The Seybold Report

ISSN 1533-9211

DOI 10.17605/OSF.IO/8ZRTW

PERFORMANCE EVALUATION OF CRYPTOGRAPHIC ALGORITHMS USING MATHEMATICAL NUMBERS

MOHAMMED SHAKEEL

Ph.D. Scholar, Department of CSE, Invertis University, Bareilly (U.P.), India, Assistant Professor, Department of FOCA, Invertis University, Bareilly (U.P.). Email: shakeel@invertis.org,

AKASH SANGHI*

Assistant Professor, Department of CSE, Invertis University, Bareilly (U.P.), India.
Corresponding Author Email: sanghiakash@gmail.com*,

YDS ARYA

Professor, Department of CSE, Invertis University, Bareilly (U.P.), India. Email: yds.a@invertis.org,

GAURAV AGARWAL

Associate Professor, Department of CSE, Invertis University, Bareilly (U.P.), India.
Email: gauravagarwal95@gmail.com

Abstract

In the real-world, data security with data confidentiality, user authentication, data integrity, and non-repudiation; play an important role. Encryption is the utmost effective way to attain data security as far as security goals are concerned. This paper presents an outlook on the current state in the field of encryption algorithms, particularly on the use of special mathematical numbers. This paper focuses on different types of encryption algorithms that use unique mathematical numbers (e.g. Armstrong Number, Palindrome Number, Composite Number, and Prime Number, etc.) for performing encryption. This paper presents a comparative study of all the techniques together, which cover the performance of the encryption processes and analyzes their security issues.

Keywords: Armstrong Number, Prime Number, Composite Number, Palindrome Number, ASCII Values, Authentication, Cryptography.

1. INTRODUCTION

1.1 Cryptography

Now days, it is very challenging to transmit data in a secure manner from one end to another end. The reason behind is that hackers are becoming more knowledgeable and equipped with the powerful penetration tools. Several techniques have been used to ensure secured data transmission, among which cryptography is one of the disciplines that is used to secure the actual information from the unauthorized users.

Cryptography is a discipline which refers to the art of secret writing. Cryptography is derived from a Greek word “kryptos” and “logos,” meaning “hidden word”. Cryptographic algorithms can be classified in several ways, one of the criteria used for classification is, that a user can use different keys for cryptographic functions. Symmetric and Asymmetric Key encryption are two types of cryptographic procedures. In symmetric key encryption, a similar key is used for encryption and decryption, also called as private or secret-key encryption. The following

ISSN 1533-9211

DOI 10.17605/OSF.IO/8ZRTW

expression is used for obtaining ciphertext by encrypting plaintext with the use of shared secret key:

$CT = E_K(PT)$---------- *Eq-1*

The expression to obtain plaintext by encrypting ciphertext using a same secret key is as follows:

$PT = D_K(CT)$ ---------- *Eq-2*

Where; PT- Plaintext

CT- Ciphertext

E- Encryption

D- Decryption

K-Secret key

Advanced Encryption Standard (AES), Rivest Cipher (RC4, RC5 and RC6), Data Encryption Standard (DES), Blowfish, International Data Encryption Algorithm (IDEA) etc. are some examples of symmetric encryption methods.

Asymmetric key encryption, also called as public-key/asymmetric key encryption, uses two different keys, one for encryption and other for decryption. The following expression is used for obtaining ciphertext by encrypting plaintext using asymmetric key encipherment.

$CT = E_{K1}(PT)$ ---------- *Eq-3*

The expression to obtain plaintext by encrypting ciphertext using asymmetric key is as follows:

$PT = D_{K2}(CT)$ ---------- *Eq-4*

Where;

K1-Reciever's Public key

K2- Receiver's Private key

A cryptosystem is an implementation of cryptographic algorithms one for the encryption of original data and another for decryption of secret data to provide data security, generation and sharing of secret key is also a part of this system. The basic Model of a cryptosystem that provides confidentiality to the data being transmitted is shown in Figure 1:

