Cryptographic System Using RSA

Ph D Bárbara Emma Sánchez Rinza[1], PH D .Carlos Ignacio Robledo Sánchez[1],
[1,]Benemerite Autonomous University of Puebla, Mexico, barbara.sanchez@correo.bup.mx, carlos.robledo@correo.buap.mx

***Abstract*–The transmission of electronic documents via the Internet has proven to be efficient, however, being an open network, it runs the risk of being vulnerable to attacks by hackers and viruses, resulting in forgery, and manipulation of documents among other security issues. This paper addresses the RSA algorithm to help protect information from this type of attack.**

The RSA algorithm ensures the transfer of electronic data through the network. This project is programmed in java language, where its operation will be shown.

Keywords-- Algorithm, Cryptography, Encryption, Security, Public key, Private key, RSA.

I. Introduction

Cryptology (from the Greek Krypto, "hidden", and graphos, "to write"; hidden writing. [1]) is the science that deals with security-related problems in the exchange of coded messages between a sender and a receiver through a communication channel.

This science is divided into two main branches: [2]

1- Cryptography: concerned with the encryption of coded messages and the design of cryptosystems.

2- Cryptanalysis: which tries to decrypt coded messages, thus breaking the cryptosystem.

Cryptography is considered one of the oldest sciences since its origins date back to the birth of our civilization. Its original use was to protect the confidentiality of military and political information, but nowadays it is important science, not only in these closed circles but for anyone interested in the confidentiality of certain data [3].

In a typical cryptographic model, there are two points: "a" and "b", which are considered trustworthy and, between them, information is transmitted through an untrusted channel. Cryptography deals with the problems related to the confidential and secure transmission over the untrusted medium, while computer security deals with ensuring the trustworthiness of nodes "a" and "b" [4].

Cryptography provides us with three fundamental elements, these are Encryption of documents, digital certificates, and electronic signatures, whereby we can propose a solution to solve security problems in the exchange of information by electronic means. With these three elements, the following is achieved

- ❖ To verify the identity of the interlocutor in a communication (authentication) [2].
- ❖ Ensure that only the selected user(s) will obtain the information (authorization-confidentiality) [2].
- ❖ Ensure that the information has not been modified during and after submission (integrity) [2].
- ❖ Ensure that the sender cannot go back on a sent message (no repudiation at source) [2].

As we mentioned previously, the two great branches of Cryptology are cryptography and cryptanalysis.

Henceforth, we will focus only on cryptography and cryptosystems instead of cryptanalysis, since we are more interested in protecting information by making systems secure, and not in breaking encryption systems.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

II. CRYPTOSYSTEMS

.

Cryptosystems are classified according to the availability of the encryption/decryption key. There are, therefore, two main groups of cryptosystems: Private key cryptosystems and Public-key cryptosystems

A. Private Key Cryptosystems

We call a private key cryptosystem (secret key, unique key, or symmetric key) a cryptosystem in which the encryption key, K, can be calculated from the decryption key, K', and vice versa. In most of these systems, both keys coincide, see figure 1, and of course, they must be kept as a secret between sender and receiver: if an attacker discovers the key used in the communication, he will have broken the cryptosystem.

Before the message m is sent, it must be encrypted using the algorithm E and the key k to obtain the encrypted message c = E(k,m). Using the decryption algorithm D and the same key k we obtain the original message m with m = D(k,c) [5].

It is said to be symmetric because both channels must use the same key "k" for encryption and decryption and the corresponding algorithms C and D are public so that any party or person who knows the key "k" can know the content of the message and it will be necessary that the message m can only be recovered from the encrypted message c, which means that for a fixed key k the encryption map must be bijective.

