Conference Proceeding Science and Technology, 3(2), 2020, 247–251

Conference Proceeding of 9th International Eurasian Conference on Mathematical Sciences and Applications (IECMSA-2020).

ISSN: 2651-544X
http://dergipark.gov.tr/cpost

On Excellent Safe Primary Numbers and Encryption

Nazlı Koca^{1,*} *Serpil Halıcı*^{2}

[1] Pamukkale Uni., Depart. of Math. Denizli,Turkey, ORCID: 0000-0002-4663-6253
[2] Pamukkale Uni., Depart. of Math. Denizli,Turkey, ORCID: 0000-0002-8071-0437
** Corresponding Author E-mail: nkoca17@posta.pau.edu.tr*

Abstract: In this study, we firstly included the definition of perfectly safe prime numbers that we created. We then examined the RSA and Rabin cryptosystem, which are the techniques of implementing prime numbers in encrypting any message. Finally, we used these perfectly safe prime numbers, which were first defined, in RSA and Rabin's encryption methodsssss.

Keywords: Prime Numbers, Distribution of Primes, Applications of Prime Numbers.

1 Introduction and Preliminaries

Prime numbers are also used to send encrypted messages in the field Cryptography in the past and today. In cryptography, each user has two different keys, one open and one secret for encryption and decryption. The public key is public and anyone can see it. The secret key is kept confidential and should not be known to anyone other than its owner. Encryption is done with a public key, while the decryption is done with a private key. These encryption keys are used in binary and the other key decodes the information that one encrypts. The most known and used encryption method today is the RSA encryption method, the public key encryption method. The name of this system carries the surnames of scientists named Ron Rivest, Adi Shamir and Leonard Adlemen in 1978, namely the method was named after factoring the integers [1]. Another public key encryption method is Rabin's encryption technique. The Rabin's encryption method is a crypto system found in 1979 by Michael Rabin. This cryptosystem is based on the asymmetric encryption technique. Rabin's cryptosystem, which is a different type of RSA method, takes advantage of the difficulty of factoring the compound numbers as in RSA [2].In this study, we will start with the definition of perfectly safe prime numbers that we will use in encryption with prime numbers. Then we will use the perfect numbers that we have created in RSA and Rabin encryptions.

Definition 1. *When applying the formula $\frac{(k-1)}{2}$ for $k > 0$ and $k \in \mathbb{Z}^+$ the lower row number of k is obtained.*

For example, the lower row number of 17 is 8.

Definition 2. *When applying the formula $\frac{(k+1)}{2}$ for $k > 0$ and $k \in \mathbb{Z}^+$ the upper row number of k is obtained.*

For example, the upper row number of 21 is 11.

Definition 3. *Let p be the prime number. So that if p's lower row number and upper row number is prime number, p number is called perfect safe prime number.*

For example, $p = 5$ prime number is six row number 2 and top row number is 7. So, $p = 5$ is the perfect safe prime number, since the lower row number and the upper row number are prime. Some perfectly safe prime numbers are: $5, 11, 23, 83, 179, 359, 719, \cdots$.
In the table 1.2 below, consecutive odd numbers are given in the white region. The upper row numbers are written on the odd numbers in this white section. To the next higher row, the upper row number of the number written below will be written. Also, the lower row number of these numbers is written in the lower part of the numbers in the white part. If the result is an even number when writing down the lower row number, it is not continued. Because we will do our operations on odd numbers. Numbers indicated in red are prime numbers. The prime number in the middle of 3 consecutive prime numbers constitutes perfectly safe prime numbers. We highlighted the perfectly safe prime number in green.

255	383	511	639	767	895	1023	1151	1279	1407	1535	1663	1791
127	191	255	319	383	447	511	575	639	703	767	831	895
63	95	127	159	191	223	255	287	319	351	383	415	447
31	47	63	79	95	111	127	143	159	175	191	207	223
15	23	31	39	47	55	63	71	79	87	95	103	111
7	11	15	19	23	27	31	35	39	43	47	51	55
3	5	7	9	11	13	15	17	19	21	23	25	27
1	2	3	4	5	6	7	8	9	10	11	12	13
		1		2		3		4		5		6
						1				2		

Table 1.1 Perfect safe prime numbers

1919	2047	2175	2303	2431	2559	2687	2815	2943	3071	3199	3327	3479
959	1023	1087	1151	1215	1279	1343	1407	1471	1535	1599	1663	1739
479	511	543	575	607	639	671	703	735	767	799	831	869
239	255	271	287	303	319	335	351	367	383	399	415	431
119	127	135	143	151	159	167	175	183	191	199	207	215
59	63	67	71	75	79	83	87	91	95	99	103	107
29	31	33	35	37	39	41	43	45	47	49	51	53
14	15	16	17	18	19	20	21	22	23	24	25	26
	7		8		9		10		11		12	
	3				4				5			
	1								2			

Table 1.2 Perfect safe prime numbers

Let's give the above table with the following theorem.