ISSN 1533-9211

DOI 10.17605/OSF.IO/8ZRTW

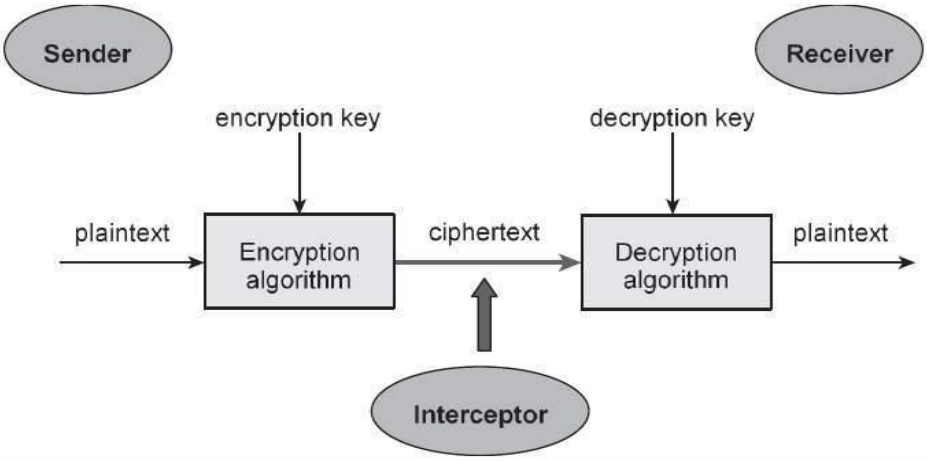


Figure 1: Basic Model of Cryptosystem [1]

Few basic terms related to cryptography and cryptosystems are as follows:

Plaintext: The Actual, intelligible message/data used as input by the algorithm.[1]. Plaintext can refer to anything which humans can understand and/or relate to.

Ciphertext: The message is jumbled and unreadable. While processing plaintext, it is the output produced by the encryption algorithm and is used as input to the decryption algorithm [2].

Encryption Algorithm: An algorithm which takes plaintext and a secret key as input to produce ciphertext as output [2].

Decryption Algorithm: An algorithm which takes ciphertext and a secret key as inputs to produce plaintext as output [2].

Secret Key: It is one of the inputs that an encryption and decryption algorithm takes into account for processing to give ciphertext and plaintext as deliverable. Two different secret keys produce two different ciphertext on the same algorithm and plaintext [2].

Cryptanalysis: It's a way for recovering a secret key or plaintext without knowing the secret value from an algorithm and ciphertext.

1.2 Armstrong Number

A number N will be an Armstrong number of order p, where p refers to number of digits.

If xyz. . . = $x^p + y^p + z^p + \ldots = N$ ----------*Eq-5*

For example, if N=371, then on taking p=3, we have;

$371 = 3^3 + 7^3 + 1^3 = 371$. Therefore 371 is an Armstrong number.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

1.3 Composite Number

A composite number N is a positive integer which is not prime (i.e., which has factors other than 1 and itself). The first few composite numbers (sometimes called "composites" for short) are 4, 6, 8, 9, 10, 12, 14, 15, 16, The number 1 is a special case which is considered to be neither composite nor prime [6].

1.4 Prime Number

A prime number is a whole number greater than 1 whose only factors are 1 and itself. The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29[7].

1.5 Amicable Number

A pair of numbers is said to be amicable if the sum of all of the first number's proper divisors (excluding it) equals the second number, and vice versa. For example, the numbers 220 and 284 are friendly. The sum of 220's proper divisors is 284, which is (1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110). Similarly, the total of 284's appropriate divisors is 220, which is (1, 2, 4, 71, and 142). As a result, 220 and 284 are friendly numbers. [8].

Two numbers are called amicable if each equals the sum of the aliquot divisors of the other. The smallest pair of amicable number is 220 and 284. The sum of the aliquot divisors of 220 is 1+2+4+5+10+11+20+22+44+55+110=284 similarly; the sum of the aliquot divisors of 284 is 1+2+4+71+142=220. Therefore 220 and 284 are amicable numbers.

2. LITERATURE SURVEY

RSA, one of the most extensively used asymmetric/public key encryption algorithms, was established by Ron Rivest, Adi Shamir, and Len Adlemen in 1977.Two prime numbers are used to generate the public key and its associated private key. The letters "e" and "d" stand for public and private keys, respectively. The sender uses the public key to encrypt the message, while the recipient uses the private key to decrypt it. The algorithm's proposed steps are as follows:

1. Choose two prime numbers p and q such that p! = q.

2. Compute N=p x q

3. Compute φ(N) = (p-1) x (q-1)

4. Choose the public key e such that GCD (φ (N), e) =1; 1<e< φ (N)

5. Choose the private key d such that d x e mod φ (N) =1

6. Perform encryption by using the formula:

CT=PT ^e mod N

7. Perform decryption by using the formula:

PT=CT^d mod N

2.1 Limitations of RSA

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

The primary RSA encryption algorithm is susceptible to a number of attacks. The subsequent are few of the points which highlight the limitations of RSA;[9], [10]

A. One of the requirements of adopting RSA is that public keys associated with users be held in a trusted/authenticated manner using a public key infrastructure.
B. The private key is constantly theoretically connected to the public key in a public-key cryptosystem. As a result, retrieving the private key from the public key is simple. To prevent the retrieval of the private key from the public key, a strong defense is required in public key encryption.
C. The technique for generating keys is quite sluggish.
D. Encryption of plaintext takes a huge time.
E. The algorithm will fail if the message length exceeds the bit length.
F. To begin, RSA requires two large prime numbers, p and q, because it is a factorization-based approach.
G. If users' private keys aren't provided, it's open to impersonation.