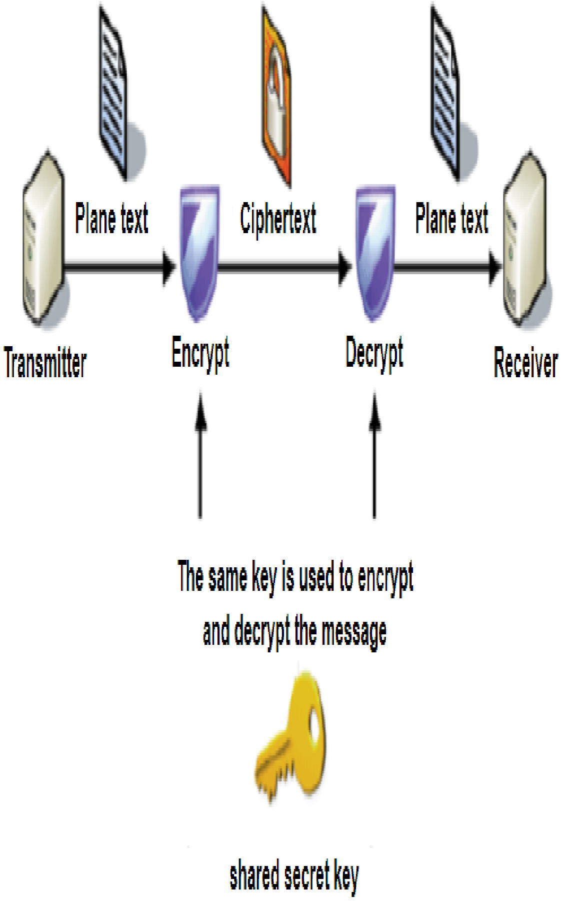


Figure 1. Operation of the private key cryptosystem (symmetrical)

Mathematically the symmetric encryption is represented as:

$$E: K \times M \rightarrow C$$

Such that for each $k \in K$ the map

$$E_k: M \rightarrow C,\ m\ 7 \rightarrow E(k,m)$$

be invertible. The elements $m \in M$ are the messages or plaintext, C is the encrypted message and $k \in K$ are the keys. E_k

is the encryption function with k as the key and the inverse function

Dk:= E^(−1)k is the decryption function [5]

B. *Public Key Cryptosystems*

This classification of cryptography, also called public-key cryptography, is based on the use of two different keys, the function of one is to encrypt and the other to decrypt what the first one encrypted.

Unlike symmetric cryptography, asymmetric cryptography does not share the secret key, here each user has a pair of keys, one called private key (sk) known only to one user and the other called public key (pk), known to all users.

In 1976 W. Diffie and M. E. Hellman published the paper "New Directions in Cryptography" which presents the idea of asymmetric or public-key cryptography, where each participant needed a set of keys k = (sk, pk), which to guarantee the security of the cryptosystem the private key (sk), see figure 2, cannot be calculated or known from the public key (pk) [6].

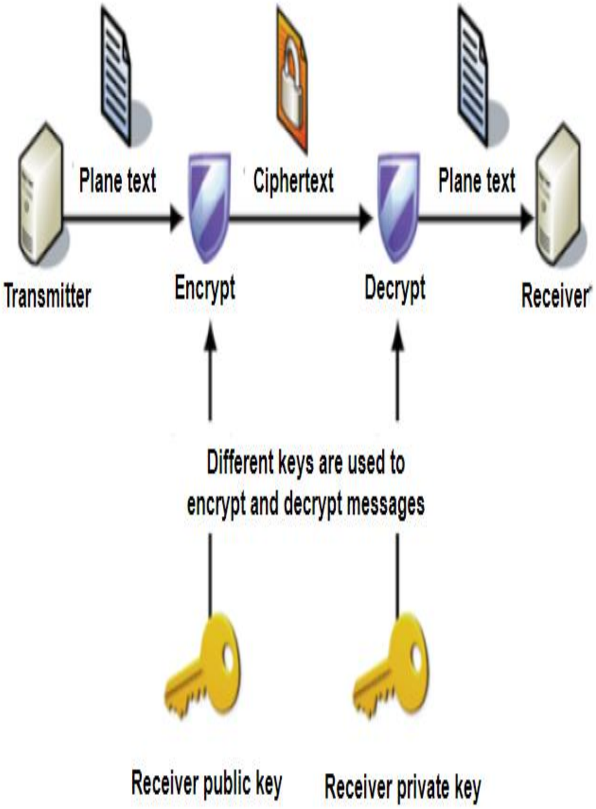


Figure 2: Operation of the public key cryptosystem (asymmetrical).