Theorem 1. *Perfect numbers are increasing rapidly as prime numbers progress irregularly.*

From here we can say that it is not easy to reach Perfect prime numbers.
In the following sections, we will use this feature of perfect numbers to use to encrypt messages. Modular mathematics is used in the RSA algorithm. Below we n ,coutline the RSA algorithm.

2 Encryption with Primary Numbers

Public Key Generation Algorithm. Each person A creates their public key as follows:
Selects two prime numbers, p and q, which are different, random and have the same number of digits. Calculates $n = pq$ and $\varphi = (p-1) \times (q-1)$.
Selects a random c number such that $1 < c < \varphi$ and $(c, \varphi(n)) = 1$. Using the Euclidean algorithm, it calculates the number d satisfying the condition.
$1 < d < \varphi(n)$ and $cd \equiv 1(mod\varphi(n))$
Person A has a public key (n, c) and his secret key becomes d.
So, encryption can generally be given as follows: The pair $(n, c)$the public key, is known to the person sending the information.
The explicit text is converted to an integer such that $M \in [0, n-1]$.
The encrypted text is calculated as $C \equiv M^c\,(modn)$.The person sending the information sends the C encrypted text to the person receiving the information [3].

PLAIN TEXT ⇒ ENCRYPTION ⇒ ENCRYPED TEXT ⇒ DECODING ⇒ PLAIN TEXT

Algorithm 2.1 Encryption and decryption algorithm

The flow chart for the RSA algorithm is given in the figure below.

SENDER
⇓
OPEN TEXT (M)
⇓
NUMBER BLOCKS $(M_1, M_2, ...)$
⇓
ENCRYPED TEXT $C_1 \equiv M_1^e modn \quad C_2 \equiv M_2^e modn$
⇓
DECODED TEXT M_1≡ C_1^e mod n M_2≡ C_2^e mod n
⇓
RECEIVER
⇓
RANDOM NUMBER (e)
HIDDEN KEY$\hookleftarrow$ $\hookrightarrow$ OPEN KEY

Algorithm 2.2 Flow Chart of RSA Algorithm

Encryption Algorithm. If person B wants to send an m message to A, person B does the following to encrypt the message m:

- First, he learns the public key (n, e) of person A.
- Writes the message m in the range $[0, n-1]$.
- Then it calculates

$C \equiv M^c \ (modn)$.

- Sends the formed C password to person A.

To find clear text from encrypted C text, person A does the following:

- By using the secret key d and executing $m \equiv cd(modn)$, m reaches the open text [4].

For example, choose prime numbers $p = 11$, $q = 17$.

Then, $n = 11 \times 17 = 187$ and $\varphi(n) = (11-1)(17-1) = 160$ For $1 < c < \varphi(n)$, choose $c = 3$. And let $d = 107$ satisfy $dc \equiv 1(mod\varphi(n))$. According to this, $dc \equiv 321 \equiv 1(mod\varphi(n))$.

Definition 4. *Let p be the prime number. So that if p is the number of the previous row and the number of next row is the prime number, p number is called the perfect safe prime number.*

For example, p is the perfectly safe prime number since $p = 5$ is the prime number, and the next 7 is the prime number. Some perfectly safe prime numbers are 5, 11, 23, 83, 179, 359, 719,...

