The Mathematics Behind The RSA Algorithm

Souad Abummaryam [1*], Hana Mohammed [2] , Najat Atbaiga [3]

[1] souad22008@yahoo.com s.ahmed@su.edu.ly, [2] Hanna.elhemali@yahoo.com, [3] Najatatbaiga@gmail.com

[1] Department of Mathematics, Faculty of Science, Sirte University, Libya
[2, 3] Department of Computing, Faculty of Science, Sirte University, Libya
*Corresponding author email:

ABSTRACT

The mathematics background of RSA algorithm represents the source of safety in the security science and particularly in the field of cryptography. RSA algorithm was taken as known mechanism of public key cryptography algorithms to encode and decode a message. In this paper we introduce the using of number theory techniques as critical point of security of public key cryptography algorithm. Furthermore mathematical aspects and issues of RSA algorithm have been validated as proof of concept.

Keywords: Public key cryptosystem, RSA algorithm ,encryption, decryption.

1. Introduction

Cryptography means secret writing. It is a technique that employed to protect data from such a security threat and prevents the unauthorized people from recognizing the meaning. Furthermore cryptographic system involves that both processes, encryption and it's reveres decryption which are performed based on key(s). Cryptographic system generally is classified into public-key cryptosystem (asymmetric) and private-Key Cryptosystem (symmetric) [1]. The figure (1) shows the general cryptographic systems. Based on the secrecy of key(s) and the strength of the cipher (cryptographic algorithm), the security of encrypted messages is guaranteed .Symmetric key cryptography , is also known as single key cryptography and conventional cryptosystem [2]. This cryptographic system single key is used to encrypt and decrypt data . Although using identical keys (in common form) of symmetric cryptosystem, makes it fast to accomplish both processes (en/decryption), it is vulnerability from point of view disclosing that single key.

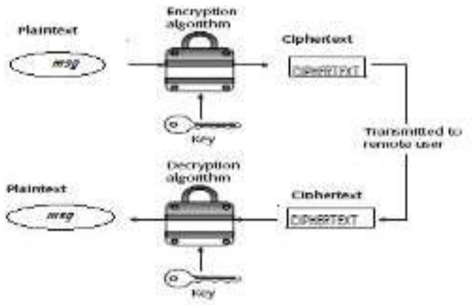

Figure 1. Cryptographic systems

The original text (plaintext, clear text) to be sent through unreliable medium is known as plain text. The encrypted plain text is known as cipher text, which is received at the other side. A cipher (cryptographic algorithm) is an algorithm for performing both encryption and decryption. The cipher text is not readable text without a proper technique to decrypt. The process of converting plaintext into cipher text is called encryption, and to retrieve it back to the original message is called decryption. The key is a number or letter, and can be sequence of digits or letters that is used in encryption (and/ or) decryption.

2. Public Key cryptography

Public-Key Cryptography is the most known factor for security and protection systems. The cryptographic systems in a form which paired of keys are used to perform the encryption and decryption process is known as public Key cryptosystem .It is also known as asymmetric key, and two –keys (paired keys) cryptographic system.

In public key cryptosystems, two keys are used in order to produce a cipher text and then retrieve back the original text. Those keys are mathematically related, one of them is known to public (public key) and the other is unknown (secret key), respectively are used to encrypt and decrypt a message in the common form. Even though sometimes private key used to encrypt and public key to decrypt. Consequently, that means in both directions, asymmetric cryptography keys can work [3].

There are four procedures that are specific and essential to a public-key cryptosystem:

(a) Deciphering an enciphered message gives you the original message, specifically

D(E(M)) = M :

(b) Reversing the procedures still returns M:

E(D(M)) = M :

(c) E and D are easy to compute.

(d) The publicity of E does not compromise the secrecy of D, so cannot figure out D from E.