There are numerous public-key schemes. Only a few algorithms are secure and practical. The reason why these algorithms are not practical is that they either have very large keys or the ciphertext produced is larger than the plaintext.

For practical uses, public-key schemes need to be fast and efficient, as they are much too slow compared to symmetric key encryption methods.

Public key algorithms are commonly used to encrypt small amounts of data, such as passwords, credit card numbers, and PINs.

These schemes are not useful for encrypting large volumes of data they are used to transport the key, which is ultimately used to encrypt the large volumes of data using symmetric key encryption methods [7].

The most popular algorithm in the family of asymmetric algorithms is RSA [8], named after the initials of the last names of its inventors (Ron Rivest, Adi Shamir, and Len Adleman).

III. RSA ALGORITHM

The RSA encryption technique is a public key encryption scheme that does not increase the size of the message. The RSA scheme is characterized by two important functions, namely, secure key exchange and digital signature. A fundamental operation in this encryption scheme is finite group exponentiation, also known as modular exponentiation.

The RSA encryption and decryption processes both use modular exponentiation. This operation is very time-consuming. An "RSA operation" regardless of whether it is for encryption or decryption, signing or authentication is essentially modular exponentiation, which is performed by a series of modular multiplications [7].

In RSA, two large prime numbers are used to construct the private key and the product of these primes to construct the public key. In this asymmetric scheme, it is difficult to obtain the private key (d) from the public key (e;n).

On the other hand, if one were able to factorize the number (n) into its prime factors (p and q) then one could compute the private exponent (d). The RSA system requires a modular multiplication process of integers that have hundreds of bits.

In RSA, the one-way function used is the multiplication of large prime numbers. It is computationally easy to multiply two large prime numbers, but for the vast majority of large prime numbers it is computationally difficult to find the prime factors p;q knowing only the p and q values. This inverse problem is the key to the electronic security system, RSA [7].

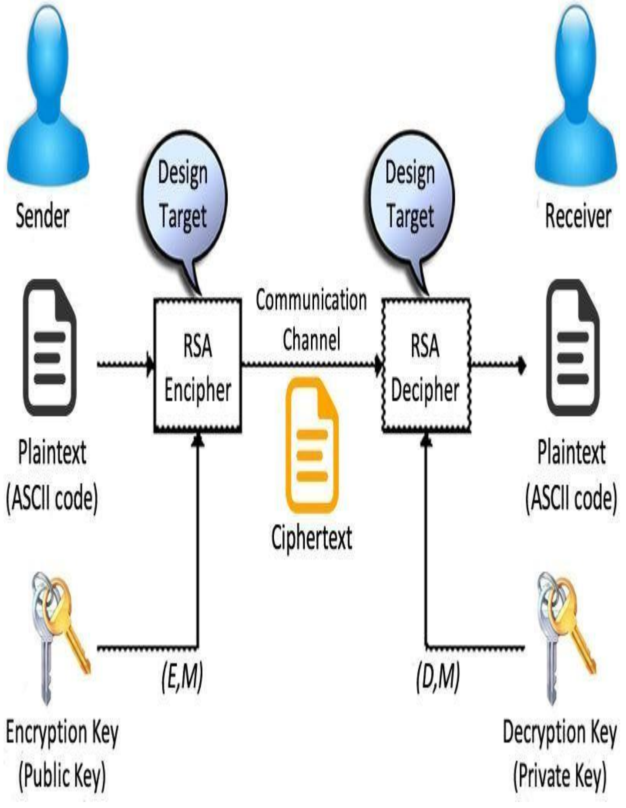


Figure 3: representation del algorithm RSA.

