Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2021 -22 Autumn

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: January 10, 2022

Assignment Submission Date: January 9, 2022

Word Count: 3725

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table of Figures

Abstract

Security techniques such as RSA are significant for communications because they provide secure data transmissions to enterprises, organizations, and individuals all over the world who require to communicate with each other for their everyday job. Friends among different organizations, who may be from different societies or even countries need to communicate with each other on a regular basis. To ensure security during transmission, the data should essentially be encrypted. As a result, the current research article leads to a unique security method for a cryptographic algorithm. This research explores the value of cryptography and emphasizes on the evolution of RSA, and raises the algorithm's difficulty to enhance security in operations where it may be used.

1. Introduction to Information Security

Security can be defined as the state of being safe from potential risks or threats. It is the state of being protected from various kinds of danger. The need for organizations to maintain secure operations of the systems has increased due to the various technical advances and the creation of internet. This is because the risk of data being stolen or damaged is very high when it can be accessed through the internet as various malicious users from the company as well as external attackers could access and modify the data using various tools and methods. The information is one of the most valuable assets of an organization. It needs to be safeguarded from any threats and vulnerabilities which may damage or destroy it. The methods and techniques created and deployed to secure critical company information against modification, disruption, destruction and observation are referred to as information security or InfoSec

The three critical components which must be there to maintain information security of assets in an enterprise are confidentiality, integrity and availability.

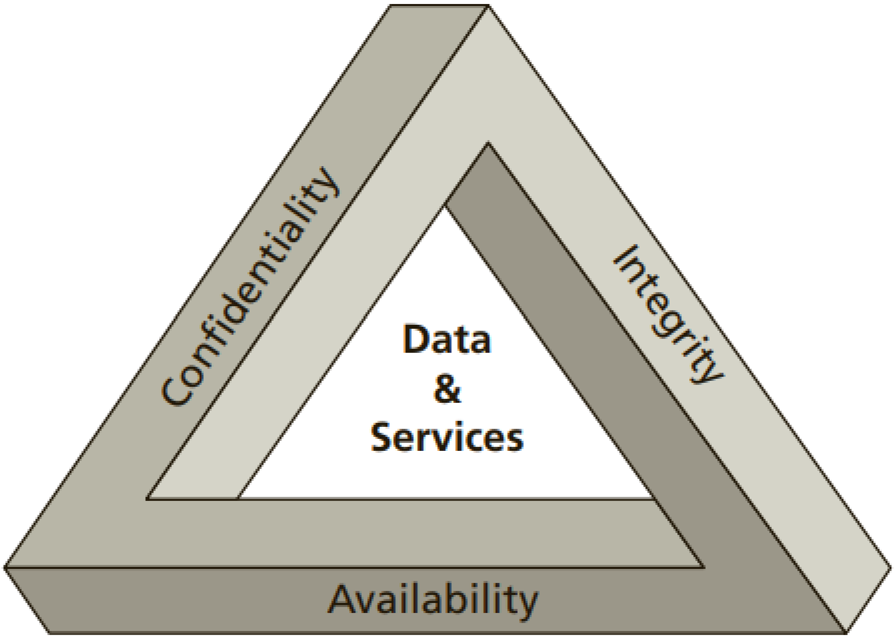


Figure 1: CIA Triad

(Whitman & Mattord, 2018)

1.1 Confidentiality:

The efforts of an organization to keep data secret or private are referred to as confidentiality. To achieve this, access to information must be restricted in order to avoid the unintentional or accidental release of data. Making sure that those who don't have necessary authorization can't access assets that are important to the organization is an important part of protecting confidentiality. An effective system, on the other hand, guarantees that those who needs access have the required permissions. For example, all the data of the customers collected by a bank is only shared to the respective customers and it is not disclosed to anyone else.

1.2 Integrity:

Integrity refers to ensuring that the data is accurate and unmodified. Only original, accurate, and dependable data maintains the integrity of the data. For example, when a person withdraws Rs. 5000 from an ATM the balance deducted from his account is Rs.5000. This means that no tampering has occurred in the process and the transaction is accurate.