Security of transmission of data is granted by using public key technique at reasonable level because of some security issues in private key technique are reduced and addressed here (in public key) . One of these issues, both parties (sender, receiver) has to exchange the shared key, and agree on it in advance. On other words whether a source of the message (sender) or the destination (receiver) generated the key; it has to share the key with the other party in a secure channel. This concern about distribution of the shared key in term of security is eliminated with public key cryptosystem [3]. Assume that single key is intercepted (attacked) thus consequently, the whole system is collapsed, and then be worthless. Whereas just one of keys in the public key cryptosystem is involved to communicate (to encrypt sent data). By using two keys instead of one; which one of them is publically distributed and the other key is private. Only the authorized (intended) recipient knows the private (to decrypt data).

So over a non-secure channel, the source and destination could be communicated [1].The private key can be derived from the known key hence they are mathematically linked. Another security issue is about providing confidentiality and authentication [4]. The authentication can be introduced by using a sender's private key to encrypt a message then the receiver can perform the decryption using the sender's public key. Figure 2 shows the use of public-key encryption to provide authentication.

C=E(PRa,M)

M=D(PUa,C)

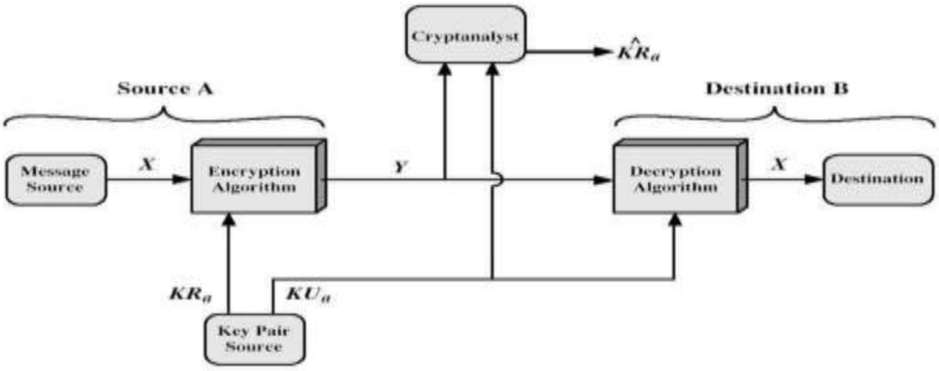

Figure 2. Authentication via public key

The authentication by this way is provided to prove that the message came from the Intended sender (A). On other hand the secrecy (confidentiality) is provided when a sender uses the intended receiver's public key for the encryption. This receiver will use his/her private key to reverse this operation and retrieve the original massage. Figure 3 shows the use of public-key encryption to provide secrecy [2].

C=E(PUb , M)

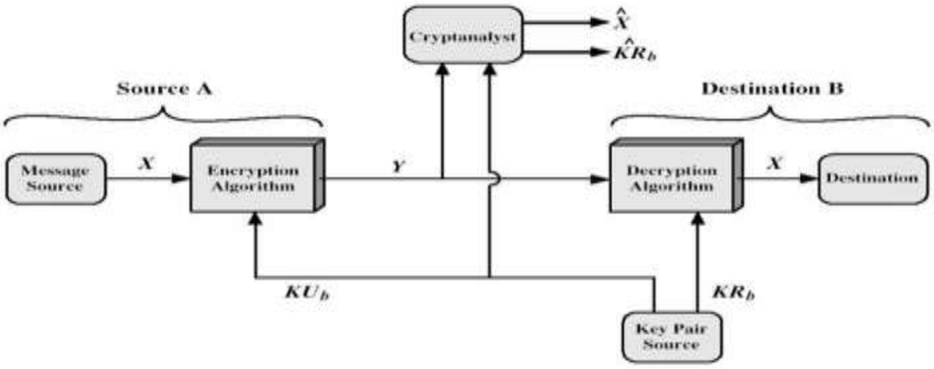

Figure 3. Public key-secrecy (confidentiality)

3. RSA Algorithm

The best known and widely used public-key algorithm is the RSA. It was developed by Rivest, Shamir & Adleman in 1977. RSA algorithm is considered to be common application of asymmetric cryptosystem which is based on mathematical theories [2] [5]. The one –way function on X which is an invertible function $E{:}X \longrightarrow X$, where it is easy for the sender to find the invertible function $E^{-1}$and not easy for anyone else to find it. This is can be calculated by modular arithmetic .