The RSA encryption and decryption algorithms are very simple and very similar to each other:

- ✓ RSA encryption algorithm [1]
- ✓ Input: $K_{pb}^{B} = (n, e)$: public component of the recipient
- ✓ x: message to encrypt
- ✓ Output: y: encrypted message
- ✓ y = x^e (mod n)
- ✓ Returns y
- ✓ RSA decryption algorithm [1].
- ✓ Input: $K_{pr}^{D} = (n, d)$: private component of the recipient
- ✓ y: message to be decrypted
- ✓ Output: x: decrypted message
- ✓ x = y^d (mod n)
- ✓ Returns x

A. *RSA algorithm security*

The security of the RSA system for encryption is mainly based on the fact that, so far, there is no efficient algorithm for factoring integers; that is, there is no known algorithm for factoring d-digit integers in polynomial time, O (dk). Then, if sufficiently large primes p and q are selected, it is impractical to calculate the factorization z = pq. If a person intercepting a message could find the factorization, he or she could decrypt the message just like the authorized receiver. Up to now, there is no known practical method for factoring integers with 200 digits or more, so if p and q are each chosen with 100 digits or more, pq will have about 200 digits or more, which seems to make the RSA system secure [5].

- The entire security of RSA is based on the assumption that factoring is difficult. Therefore, if someone finds an easy-to-factorize algorithm, this will invalidate RSA.

- To have an acceptable level of security in RSA, conditions must be given on the primes p; q to minimize attacks on RSA.

- Network security problems due to the increase in Internet transaction traffic have made their appearance and have evidenced the need for further research in cryptographic algorithms. RSA is currently widely used [7,10].

IV. IMPLEMENTATION OF THE RSA ALGORITHM

In this section, it will be shown the result of the implementation of the RSA algorithm, programmed in java language.

This algorithm has a sequence of intertwined steps, that is to say, each of them depends on the previous one:

- Generate keys to encrypt the message.
- Message encryption.
- Decrypted message.

A. RSA algorithm Interface

The interface of this system is simple to understand, first, we start with the title of our algorithm, then we have a box where we can enter the text we want to encrypt.

We must take into account that the text we enter must be short or moderately long since when entering a very long text, our system becomes slow because the RSA algorithm uses modular exponentiation and this operation consumes a lot of time.

After that, we have a "calculate" button that, when pressed, calculates the elements of the public key and the private key; the same as displayed on the interface.

Having calculated the keys, both private and public, the algorithm performs the methods of encryption and decryption of the text entered; at the end of these calculations the system prints the encrypted and decrypted texts in their respective boxes on the interface.

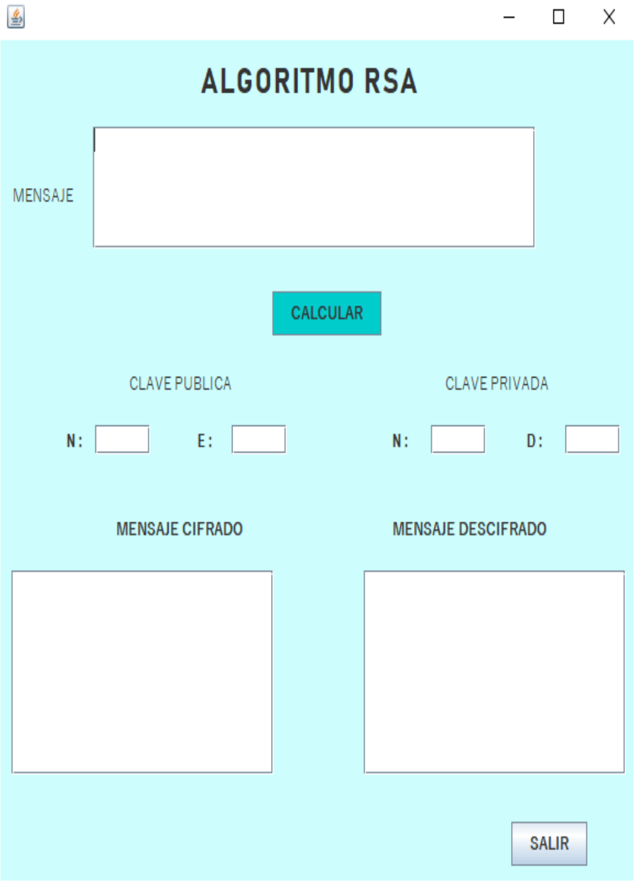


Figure 4. RSA algorithm interface.