1.3 Availability:

Even if data is kept secure and its integrity is preserved, it is generally meaningless unless it is accessible to individuals within the business as well as the clients they serve. This implies that systems, networks, and applications must all work properly and at the appropriate times. Individuals who have access to certain data must also be able to access it when they need it, and acquiring the data should not take an excessive amount of time. For example, an ATM machine provides 24-hour service to its customers, it means that the service is accessible to the customer whenever it is required.

2. Introduction to Cryptography

Cryptography is derived from the Greek words “Kryptos” and “Graphein’”. “Kryptos” means hidden and “Graphein” means writing. Therefore, cryptography is the process of securing the information using various algorithms so that it can only be understood by the writer and the intended reader. It can also be understood as converting the plain text (readable form) into cipher text (unreadable form) and vice-versa. It is the art of building an encryption system which facilitates the communication of secret data through an insecure path. Cryptography is important in the field of information security because it enables the information of the user to be concealed from everyone except the sender and the receiver. It also helps to achieve several goals of InfoSec like maintaining confidentiality, integrity and ensuring authenticity (Zakariyah, 2021).

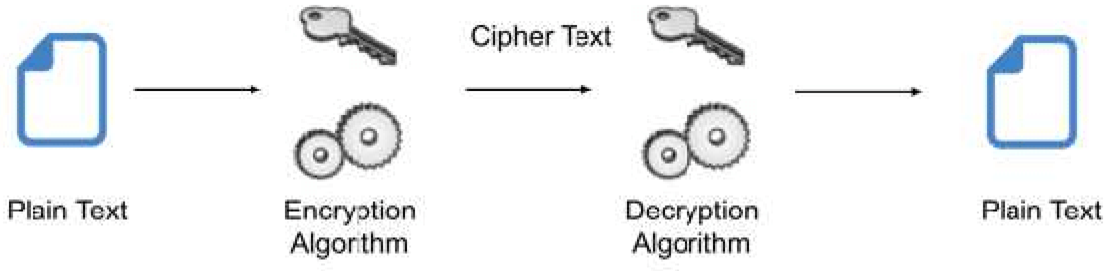


Figure 2: Cryptographic Process

(Albugmi, et al., 2016)

2.1 Key Terminologies of Cryptography

Plain text: It is the unmodified message which is in its original form. This type of message is not secure because it can be read and understood by anyone who has access to it.

Cipher text: It is the message which has been converted into unrecognizable form. This type of message is secure because it can be read and understood by only those who have the key to decipher it.

Key: It is the tool which is used to decrypt the cipher text into plain text. It is important because only those who have the key for a particular encrypted message can use it to decrypt the message.

Encryption: It is the process of converting the plain text into cipher text using a specific algorithm. A key is generated during the encryption process so that the reader can use it to decipher the encrypted message.

Decryption: It is the process of reverting the cipher text into the original plain text. A specific key generated during the encryption is required to decipher the cipher text to plain text.

Algorithm: It is a finite sequence of well-defined instructions, typically used to solve a class of specific problems or to perform a computation.

2.2 History of Cryptography

The origin of cryptography is believed to be from the Egyptian civilization. The oldest known cryptographic technique “Hieroglyph” was developed around 4000 years ago. The Egyptians used “Hieroglyph” to communicate messages secretly on behalf of the kings. The Hieroglyph symbols are depicted as objects but they usually represent particular sounds. Later the Romans created a method of cryptography around 100 BC, which is popularly known as Caesar Shift Cipher. The encryption was carried out by shifting the letters of the message by an agree number (number of one’s choice) and decrypted by shifting the letters back by the same number to obtain the original message.

Figure 3: Hieroglyph – The Oldest Cryptographic Technique

(Tutorialspoint, 2015)

In the 15th century, improved coding techniques like as "Vigenère Coding" were developed, which allowed changing letters in a message to a variety of different positions rather than moving them the same number of times. Cryptography progressed from ad hoc techniques to encryption to the more sophisticated art and science of information security only in the 19th century (Tutorialspoint, 2015).

The introduction of mechanical and electromechanical technologies, such as the Enigma rotor machine, enabled more advanced and efficient techniques of coding information in the 20th century. Later, both cryptography and cryptanalysis became extremely mathematical during World War II. Since then, the cryptography has become more sophisticated (Tutorialspoint, 2015).

In the present day, among all cryptographic systems, Symmetric and Asymmetric key encryption are the most commonly used techniques.