RSA is based on number factorization. Multiplying two large numbers is not difficult, but factoring large numbers is critical point in this algorithm which is related to mathematics [1][6]. Number theory plays a very important role in RSA, because the most basic cryptographic techniques, used are based on number theory.

4. RSA Key Generation

Public-key needs two keys which are a pair of positive integers: (e, n) is encryption key and (d, n) is decryption key. The encryption is public, while the decryption one is private.

Each user generates a public/private key pair by:

Step1- The sender chooses randomly two sufficiently large prime numbers p, q, which they are, a part of the secret key (private choice).

Step 2-The sender also compute n=p.q , which is part of the public key (n is used as the modulus for both the public and private key). p and q will not be revealed from (n) (public).

Step 3-The sender calculate ø (n) = (p-1)(q-1).

Step 4-The sender choose an integer (e), as the public key (encryption exponent) such that

1<e< ø (n), gcd(e, ø (n))=1.

Step 5- The sender find d (decryption exponent), as the private key such that

$$\mathrm{de} = 1 \bmod ø(\mathrm{n}), \qquad 0 \le \mathrm{d} \le \mathrm{n}. \text{Hence}$$

$$\mathrm{ed} = 1 + \mathrm{k}.ø(\mathrm{n}) \text{ for some } \mathrm{k}$$

$$\mathrm{d} = \mathrm{e}^{-1} \bmod ø(\mathrm{n})$$

The sender define the function $\mathrm{E(x)} = \mathrm{d^e} \bmod \mathrm{n}$, while anybody can calculate E. The symbol (e, n) is the public key for the sender. While the sender is only the one who knows the private key d, then the sender can compute the invertible function E^{-1}.

Step 4, 5 can be computed by extended Euclidean algorithm. Also, can be computed by finding k where

$$d = \frac{\mathrm{k}\, ø(\mathrm{n}) + 1}{e}$$

Both sender and receiver have to know the value of (n). The sender knows the value of (e), and only the receiver knows (d).

4.1 Encryption

The sender transmits her public key (e, n) to the receiver and keeps the private key secret. The receiver then wants to send plain message M to the sender.

He first turns M into an integer number $< n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text C

$$C = M^e mod\ n$$

The receiver then transmits C to the sender.

4.2 Decryption

The sender can recover M from C by using her private key exponent d by the

$$\mathrm{M} = C^d mod\ n$$

$$\mathrm{M} \ = (\mathrm{M}^{\mathrm{e}})^{\mathrm{d}} mod\ n = M^{ed} mod\ n$$

$$\mathrm{M, C< n.}$$

Then, what is the relation for

$$\mathrm{M} \ = M^{ed} mod\ n$$

$$\mathrm{C}^{\mathrm{d}} = \mathrm{M}^{\mathrm{ed}} = \mathrm{M}^{1+\mathrm{k}\o(\mathrm{n})} = \mathrm{M}^1\left(\mathrm{M}^{\o(\mathrm{n})}\right)^{\mathrm{k}} \mathrm{\ mod\ n}$$

$$= \mathrm{M}^1(1)^{\mathrm{k}} \mathrm{\ mod\ n} = \mathrm{M}^1 \mathrm{\ mod\ n = M\ mod\ n}$$

This can be achieved by e.d=1+k.ø(n) $\equiv 1$ mod ø(n), k is an integer.
The above result can be proved by the following theorems:
Euler's theorem: For n, a positive and relatively prime

$$\mathrm{a}^{\o(\mathrm{n})}\mathrm{mod\ n} = 1 \quad , \quad \text{where gcd(a,n)=1}$$

gcd means greatest common divisor, $\emptyset(\mathrm{n})$ is the Euler's totient function.