2.2 Variants of RSA

Ravi Shankar Dhakar et al. [9] had proposed a method entitled as Modified RSA Encryption algorithm (MREA). This approach becomes more secure by taking 4 prime numbers in place of two. The complexity of decomposing the modulus into its parts increases as the length of the modulus increases. This increases the length of the private key and, as a result, the difficulty of detecting it. In this approach the author has taken one additional parameter i.e. named as multiplicative inverse denoted by μ.

$\mu=\lambda^{-1} \bmod N$----------*Eq-6*

Where, N=p x q (p and q are two prime numbers)

This additional parameter is a part of the private key which makes the brute force attack more difficult for the attacker to obtain the private key.

Aiswarya P M et al. [11] In this paper the ciphertext received after encryption is translated into binary code in this work, which offers a change to the MREA (Modified RSA Encryption Technique) algorithm. The ciphertext in the MREA technique is in decimal format, with digits ranging from 0-9. To convert these digits into binary codes maximum 4-bit pattern are required to represent a number. The author assigned binary codes to each digit and used these fixed values to translate the ciphertext digits, resulting in a binary pattern of 1s and 0s. Table 1 shows the pre-assigned codes.

Table 1: Pre-assigned codes used in MREA

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

S.No.	Ciphertext(digits)	Replaced with (Binary code)
1	0	0000
2	1	0001
3	2	0010
4	3	0011
5	4	0100
6	5	0101
7	6	0110
8	7	0111
9	8	1000
10	9	1001

Along with the ciphertext, the above-mentioned pre-assigned codes are also sent to the receiver. This will frustrate the attacker/ intruder to extract the plaintext from this binary pattern.

Alaa Hussein Al-Hamami et al. [12] had suggested an approach in which the author proposed to use three prime numbers instead of two to produce a public and its corresponding private key. This will generate the variable N (N=p*q*r) to a large value. Factorization of N is more complex as compare to N in the original RSA algorithm as N=p*q resulting frustration for the intruder in finding the 3 prime numbers. In this paper the author concluded that;

- ✓ The proposed strategy has succeeded in making the analysis of the variable N more complex.
- ✓ Increasing the speed with which keys are generated.
- ✓ It accelerates the encryption and decryption processes.

Shilpi Gupta et al.[14]had emphasis on the scope of improvement on strengthening and safeguarding the communication. In this paper the author proposed an innovative approach by mingling the two utmost extensive algorithms named as RSA and Diffie-Hellman in order to achieve added security. In the original RSA the public key is expressed as P_{PUB} = (e, N) and private key as P_{PRV} = (d, N). The algorithm in the proposed approach computes the value of "e" and "d" as in RSA after that three prime constants are generated automatically (say R, S and G).By using these values, public numbers referred as X and Y are calculated by using the following expression;

$X = G^e \bmod R$ ----------*Eq-7*

$Y = G^d \bmod R$----------*Eq-8*

Here Diffie Hellman works to compute the session key by using the following expression;

$K_A = Y^A \bmod R$----------*Eq-9*

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

$K_B = X^B \bmod R$----------*Eq-10*

Such that $K_A = K_B = K$.

Finally, in order to accomplish encryption and decryption, the sender and receiver share this key denoted as K. The plaintext is XORed with the session key (K) at the sender site to produce encryption text. At the receiver site, the plaintext was created by XORing the encrypted text with the session key (K).

Junnel E. Avestroet al. [13] proposed a hybrid method that included Modified Diffie Hellman and Rivest, Shamir, and Adelman (RSA). The classic Diffie-Hellman algorithm uses primitive root but the projected modified Diffie-Hellman uses two prime numbers for key exchange. Man-in-the-middle attacks will be limited as a result. The modified Diffie-Hellman can also use for authentication purpose, in which if the shared secret-key by the sender and receiver both are equal, communication will take place otherwise, not. The two prime numbers obtained earlier using the Modified Diffie Hellman (MDH) technique will also be used by the RSA algorithm. Encryption and decoding were carried out using these prime numbers. To overcome the problem of prime factorization of N in RSA, the suggested technique generates the value of N in a secret manner, causing the intruder to be frustrated in performing prime factorization. The proposed system modifies Diffie-Hellman to provide authentication so that key exchange can be done only with an authenticated user in a secure manner. The proposed algorithm also solves the problem of primitive root generation.