2.3 Symmetric Encryption

Symmetric encryption is a technique in which a message is encrypted using a key and then decrypted with the same key, making it simple to use but less secure. It also requires a secure mechanism of passing the key from one party to the other. There are many algorithms which use symmetric key encryption. Some of them are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, CASTS5, etc (GeeksforGeeks, 2020).

2.4 Asymmetric Encryption

Asymmetric encryption is a technique that uses public and private keys to encrypt information. It encrypts and decrypts the message using two separate keys. Although it is more secure than symmetric key encryption, it is generally slower than symmetric encryption. There are many algorithms which use asymmetric key encryption. Some of them are Rivest Shamir Adleman (RSA), Digital Signature Standard (DSS), Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC), etc. (GeeksforGeeks, 2020)

3. RSA

3.1 Background

The RSA algorithm was developed in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman as a public key encryption algorithm. It is the most extensively used key cryptographic system. The RSA algorithm was the first to be appropriate for encryption and decryption; it involved modular multiplication and exponentiation. For some 'n', the RSA algorithm is a cipher block in which the plaintext and cipher text are integers between 0 and n-1. This method is one of the finest asymmetric key cryptosystems for exchange keys, digital signatures, and data encryption blocks that uses prime integers. Asymmetric cryptography, also known as public key cryptography, employs two distinct keys for encryption and decryption. One key is public, while the other is kept private. The keys are generated by performing a mathematical calculation on two large prime numbers. The public key is sent to everyone in the system but the private key is kept secret in RSA. The RSA cryptosystem's security is based on the mathematical difficulty of factoring large prime numbers. The attacker cannot obtain the factor prime of n and hence the private key by using information from the public key, which contains n (multiplication of prime numbers). As a result, the RSA algorithm is highly secure (Hatem, et al., 2019).

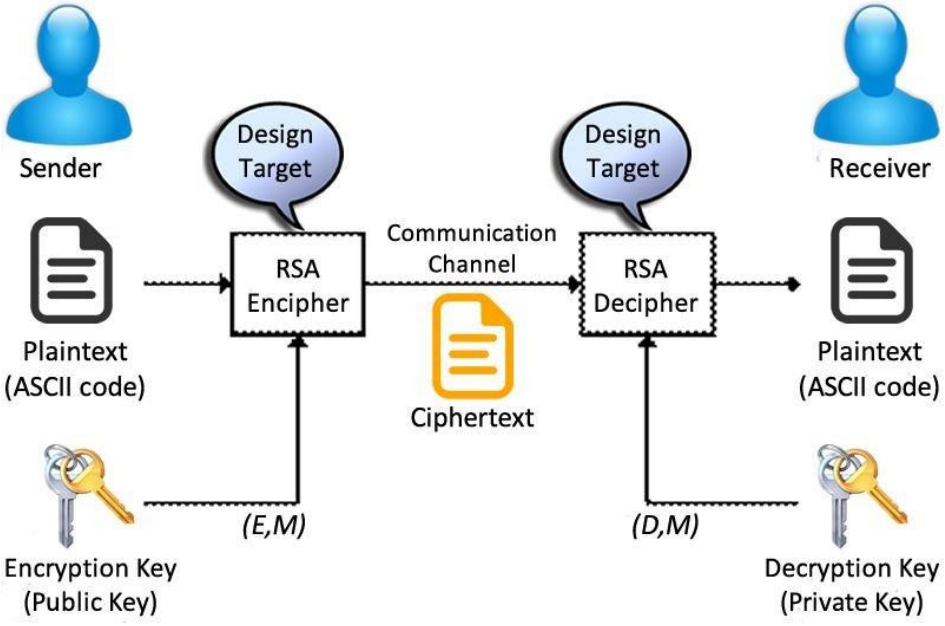


Figure 4: RSA cryptosystem

(Bodur & Kara, 2015)

There are three steps in the RSA algorithm: key generation, encryption, and decryption. Each of them is elaborated below.