3 RSA Method and Perfect Prime Numbers

Now, in this section, an application of the RSA security algorithm for perfectly safe prime numbers will be given. Let p and q be two consecutive perfectly safe prime numbers: $p = 11, q = 23$ then we write $n = (2q+1)(2q+1) = 23.47 = 1081$ $\varphi(n)$=$\frac{(p-1)}{2} \times \frac{(q-1)}{2}$= 5 × 11=55. Let's choose a random number e. And $e = 19$ with $1 < e < n$ and $(e, \varphi(n)) = 1$. $d = 29$ can be taken as a number that satisfies $de \equiv 1(mod\varphi(n))$. Since, $de \equiv 551 \equiv 1(mod\varphi(n))$ the public key becomes $(n, e) = (1081, 19)$. Thus, the closed key is $(n, d) = (1081, 29)$.
As a example let us choose $p = 5, q = 11$ consecutive perfectly safe prime numbers. $n = (2p+1) \times (2q+1) = 253$ $\varphi(n) = \frac{(p-1)}{2}. \frac{(q-1)}{2} = 10$.
Let's choose a random number e. Let this number be prime between $1 < e < n$ and $(e, \varphi(n)) = 1$. If we take $e = 3$, then we have $de \equiv 1(mod\varphi(n)), d = 7$ and $de = 21 \equiv 1(mod\varphi(n))$. The public key is
$(n, e) = (253, 3)$ and the closed key is $(n, e) = (253, 7)$.
Now, let the text you want to send be "SIFRE". If the letters are numbered respectively,$S = 1$, $I = 2$, $F = 3$, $R = 4$, $E = 5$. The person to whom the message will be sent and anyone who reads the message is given the numbers n calculated above and randomly selected e. Calculation is made according to
$e = 3$ and $(mod10)$ for $SIFRE = 12345$.

$$\begin{gathered}1^3 \equiv 1 \ (mod10)\\ 2^3 \equiv 8 \ (mod10)\\ 3^3 \equiv 7 \ (mod10)\\ 4^3 \equiv 4 \ (mod10)\\ 5^3 \equiv 5 \ (mod10).\end{gathered}$$

So the password to be sent will be 18745. Deciphering is completed by converting this number into "SIFRE" text using our codes. For example, letters are matched to numbers between integer values in $[0, \varphi(n-1)]$.

A	I	K	M	N	O	R	S	U	Y
0	1	2	3	4	5	6	7	8	9

Table 3.1 Encryption table of some letters.

To be able to send a message using the letters we have numbered above, let's encrypt our message first. We find the values required for encryption as $\varphi(n) = 10$ and $e = 3$.

$Message$	M	I	R	A	Y	K	O	N	U	S	U	Y	O	R
$Number\,Value$	3	1	6	0	9	2	5	4	8	7	8	9	5	6
$Power\ of\ e$	3^3	1^3	6^3	0^3	9^3	2^3	5^3	4^3	8^3	7^3	8^3	9^3	5^3	6^3
$Value$	27	1	216	0	729	8	125	64	512	343	512	729	125	216
$Remaining$	7	1	6	0	9	8	5	4	2	3	2	9	5	6
$Password\ message$	S	I	R	A	Y	U	O	N	K	M	K	Y	O	R

Table 3.2 message encryption table.

The person who receives our encrypted message will do the following to turn this message into understandable text.

$Password\ message$	S	I	R	A	Y	U	O	N	K	M	K	Y	O	R
$Power\ of\ d$	7^7	1^7	6^7	0^7	9^7	8^7	5^7	4^7	2^7	3^7	2^7	9^7	5^7	6^7
$Value$	27	1	216	0	729	8	125	64	512	343	512	729	125	216
$Remaining$	3	1	6	0	9	2	5	4	8	7	8	9	5	6
$Message$	M	I	R	A	Y	K	O	N	U	S	U	Y	O	R

Table 3.3 encryption message decoding.

It should be noted that for open the encrypted message we need to know the secret key $d = 7$.
In the section below, we have examined a different encryption method using the special prime numbers we have defined.

Rabin's Encryption Algorithm. This method is a cryptosystem method given by Michael Rabin in 1979. This cryptosystem is an asymmetric encryption technique. The Rabin's cryptosystem is a version of RSA. But there are some differences between them. Some of these are given below.
It is a great advantage over RSA that it is not easy for any text in the Rabin's cryptosystem to be able to obtain the encrypted text by someone who can factor only the n public key. The decoding of the Rabin cryptosystem proved to be equivalent to the factor of dividing integers. Therefore, the Rabin method is safer than the RSA method. When $e = 3$ is taken, there is a modular multiplication and a modular squared operation in the RSA method. However, since there is only one modular squaring process in the Rabin method, the processes are faster than the RSA method [2]. The disadvantage of the Rabin's cryptosystem is difficult to find out which of the four different keys is correct. This is a disadvantage compared to the RSA method, although it is attempted to select the correct output with the addition method [3].