Modified key exchange algorithm is divided into two sections in the suggested technique. The initial part is the key exchange for the MDH algorithm. The final part is that it encrypts and decrypts the message using the RSA technique, but both sides produce two keys using the RSA approach, which is referred to as the sender key for encryption and the receiver key for decrypting incoming messages.

S. Pavithra Deepa et al. [3] had proposed a method to encrypt data using the RGB color and Armstrong number. In this approach, each color has a set of intensity values corresponding to every color such as Pink (255,192,203) assigned to each user as well as every user will have a key value. The key value comprises of three integer values such as (+10, -5, -5). Color value and key value will be known to everyone same as public key. Armstrong number will be selected randomly to be treated as private key.

Encryption:

If the sender wants to send a message to any receiver, the receiver's color value is added to the sender's key value. The calculated value will be sent to the reviver for user authentication. The ASCII value of the Plaintext characters will be added to the Armstrong number pattern by the sender (i.e. by separating each digit of selected Armstrong number, then square of each digit, then cube of each digit and again repeating the pattern as digits, squares and cubes and so on.). 153 is one of an Armstrong number, so 1, 5, 3, 1, 25, 9, 1, 125, 27, 1, 5, 3, and so on.

The resultant will be converted into a matrix form (say A). An encoding matrix gets generated by using the selected Armstrong number (say B). Calculate the product of both matrixes to

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

generate matrix C. The final resultant values will be considered as the ciphertext values.

Decryption:

To begin, the user's identity will be verified by subtracting the key value from the color value provided. To perform the decryption first calculate the inverse matrix (say D) of encoding matrix (say B) and it will be multiplied with encrypted matrix (say C). Now subtract the pattern of Armstrong number from the resulting matrix values. Finally convert the ASCII equivalents of the resultant value to obtain the plaintext.

J Gitanjali et al. [4] had proposed a method to encrypt data using ASCII values and Palindrome numbers. In this approach every user has a unique alphanumeric id comprises of 3 alphabets and 1 number. All the ids are stored in the database.

The Encryption process has the following steps;

In step-I a key comprises of 4 numbers is generated randomly at the sender site. While sending the data to an intended receiver, this value is get added to the ASCII equivalent of the alphanumeric key of that receiver. The resultant value is used for user authentication while decrypting the ciphertext.

In step-2 the selection of Palindrome number is done by adding the numbers of the resultant value. Now pick the Palindrome number nearest to the sum.

Unique alphanumeric id	S	R	P	I
ASCII equivalent	83	82	80	49
Random key	8	7	14	11

Resultant value	91	89	94	60

Sum of numbers to select Palindrome number 91 + 89 + 94 + 60 = 334

The closest palindrome to 334 is 343. The original data is encrypted using this number. The digits of selected palindrome number is used to form a matrix (A) called as encoding matrix by using the following expressions;

First Row	a=3	b=4	c=3
Second Row	(a+1)*3	(b+3)*4	(c+5)*3
Third Row	((a+1)*3)*3	((b+3)*4)*4	((c+5)*3)*3

In step-3 we take the original data as Plaintext and convert each alphabet of it into its ASCII equivalent after that we create a matrix (B) by using the ASCII numbers.

In step 4, we combine the column components of matrix B with the row elements of matrix A to form Matrix-C. Now multiply A by C to get the Matrix-D cipher values. In the process of

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

Decryption, the receiver is first authenticated after receiving the encrypted data and key. It's done by subtracting random numbers from the key (produced by the sender). After the successful authentication the decoding matrix (F) is created by performing multiplicative inverse of encoding matrix (A) is calculated. Now multiply F and A producing another matrix (G). The final matrix (H) is obtained by subtracting the row of E from the columns of G, which is the ASCII equivalent of the original text or plaintext. Hegadi Rajendra et al. [15] had proposed a method to encrypt data using prime and composite numbers. The Encryption process has the following steps;

In this approach three prime numbers are taken and compute a composite number (n) using Euler's Totient function. We have a commutative group N after computing a composite number, which is a collection of all integers from 1 to that composite number. In this group we exclude those integers which are multiples of selected prime numbers. The group (G) is now partitioned into integer blocks. Each block has a size of 26 integers. The following table shows the first block by taking 7, 7 and 11 as prime numbers and commutative group G as below:

G = {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25, ...538, 539}.

This group has 539-(49+77-7) = 420 integers out of which we exclude 1 and 538 as their inverse are themselves. So finally, we have 418 integers in the group.