3.1.1 Key Generation

A public key and a private key are used in RSA. Everyone has access to the public key, which is used to encrypt messages. The only way to decrypt messages encrypted using the public key is to use the private key. The public key exponent 'e' is revealed, but the private key exponent 'd' is protected (Bonde & Bhadade, 2017). The steps for generating a key are as follows:

1. Select “p” and “q” where $p \neq q$ and both p and q are large prime numbers.
2. Determine $n = p \times q$.
3. Compute $Ø(n) = (p-1) \times (q-1)$, where “Ø” is Euler's totient function.
4. Choose Public Key exponent “e” such that, $1 < e < n$ and $GCD(e, Ø(n)) = 1$.
5. Evaluate the secret Private Key exponent “d” such that, $1 < d < Ø(n)$ and $e \times d \bmod Ø(n) = 1$.
6. Public Key = (n, e)
7. Private Key = (n, d)

3.1.2 Encryption

The following are the processes for encrypting a message to obtain the cipher-text:

1. Obtain the recipient’s Public Key – (n, e).
2. Denote Plain Text message as a positive integer M.
3. Compute the cipher text as $C = M^e \bmod n$.

3.1.3 Decryption

The following are the processes for decrypting cipher-text in order to obtain the original message:

1. Acquire the recipient’s Private Key – (n, d).
2. Calculate the plain text as $M = C^d \bmod n$.

3.2 Advantages of RSA algorithm

The following are some of the advantages of RSA algorithm:

- The RSA algorithm is simple to implement.
- The RSA algorithm provides a safe and secure way to transfer confidential information.
- The RSA method is extremely tough to crack because it includes complex mathematics.
- It is simple to distribute the public key to users.
- It can be implemented using any programming language.
  (GeeksforGeeks, 2021)

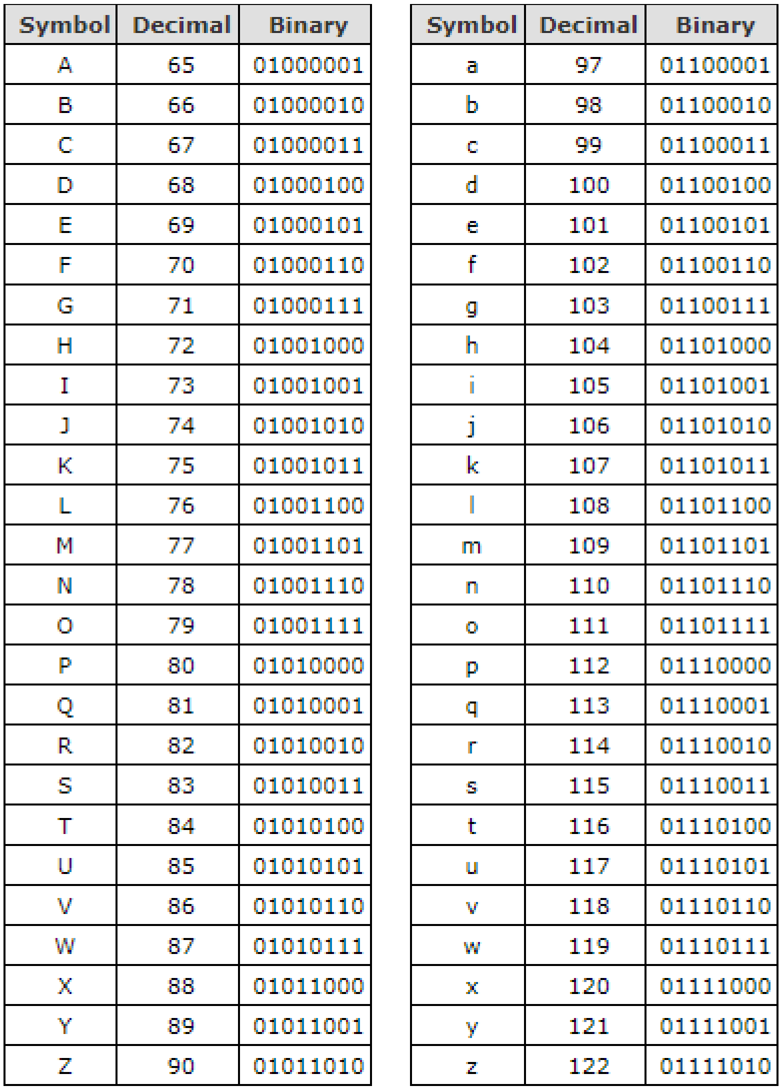
3.3 Disadvantages of RSA algorithm

The following are some of the disadvantages of RSA algorithm:

- It may fail occasionally because full encryption requires both symmetric and asymmetric encryption, while RSA only employs symmetric encryption.
- Due to the large mathematical numbers, the data transfer rate is slow.
- Reliability of the public keys needs to be verified by third party.
- Decryption demands a lot of processing at the receiver's end.
- If the prime numbers taken are small, it’s strength will be poor.
  (GeeksforGeeks, 2021)

4. Modified RSA algorithm

The newly developed algorithm provides an additional layer of security to the already robust cryptographic algorithm, RSA. This algorithm takes the plain text letter, converts it into it's respective ASCII value which is in decimal form and separates the decimal numbers in a way that isolates each decimal number. Then, each of the isolated decimal numbers is converted into their respective binary values and the result is inverted. This means that if the binary value which is 1 is inverted to 0 and vice-versa. The obtained inverted binary value is then converted into its decimal form which gives a new number. The newly obtained decimal numbers represents the value for the plain text and is used in the encryption and decryption process.



Symbol	Decimal	Binary	Symbol	Decimal	Binary
A	65	01000001	a	97	01100001
B	66	01000010	b	98	01100010
C	67	01000011	c	99	01100011
D	68	01000100	d	100	01100100
E	69	01000101	e	101	01100101
F	70	01000110	f	102	01100110
G	71	01000111	g	103	01100111
H	72	01001000	h	104	01101000
I	73	01001001	i	105	01101001
J	74	01001010	j	106	01101010
K	75	01001011	k	107	01101011
L	76	01001100	l	108	01101100
M	77	01001101	m	109	01101101
N	78	01001110	n	110	01101110
O	79	01001111	o	111	01101111
P	80	01010000	p	112	01110000
Q	81	01010001	q	113	01110001
R	82	01010010	r	114	01110010
S	83	01010011	s	115	01110011
T	84	01010100	t	116	01110100
U	85	01010101	u	117	01110101
V	86	01010110	v	118	01110110
W	87	01010111	w	119	01110111
X	88	01011000	x	120	01111000
Y	89	01011001	y	121	01111001
Z	90	01011010	z	122	01111010

Figure 5: ASCII Table for alphabet characters

Since, this algorithm requires isolating and inverting the values, it is named as **IIRSA**. Because of the addition of these extra steps, the algorithm is now one of its kind. The original RSA is a well-known algorithm so many hackers know how it works and can decrypt the cipher text if they have the required time and computational technology. This modification makes this algorithm unique so it cannot be cracked without knowing the additional steps that have been added into it. Thus, it makes this algorithm more secure than the original RSA. The various aspects regarding the complete process of encryption and decryption are elaborated below.

The ASCII values for the alphabet characters can be obtained from the figure above. Assuming the message is "DOG".

First, convert the plain text letters into their respective ASCII values.

D	O	G
68	79	71

Now, isolate the letters, convert into binary and get the inverted decimal value.

D = 68

Where, 6 = 0110 [Binary] 8 = 1000 [Binary]

↓ ↓

1001 [Inverted] 0111 [Inverted]

↓ ↓

9 [Decimal] 7 [Decimal]

The new value of D is 97.

O = 79

Where, 7 = 0111 [Binary]	9 = 1001 [Binary]
↓	↓
1000 [Inverted]	0110 [Inverted]
↓	↓
8 [Decimal]	6 [Decimal]

The new value of O is 86.

G = 71

Where, 7 = 0111 [Binary]	8 = 1000 [Binary]
↓	↓
1000 [Inverted]	0111 [Inverted]
↓	↓
8 [Decimal]	7 [Decimal]

The new value of G is 87.

Here, DOG is encrypted as ‘978687’ by the using the IIRSA method.