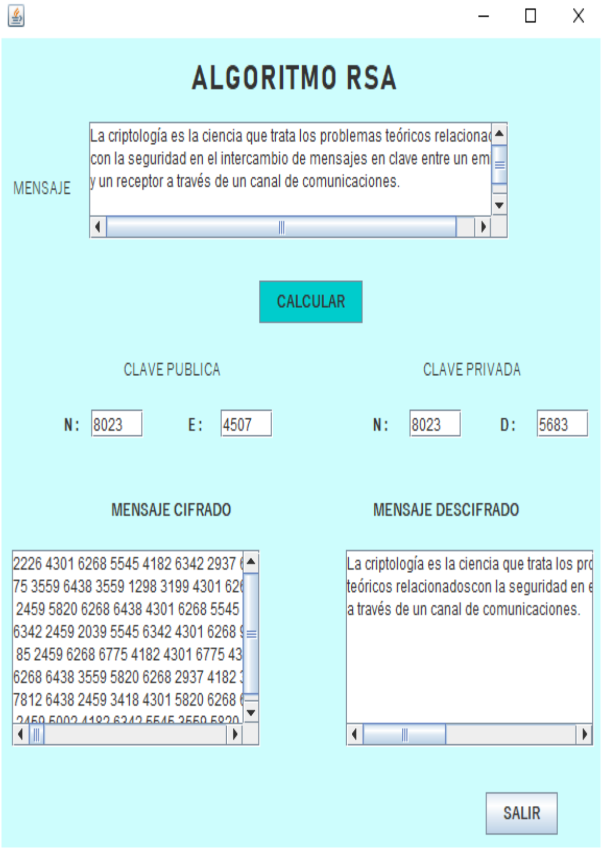
Note: The text to be entered can contain any English language symbol since the system is programmed to make use of the 255 characters of the ASCII code.

B. System execution

Figure 5, shows the final result of the calculation of the RSA algorithm, showing its two different forms:

❖ Text encryption: this is displayed numerically, indicating that the original text was encrypted to hide important information that only the sender wishes to share with one recipient and no one else.

❖ Text decryption: this shows the decoded text and means that the message and the keys arrived correctly to the recipient, who can decode the information sent without any modification by third parties.


ALGORITMO RSA

MENSAJE

La criptología es la ciencia que trata los problemas teóricos relaciona
con la seguridad en el intercambio de mensajes en clave entre un em
y un receptor a través de un canal de comunicaciones.

CLAVE PUBLICA

N: 8023 E: 4507

CLAVE PRIVADA

N: 8023 D: 5683

MENSAJE CIFRADO

```
2226 4301 6268 5545 4182 6342 2937
75 3559 6438 3559 1298 3199 4301 62
 2459 5820 6268 6438 4301 6268 5545
6342 2459 2039 5545 6342 4301 6268
 85 2459 6268 6775 4182 4301 6775 43
6268 6438 3559 5820 6268 2937 4182
7812 6438 2459 3418 4301 5820 6268
 2459 5002 4182 6342 5545 3559 5820
```

MENSAJE DESCIFRADO

La criptología es la ciencia que trata los pro
teóricos relacionadoscon la seguridad en e
a través de un canal de comunicaciones.

Figure 5. RSA algorithm execution

V. ATTACKS ON RSA

As a system developed in 1977, RSA has been the subject of numerous analyses and that is one of its strengths: no attack has been found that compromises the security of the system.

Most of the attacks known to date take advantage of the very features of the cryptosystem implementation. They generally exploit its misuse, the poor choice of the private component "d" or the public component "e", the relationship between encrypted messages, etc.