Table 2: Mapping of integers with inverse integer and alphabets [15]

N	Alphabet	Inverse Integer (Mod 539)	Inverse Alphabet	Block Number
2	A	270	B	B9
3	B	180	J	B6
4	C	135	Z	B4
5	D	108	F	B4
6	E	90	R	B3
8	F	337	B	B11
9	G	60	T	B2
10	H	54	P	B2
12	I	45	H	B2
13	J	83	M	B3
15	K	36	A	B2
16	L	438	C	B14
17	M	222	P	B7
18	N	30	W	B1
19	O	227	T	B7
20	P	27	U	B1
23	Q	375	E	B12
24	R	292	S	B9
25	S	345	H	B11
26	T	311	H	B10
27	U	20	P	B1
29	V	316	L	B10
30	W	18	N	B1
31	X	313	J	B10

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

32	Y	219	N	B7
34	Z	111	H	B4

In Table 2 each column has the following information-

Col-1: Block-B1 is assigned a set of integers from G.

Col-2: Alphabet has a one-to-one correspondence with numbers.

Col-3: Under modulo n, the corresponding inverse integers from N

Col-4: The inverse alphabet for the matching alphabet.

Col-5: The inverse integers and inverse alphabets belong to the Block numbers.

Let us consider a plaintext JERRY. To encrypt it, each letter of plaintext must be associated with a different block in a random order, such as,

J→B1, E→ B3, R→ B7, R→ B9 and Y→ b16

The following table shows the encryption process of the plaintext as;

Table 3: Encryption of plaintext [15]

Plaintext Alphabets	**J**	**E**	**R**	**R**	**Y**
Block Number (Random Association)	B1	B3	B7	B9	B16
Associated Integer	13	74	225	257	534
Inverse Integer (mod 539)	83	51	218	388	431
Block Number of Inverse Integer	B3	B2	B7	B12	B13
Inverse Alphabet (Ciphertext)	M	M	M	W	W

For decryption the receiver must have cipher characters, associated integers and the computed composite number.

In this paper following points are not clear;

1. When the composite number is large it is difficult to perform prime factorization for the receiver.
2. While performing encryption random association of block number is useless.
3. If a plaintext is encrypted is encrypted using only one block, then there will be no need of using Block number.
4. Encryption using only a single block doesn't frustrate attacker to decipher it.

Mandal J. K et al [16] had proposed a cryptographic algorithm named as FBPS (Fibonacci based Position Substitution) encoder for data encipherment using Fibonacci series. This algorithm takes the data and convert it into binary pattern, the stream of bits is then divided into M-blocks of a fixed size (say n-bits). Each block is converted into its decimal equivalent, then the algorithm will find the position of that decimal number in the series. The position (say P) is then used to find the target value (say V) using the following expression;

$F_{P-1} <= V < F_P$----------*Eq-11*

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

If the above condition is satisfied the algorithm computes the next target value by using the following expression;

$V = V - F_{P-2}$----------*Eq-12*

If $V<F_{P-2}$ the cipher bit will be 0 else 1. This will continue until V is reached to 0 or 1. As soon as the value of V reached to 0 or 1 the algorithm will collect all the bits from bottom to top as a cipher bit for the first block. Similarly, FBPS is applied on all the remaining blocks to compute the corresponding ciphertext.

Let suppose $C = C_0C_1C_2$ .....C_{T-1} is a block in the ciphertext, where the size denoted by T is obtained from secret key. In decryption, bit C_0 is used to initialize V, and then the value of V is appended with F_N. Otherwise; V is appended with F_{N-1} if the next cipher bit is 0. The stream containing the plaintext of the encrypted block is generated by the final value of V.

Das.Ret al, [8] had projected a scheme to encrypt data using Amicable numbers. Distribution of private key in public key cryptographic systems is a crucial job. Such systems require a high level of security for the distribution of private key through communication channels. As a result, apart from safeguarding the real private-key, the author focuses on an undiscovered technique for generating a secret value from a private-key that can be utilized for encryption. The secret value is generated by selecting the first or second number from the N^{th} pair of the amicable number set. N is a positive integer that falls inside the range (N=1 to 1024) that is defined by the user. Starting with a user-defined value called Base Value; the selection of the N^{th} pair of amicable numbers is made in either a forward or backward manner, with the user-input determining the direction of travel.