Let's say the prime numbers P and Q are 31 and 41, respectively.

n = p * q = 1271 [i.e., 31 * 41]

Ø (n) = (p - 1) * (q - 1) = 1200 [i.e. (31 – 1) * (41 - 1)]

e = 7, since GCD (7, 1200) = 1 < 7 < 1271

d = 343, since e * d mod Ø (n) = 1

So, the public key = (1271, 7)

The private key = (1271, 343)

Encryption

Plain text ‘D’ = 97

C = M ^ e mod n

C = 97 ^ 7 mod 1271

C = 977 (Cipher text)

Decryption

M = C ^ d mod n

M = 977 ^ 343 mod 1271

M = 97 (Original message)

Encryption

Plain text ‘O’ = 86

C = M ^ e mod n

C = 86 ^ 7 mod 1271

C = 189 (Cipher text)

Decryption

M = C ^ d mod n

M = 189 ^ 343 mod 1271

M = 86 (Original message)

Encryption

Plain text ‘G’ = 87

C = M ^ e mod n

C = 87 ^ 7 mod 1271

C = 676 (Cipher text)

Decryption

M = C ^ d mod n

M = 676 ^ 343 mod 1271

M = 87 (Original message)

4.1 Flowchart

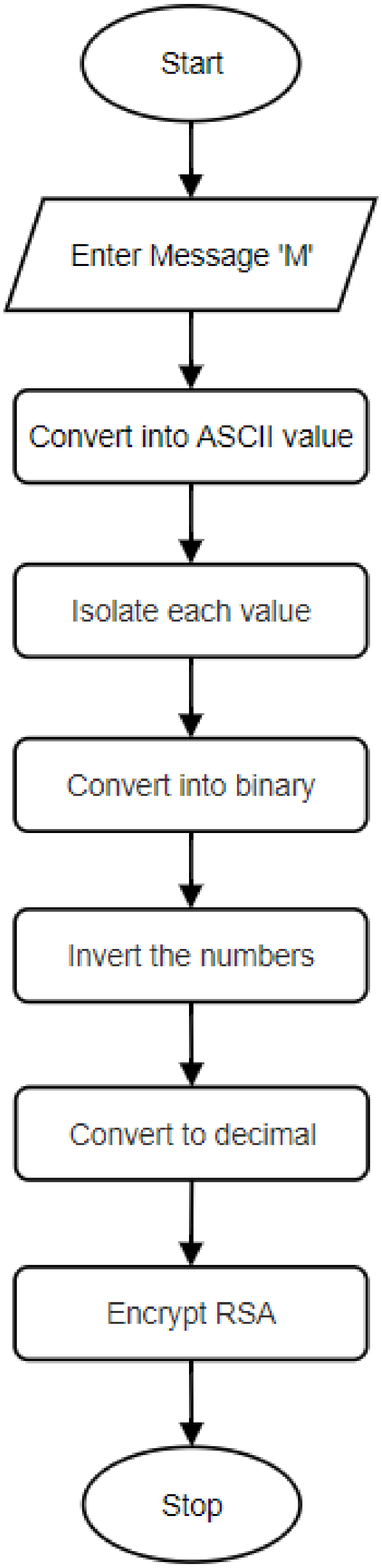


Figure 6: IIRSA encryption algorithm

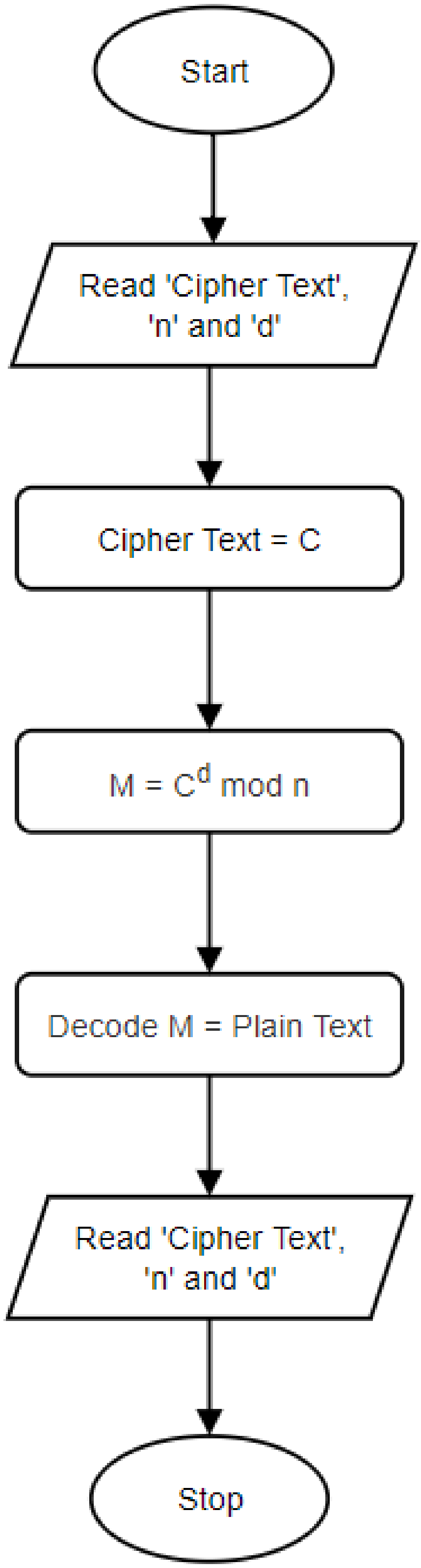


Figure 7: IIRSA decryption algorithm

4.2 Working steps of algorithm

Step 1: Separate each letter in the plain text.

Step 2: Get the ASCII values for each character.

Step 3: Isolate each decimal number.

Step 4: Get the binary value for each decimal.

Step 5: Invert the binary numbers.

Step 6: Convert the obtained value to decimal.

Step 7: Generate the private and public keys.

Step 8: Encrypt and decrypt the message using the generated public and private key.

5. Test Cases

Test 01

Considering the plain text is “G”,

G = 71 [i.e., G = 71 in ASCII value]

Isolating the ASCII values getting the binary values for each,

7 = 0111, 1 = 0001

Inverting the obtained binary values and converting the inverted value into decimal.

1000 = 8, 1110 = 14

Here, G = 814 which is the new value for the plain text.

Let's say the prime numbers P and Q are 43 and 19, respectively.

n = 43 *19 = 817

Ø (n) = (43 - 1) * (19 - 1) = 756

Public Key = (817, 5)

Private Key = (817, 605)

Now,

Encryption

Plain Text ‘G’ = 814