The key generation in the Rabin cryptosystem is done as follows:
Approximately the same size, large and random p, q prime numbers are selected. $n = p \times q$ is calculated. Therefore, the number n is the public key and the (p, q) ordered pair is the secret key. When encrypting in the Rabin's cryptosystem method, someone who wants to encrypt the m message is created with the number m not less than n. The sender's public key is reached. And the equivalence of $c \equiv m^2(modn)$ is calculated. The sender sends the encrypted c message to the person he wants.
Password decoding with the Rabin's cryptosystem method is done as follows:
The person receiving the encrypted message calculates the m value using his private key.
Accordingly, there are two solutions of m_p and m_q . Using the extended Euclidean algorithm, $y_p \times p + y_q \times q = 1$ is calculated. Then the roots of m_1, m_2, m_3, m_4 are calculated as follows.
$m_1 = (y_p \times p \times m_q + m_q \times q \times m_p)(modn)$, $m_2 = n - m_1$, $m_3 = (y_p.p.m_q - m_q.q.m_p)(modn)$, $m_4 = n - m_3$

Here, one of the roots m_1, m_2, m_3, m_4 is the key for us to open the sent text. For example, for person A key generation; $p = 277$and $q = 331$
by choosing the prime numbers, he finds $n = 91687$. The public key of person A is $n = 91687$ and the secret key is $p = 277$, $q = 331$. For the encryption process, the message of person A to be encrypted is $m = 40569$. Then, $c \equiv 40569^2(mod91687) = 62111$ is obtained. This found c message is sent to person B.

Decryption. Person B calculates c encrypted text with $n = 91687$ public key, four square roots of c according to $(modn)$ The following four roots are available from different roots:
$m_1 = 69654$, $m_2 = 22033$, $m_3 = 40569$, $m_4 = 51118$.
Here m_3 opens the message c, which is the encrypted text, and reaches the original, real message. Let's examine the Rabin's method using the perfect prime numbers in the example below:
Our message to be encrypted: get MRY.

M	1
I	0
R	5
A	7
y	8

Table 3.4 Coding table of some letters.

We matched the letters with the numbers we chose arbitrarily. Now let's choose perfectly safe primes $p = 11$ and $q = 23$. From here, $n = p.q = 253$. Our public key is $n = 253$, and our private key is $(p, q) = (11, 23)$.

Let's choose the number m as $m = 158$ so that $m < n$. So, $c \equiv 158^2(mod253) = 170$.

Our secret message we send is MAI. The recipient of our secret message with MAI, using his public key, $n = 253$ $m_{11} \equiv 170^{\frac{(11+1)}{4}}(mod11) = 4$ and $m_{23} \equiv 170^{\frac{(23+1)}{4}}(mod23) = 3$ finds their numbers. Using the extended Euclidean algorithm, $y_p \times p + y_q \times q = 1$. There are unknown things from equality:

$y_p = -2$, $y_q = 1$. The roots are follows:

$m_1 = (-2 \times 11 \times 3 + 1 \times 23 \times 4)(mod253) = 26$,

$m_2 = 253 - 26 = 227$,

$m_3 = (-2 \times 11 \times 3 - 1 \times 23 \times 4)(mod253) = 95$,

$m_4 = 253 - 95 = 158$.

The root that opens the real message here is the number m_4. So, our encrypted MAI secret message is calculated by the public key, $n = 253$, the actual message $m_4 = 158$ found; MRY opens.

4 Conclusions

As a result, we have created perfectly safe prime numbers by taking advantage of the irregular progression of the prime numbers. Thus, we used the perfectly secure prime numbers we obtained in RSA and RABIN cryptosystems and thus made encryption more secure.

5 References

1 Akbar, A. A., *Asal Sayıların Sifreleme Teorisindeki Uygulamalari*, Yüksek Lisans Tezi, Atatürk Uni. Fen Bil. Enst., Erzurum, (2015).

2 http://bilgisayarkavramlari.sadievrenseker.com, 2009, **6**(4), /rabin-sifreleme. $1.06.2020$.

3 Beskirli, A., Ozdemir, D., Beskirli, M., *Sifreleme Yontemleri ve RSA Algoritması Uzerine Bir Inceleme*, Avrupa Bilim ve Teknoloji Derg., Ozel sayi, 2019, 284-291.

4 Zuckerman, H.S., Niven, I. And Monygomery H.L., *An Introduction To The Theory Of Numbers*, New York: John Wiley Sons, 1991, 25-26.