A user-defined order is imposed for storing encrypted characters block by block in the ciphertext file, providing additional security because the base value, forward or backward movement, and Nth term used to compute amicable number are all user-defined, changing any of these factors will result in a new amicable number that can be used as a secret value for encryption. Furthermore, because user-defined cipher block sequencing techniques are employed, encrypted character positioning in the ciphertext file differs from that of the plaintext file. The following table lists the various cipher block sequencing techniques:

Table 4: Techniques for Sequencing Cipher Blocks [8]

Value	Term	Sequencing Techniques Definition
0(00)	Exchange Even From Right (EEFR)	Starting from the right end, characters from even numbered blocks are exchanged. The characters in the odd-numbered blocks are in the similar order in the ultimate encrypted file.
1(01)	Exchange Even From Left (EEFL)	Starting from the left end, characters from even numbered blocks are swapped. The characters in the odd-numbered blocks are in the similar order in the ultimate encrypted file.
2(10)	Exchange Odd From Right (EOFR)	Starting at the right end, characters from odd numbered blocks are exchanged. The characters in the even-numbered blocks are in the similar order in the ultimate encrypted file.
3(11)	Exchange Even From Left (EOFL)	Starting from the left end, characters from odd numbered blocks are switched. The characters in the even-numbered blocks are in the

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

		similar order in the ultimate encrypted file.

3. EXPERIMENTAL OUTCOME AND RESULTS

3.1 Comparative study of cryptographic algorithms based on Mathematical numbers.

Table 5 illustrates the summarized comparative study of cryptographic algorithms discussed in this paper.

Table 5: Comparative study of Cryptographic Algorithms

Parameters/ Algorithm	Published	Proposed by	Mathematical Number used	Stream/ Block	Symmetric/Asymmetric	Mathematical Operations
RSA	1977	Ron Rivest, Adi Shamir, Len Adlemaen	Prime Number	Block	Asymmetric	Multiplication, ModularExponentiation
Prime and Composite No.	2007	RajendraHegadi,MuppinaiyaNagaraj	Prime and Composite Number	Block	Symmetric	Multiplicative Inverse, Modulus
Fibonacci No.	2009	J. K. Mandal, Mangalmay Das	Fibonacci Numbers	Block	Symmetric	Block genertator,Decimal value selection
Armstrong Nnumber with RGB	2011	S. PavithraDeepa, S. Kannimuthu, V. Keerthika	Armstrong Number	Stream	Symmetric	Color assignment,Key value assignment, Matrix multiplication
MREA	2012	Ravi Shankar Dhakar, Amit Kumar Gupta,Prashant Sharma	Prime Number	Block	Asymmetric	Modular Exponentiation, Modular multiplicative inverse
RSA with 3 Prime Numbers	2012	Prof.Dr.Alaa Hussein Al-Hamami, IbrahemAbdallahAldarise h	Prime Number	Block	Asymmetric	Modular Exponentiation, GCD
RSA with Diffie-Hellman[Shilpi Gupta et al]	2012	Shilpi Gupta, Jaya Sharma	Prime Number	Block	Both	Modular Exponentiation, XOR
Palindrome No. with ASCII values	2014	J Gitanjali , Dr.N.Jeyanthi,C.Ranichandra,M.Pounambal	Palindrome Number	Stream	Symmetric	Matrix Multiplication, ASCII conversion
BREA	2016	Aiswarya P	Prime Number	Block	Asymmetric	Multiplicative

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

		M, Archana Raj, Dona John				inverse, Modular Exponentiation, Binary conversion
AmicableNo.	2018	R. Das, S.Dutta	Amiable Number	Block	Both	Selection of Amicable No., Transposition, XOR, ASCII conversion
RSA with Diffie-Hellman[Junnel E. Avestro et al]	2019	Junnel E. Avestro, Ariel M. Sison, Ruji P. Medina	Prime Numbers	Block	Both	

The proposed work has taken prime numbers (required for existing algorithm e.g., RSA require 2 prime numbers and so on.) and tested for 3 sets of inputs considering key generation time, encryption time, decryption time and total time in seconds. Table 6 shows the simulation results of various cryptographic algorithms.

Table 6: Simulation Results of various Cryptographic Algorithms

SN	Algo- rithm	Prime-1	Prime-2	Prime-3	Prime- 4	Key Generation Time (Sec)	Encryption Time (Sec)	Decryption Time (Sec)	Total time (Sec)
1	RSA	2971	4013	N/A	N/A	0.144589	0.110299	0.091213	0.346101
		2543	3347	N/A	N/A	0.137316	0.119691	0.098761	0.355768
		3413	3671	N/A	N/A	0.121129	0.124101	0.100889	0.346119
2	MREA	53	131	397	563	0.484108	0,329221	0.126211	0.610319
		67	151	599	773	0.172133	1.672016	0.485363	2.329512
		101	277	607	911	0.172134	0.890882	0.385736	1.448752
3	BREA	59	137	401	569	0.441288	0,282291	0.162821	0.604109
		71	157	601	787	0.163216	1.581629	0.286753	2.031598
		103	281	613	919	0.153483	0.709269	0.487636	1.350388
4	ERSA	137	139	149	N/A	0.109175	0.115445	0.095505	0.320125
		151	191	233	N/A	0.119178	0.112147	0.093591	0.324916
		167	211	251	N/A	0.137658	0.107731	0.089468	0.334857
5	HRSA	43	47	53	61	0.201587	0.041137	0.037679	0.280403
		41	47	53	59	0.211045	0.038338	0.033949	0.283332
		43	47	59	61	0.238035	0.033983	0.028657	0.300675

On the basis of the values of different parameters (key generation time, encryption time and decryption time) as shown in Table 6. Average values of these parameters for above mentioned algorithms are calculated and shown in the Table 7.