C = M ^ e mod n

C = 814 ^ 5 mod 817

C = 574 (Cipher text)

Decryption

M = C ^ d mod n

M = 574 ^ 605 mod 817

M = 814 (Original message)

Test 02

Considering the plain text is “R”,

R = 82 [i.e., G = 82 in ASCII value]

Isolating the ASCII values getting the binary values for each,

8 = 1000, 2 = 0010

Inverting the obtained binary values and converting the inverted value into decimal.

0111 = 7, 1101 = 13

Here, G = 713 which is the new value for the plain text.

Encryption

Plain Text ‘R’ = 713

C = M ^ e mod n

C = 713 ^ 5 mod 817

C = 497 (Cipher text)

Decryption

M = C ^ d mod n

M = 497 ^ 605 mod 817

M = 814 (Original message)

Test 03

Considering the plain text is “A”,

A = 65 [i.e., A = 65 in ASCII value]

Isolating the ASCII values getting the binary values for each,

6 = 0110, 5 = 0101

Inverting the obtained binary values and converting the inverted value into decimal.

1001 = 9, 1010 = 10

Here, G = 910 which is the new value for the plain text.

Encryption

Plain Text ‘A’ = 910

C = M ^ e mod n

C = 910 ^ 5 mod 817

C = 424 (Cipher text)

Decryption

M = C ^ d mod n

M = 424 ^ 605 mod 817

M = 910 (Original message)

Test 04

Considering the plain text is “P”,

P = 80 [i.e., P = 80 in ASCII value]

Isolating the ASCII values getting the binary values for each,

8 = 1000, 0 = 0000

Inverting the obtained binary values and converting the inverted value into decimal.

0111 = 7, 1111 = 15

Here, P = 715 which is the new value for the plain text.

Encryption

Plain Text ‘P’ = 715

C = M ^ e mod n

C = 715 ^ 5 mod 817

C = 65 (Cipher text)

Decryption

M = C ^ d mod n

M = 65 ^ 605 mod 817

M = 715 (Original message)

Test 05

Considering the plain text is “E”,

E = 80 [i.e., E = 80 in ASCII value]

Isolating the ASCII values getting the binary values for each,

6 = 0110, 9 = 1001

Inverting the obtained binary values and converting the inverted value into decimal.

1001 = 9, 0110 = 6

Here, E = 96 which is the new value for the plain text.