VI. CONCLUSIONS

Cyclic encryption consists of repeatedly encrypting the intercepted cryptogram with the recipient's public key until the cryptogram is obtained again, which will happen sooner or later and will reveal a clear message.

However, since the realization of this cycle is extremely high, these attacks are not considered a real threat to the security of the RSA cryptosystem [1].

Lateral Channel

Attack based on information obtained from the physical implementation of a computer system itself, rather than based on weaknesses in the implemented algorithm.

The underlying principle is that the physical effects caused by the operation of a cryptosystem can provide useful information.

In many of the implementations of these methods that have been proposed, the side-channel attack relies on the precise measurement of information about a piece of hardware that performs RSA operations, such as modular exponentiation.

Thus, for example, the power spikes consumed by the CPU during an algorithm run without modular exponentiation may differ from those resulting during an algorithm run with it.

These measurements allow locating and monitoring each of the steps of the modular exponentiation involving Kpr, leading to obtaining each bit of the key at each step [1].

Factoring is the problem that sets the bar on security in public-key ciphers. Any security problem in the RSA cryptosystem can be fixed. However, factoring is a problem of which the size cannot be known. If n can be factored, in the general case, the RSA private key is obtained [1,11].

REFERENCES

[1] Barbara Emma Sanchez Rinza, Maria del Rocio, et, Decryption system of thematical texts in Spanish using frequency analysis including unigrams, bigrams, and trigrams, IJEIT, vol 5, N6 December 2015, ISSN 2277-3754

[2] Marí Salvador. N. (2018). Una propuesta híbrida para el criptoanálisis RSA. [tesis para maestría, Universidad Tecnológica de Valencia, https://riunet.upv.es/bitstream/handle/10251/107779/MAR%C3%8D%20-%20Una%20propuesta%20h%C3%ADbrida%20para%20el%20criptoan%C3%A1lisis%20RSA..pdf?sequence=1&isAllowed=y].

[3] Ordoñez Hernández. A. (2016). Cifrado y distribución de documentos vía web utilizando algoritmos Triple DES-96 y RSA. [Tesis de maestría, INSTITUTO POLITECNICO NACIONAL, https://tesis.ipn.mx/bitstream/handle/123456789/19971/Cifrado%20y%20distribuci%C3%B3n%20de%20documentos%20v%C3%ADa%20web.pdf?sequence=1&isAllowed=y].

[4] Antonio Villalon Huerta, "SEGURIDAD EN UNIX Y REDES", Nau Llibres (Edicions Culturals Valencianes, S.A.); edición 1st, 2002, ISBN-10: 8418047046.

[5] Yran Marrero, "La Criptografía como elemento de seguridad informática", ACIMED v.11 n.6, 2003, ISSN 1024-9435

[6] Richard Johnsonbaugh. Matemáticas Discretas, Sexta Edición. SPrentice Hall, México, July 2005. ISBN 970-26-0637-3.

[7] Kenneth H. Rosen. Discrete Mathematics and Its Applications, Seventh Edition. Springer, July 2012. ISBN 978-0-07-338309-5.

[8] Espinosa Lazo. J, G. (2004). Autenticación entre componentes en un prototipo de aplicación empresarial distribuida. [Tesis de maestría, UNIVERSIDAD AUTÓNOMA METROPOLITANA UNIDAD AZCAPOTZALCO, http://zaloamati.azc.uam.mx/bitstream/handle/11191/1174/Autenticacion_entre_componentes.pdf?sequence=1].

[9] Delgado,V & Palacios, R. "Introducción a la criptografía: tipos de algoritmos", Anales de Mecánica y Electricidad, LXXXIII, pp. 44-46, 2006, ISSN 0003-2506.

[10] Sánchez, B. Bigurra, Diana. et all. De-Encryption of a text in Spanish using probability and statistics. 18th International Conference on Electronics, Communications and Computers: 2008.

[11] Sánchez, B. Cruz, S. Cesar decryption algorithm, but the method of frequency points in the Spanish language. International Journal of Engineering and Innovative Technology: 2013.