ISSN 1533-9211

DOI 10.17605/OSF.IO/8ZRTW

Table 7: Average values of Simulation Results

Algorithm	Average Key Generation Time	Average Encryption Time	Average Decryption Time
RSA	0.13434	0.11803	0.096954
MREA	0.27613	0.8543	0.332437
BREA	0.25266	0.76363	0.312403
ERSA	0.122	0.11177	0.092855
HRSA	0.21689	0.03782	0.033428

The graphical representation of the average key generation time for several techniques is shown in Figure 2. The graph shows unequivocally that ERSA takes the shortest amount of time to generate keys when compared to other algorithms.

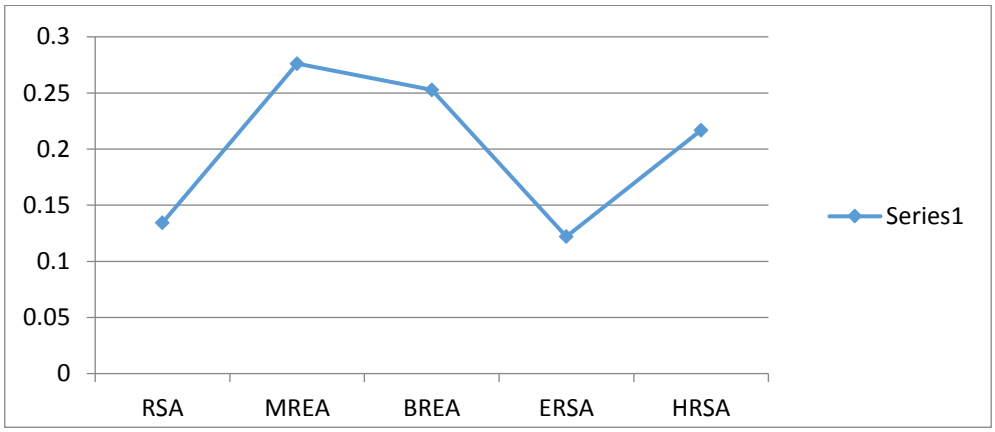
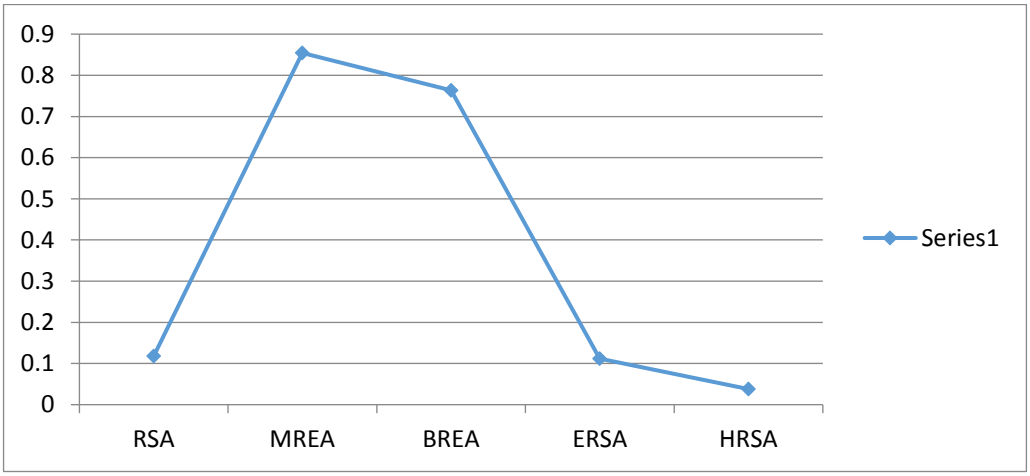


Figure 2: Average Key Generation time

Figure 3 shows the graphical representation of average encryption time of different algorithms. The graph clearly represents that the encryption time of HRSA is minimum as compared to other algorithms.



ISSN 1533-9211

DOI 10.17605/OSF.IO/8ZRTW

Figure 3: Average Encryption time

The graphical depiction of the average decryption time for various algorithms is shown in Figure 4. The graph shows unequivocally that HRSA takes the least amount of time to decipher data as compared to other algorithms.

