. (Online): 2249-3255