Encryption

Plain Text ‘P’ = 96

C = M ^ e mod n

C = 96 ^ 5 mod 817

C = 799 (Cipher text)

Decryption

M = C ^ d mod n

M = 799 ^ 605 mod 817

M = 96 (Original message)

6. Critical Evaluation of the new Cryptographic Algorithm

6.1 Strengths of the algorithm

Mentioned below is a list of strengths of this new cryptographic algorithm:

- It adds additional steps before encrypting the message through RSA which make it more secure.
- It is extremely difficult for anyone to factor n, i.e., to find p and q.
- It is impossible for anyone to find d, unless they know Ø(n).
- It is a computationally secure algorithm.

6.2 Weakness of the algorithm

Mentioned below is a list of weakness of this new cryptographic algorithm:

- It requires a long time to encrypt data.
- The key may be found if the prime numbers p and q are too close to each other.
- If part of the private key 'd' is too small then it can be easily cracked.
- If the key is less than 1024 bits, it may be cracked by someone with the necessary computational power and time.

6.3 Application Area

An implementation of this cryptographic algorithm is that it can be applied to encrypt an electronic file such as student records, email, and classified documents. It may be implemented in a variety of cryptographic libraries, including OpenSSL, wolfCrypt, cryptlib, and many others. Encrypting and decrypting a huge file takes a long time. As a result, it's ideal for small files. RSA established the foundation for most of current secure communications as one of the earliest public-key encryption systems that was extensively utilized. It was the first method used in PGP encryption and was traditionally used in TLS. Many internet browsers, VPNs, email, chat, and other communication methods still use the RSA. Secure connections between VPN clients and VPN servers are commonly produced using RSA. RSA encryption can be used in TLS handshakes for exchanging keys and establishing a secure link under protocols like OpenVPN.

7. Conclusion

The various concepts of information security have been discussed in this document. The fundamental aspects which must be maintained in order to ensure information security are confidentiality, integrity and availability. In order for these goals to be met, various actions need to be implemented. Cryptography is one method through which these goals of information security like confidentiality and integrity can be met. The history and evolution of the cryptographic systems has been discussed in this document from its origin to the present structure which entails various modifications and variations that have been made to the cryptosystems over the years. Of the many cryptographic techniques, the RSA algorithm has been selected to be modified in this document. The foundation of RSA, its pros and cons and its various processes like key generation, encryption and decryption has been discussed. The changes made to the RSA algorithm along with the flowchart for encryption and decryption and the working steps of algorithm have been elaborated in detail. Moreover, the modified algorithm has been tested and critically evaluated for its strengths and weaknesses and the application areas in which it might be implemented.

8. References

Albugmi, A., Walters, R. J., Alassafi, M. O. & Wills, G., 2016. Data Security in Cloud Computing. *Fifth International Conferance on Future Generation Communication Technologies (FGCT),* Volume 1, pp. 55-59.

Bodur, H. & Kara, R., 2015. Secure SMS Encryption Using RSA Encryption Algorithm on Android. *3rd International Symposium on Innovative Technologies in Engineering and Science,* Volume 1, p. 10.

Bonde, S. Y. & Bhadade, U. S., 2017. IMPLEMENTATION OF RSA ALGORITHM AND MODIFIED RSA ALGORITHM METHODS:A REVIEW. *International Journal of Advanced Technologyg in Engineering and Science,* 5(5), pp. 176-181.

GeeksforGeeks, 2020. *Difference Between Symmetric and Asymmetric Key Encryption.* [Online]
Available at: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/
[Accessed 6 Jan 2021].

GeeksforGeeks, 2021. *RSA Full Form.* [Online]
Available at: https://www.geeksforgeeks.org/rsa-full-form/
[Accessed 7 January 2021].

Hatem, M., Rasha, A., Hatem, A. E. & Reda, H., 2019. Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem. *I.J. of Electronics and Information Engineering,* 10(1), pp. 51-64.

Tutorialspoint, 2015. *Cryptography Just For Beginners.* 1st ed. Hyderabad: Tutorials Point (I) Pvt. Ltd. .

Whitman, M. E. & Mattord, H. J., 2018. *Principles of Information Securrity.* 6th ed. Boston: Cenage Learning.

Zakariyah, W. O., 2021. *Cryptography,* Ilorin: Department of Telecommunication Science, University of Ilorin.