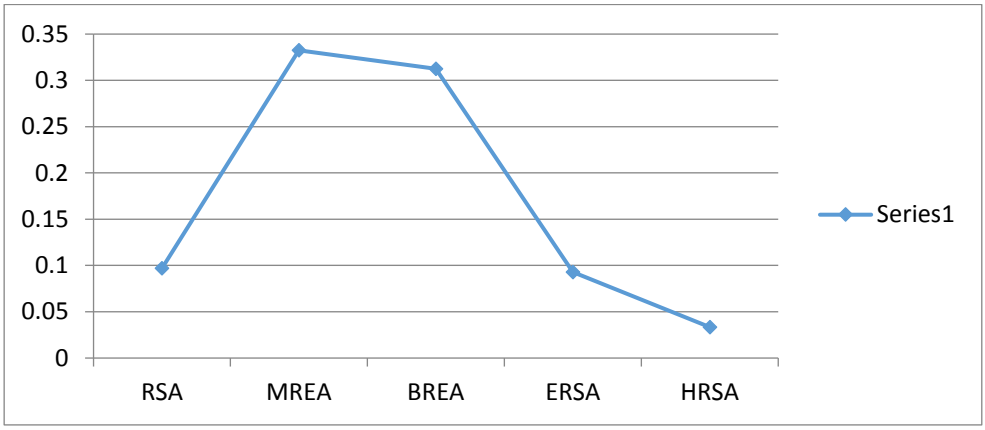


Figure 4: Average Decryption time

4. CONCLUSION AND FUTURE SCOPE

According to the analysis above, it can be inferred that the HRSA algorithm performs better than other algorithms in terms of encryption time and decryption time, whereas ERSA performs better in terms of key generation time. It may be said that none of the aforementioned algorithms performs best across the board.

These algorithms are most suitable while working on prime numbers. There are other mathematical numbers can also be used instead of prime numbers. Cryptographic cipher techniques usually use prime numbers among the different mathematical numbers. In future other numbers e.g. Amicable number (which are less explored) also can be used instead of prime numbers which can give better results.

References

1) William Stallings.2011. Cryptography and Network Security Principles and Practice, 5th Edition.Pearson Education.

2) Ramesh Yegireddi, R Kiran Kumar, "A survey on conventional encryption algorithms of Cryptography," 2016(IEEE) International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-4, doi: 10.1109/ICTBIG.2016.7892684.

3) S. PavithraDeepa,S. Kannimuthu, V. Keerthika., "*Security Using Colors and Armstrong Numbers*", Proceedings of the National Conference on Innovations in Emerging Technology, 17 & 18 February, 2011.pp.157-160

4) J. Gitanjali, N. Jeyanthi, C. Ranichandra and M. Pounambal, "ASCIi based cryptography using unique id, matrix multiplication and palindrome number," The 2014 International Symposium on Networks, Computers and Communications, Hammamet, 2014, pp. 1-3, doi: 10.1109/SNCC.2014.6866509.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/8ZRTW

5) https://pages.mtu.edu/~shene/COURSES/cs201/NOTES/chap04/arms.html.

6) https://mathworld.wolfram.com/CompositeNumber.html.

7) https://whatis.techtarget.com/definition/prime-number.

8) R. Das, S. Dutta, *"A Private Key Encryption Scheme based on Amicable Number with User defined Cipher Block Sequencing Techniques,"*International Journal of Computer Sciences and Engineering, Vol.6, Issue.5, pp.34-41, 2018.

9) Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). "Modified RSA Encryption Algorithm (MREA)". In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 426-429). IEEE.

10) AjitKarki, "A Comparative Analysis of Public Key Cryptography". International Journal of Modern Computer Science (IJMCS) ISSN: 2320-7868 (Online) Volume 4, Issue 6, December, 2016

11) P. M. Aiswarya, A. Raj, D. John, L. Martin, and G. Sreenu, "Binary RSA encryption algorithm," 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, 2016, pp. 178-181.

12) Al-Hamami, A. H., &Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408).

13) Junnel E. Avestro, Ariel M. Sison, Ruji P. Medina, 2019 IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E) Bali, Indonesia, November 13-15, 2019

14) Gupta, S., & Sharma, J. A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman. 978-0-7695-4587-5/11.

15) Rajendra Hegad Muppinaiya Nagaraj, Shamshekhar S Patil, "Encryption and Decryption Process Using Composite Numbers". Ijcsns International Journal of Computer Science and Network Security, Vol.7 No.1, January 2007

16) J. K. Mandal and Mangalmay Das, "Fibonacci Based Position Substitution (FBPS) Encoder for Secured Message Transmission", IEEE International Advance Computing Conference (IACC) Patiala, India, pp.964-970, 6-7 March 2009.