Let p and q are prime numbers, where n=pg, 0< a<n. Then we have

$$a^{\o(\mathrm{n})+1} = a^{(p-1)(q-1)+1} = a \mathrm{\ mod\ n}$$

If gcd(a,n)=1, so it holds (Euler's theorem). This mean (a) will not be multiple of (p) or (q).
But if $\gcd(\mathrm{a}, \mathrm{n}) \neq 1$, this means (a) is a multiple of (p) or (q). Equivalently (a=kp or a=kq). Then for gcd(a,n)= 1 Euler's theorem hold and we have

$$\mathrm{a}^{\o(\mathrm{q})} = 1 \mathrm{\ mod\ q}$$

By modular arithmetic

$$\left(\ \mathrm{a}^{\o(\mathrm{q})}\right)^{\o(\mathrm{p})} \equiv 1 \mathrm{\ mod\ q}$$

$$\mathrm{a}^{\o(\mathrm{n})} \equiv 1 \mathrm{\ mod\ q}$$

This means that, there an integer k such that

$$a^{\text{ø}(n)} = 1 + kq$$

If we multiply both sides by a=Kp, then we have

$$a^{\text{ø}(n)+1} = a + kKpq = a + kKn$$

$$a^{\text{ø}(n)+1} = a \mod n$$

Theorem: Let we have e and d satisfying

$$ed \mod \emptyset(n) \equiv 1,$$

where,

M is a message, where $0 < M < n - 1$ such that $\gcd(M, n) = 1$

Then $(M^e \mod n)^d \mod n = M$

Proof: We have $(M^e \mod n)^d \mod n = M^{ed} \mod n$

The relation between e, d is $ed \mod \text{ø}(n) = 1$, which is equivalent to:

ed=1 mod ø(n) , 0≤d≤n ⟹ed = 1+ k ø(n) for some integer k

⟹d=e^{-1} mod ø(n)

(e) and (d) are multiplication inverse mod ø(n), with respect to modular arithmetic, if (d) or (e) are relatively prime to ø(n)

gcd(ø(n),d)= gcd(ø(n),e)=1

By Eluer’s theorem

$$M^{ed} = M^{1+k\text{ø}(n)} = M^1\left(M^{\text{ø}(n)}\right)^k \mod n$$

where,

$$M^{k\text{ø}(n)} \mod n = \left(M^{\text{ø}(n)} \mod n\right)^k \mod n \quad = \quad 1^k \mod n = 1$$

Therefore, $M^{ed} \mod n = (M.1) \mod n = M.$

This can be achieved by e.d=1+k.ø(n) ≡ 1 mod ø(n).

By symmetric, decryption and decryption are commutative and inverses. Therefore

$\left(M^d \mod n\right)^e \mod n =, \ M^{ed} \mod n = M$

To prove M=C^dmod n

Proof: We know M< n, then

$$\begin{aligned} M &= M \mod n \\ &= M^{ed} \mod n \\ &= (M^e \mod n)^d \mod n \\ &= C^d \mod n \end{aligned}$$

5. Examples and Discussion

In this section, we give some examples to illustrate how RSA public key encryption algorithm works:

Example 1: p=53, q=59$\Longrightarrow$ n=3127

We also need small integer exponent,

Generate private key $\Longrightarrow$ ø(n) = (p-1) (q-1) = 3016

Calculate private key $\Longrightarrow$ d $=\frac{2(3016)+1}{3}=$ 2011 or can be found by Extended Euclid's Algorithm.

Encrypt data with public key:

Public key is made of (n) and (e): 3127 and 3

Private Key is made of (n) and (d): 3127 and 2011

Example2: Let en encrypt **HI**, If we put instead of letter numbers such that H=8 and I=9, which is HI=89

C=Encrypted data

C=89^3 mod 3127

Decrypt data with private key

=C^d mod n

89=1394^{2011} mod 3127

H=8, I=9

Example3:

- Let p=17 & q=11
- Calculate n = pq =17 x 11=187
- Calculate ø(n)=(p–1)(q-1)=16x10=160
- Select e: gcd(e,160)=1; choose e=7
- Determine d: de=1 mod 160 and d < 160, d=23 since 23x7=161= 10(160)+1, d is calculated using Extended Euclin Algorithm.
- Publish public key PU(e, n)={7,187}
- Keep private key PR(d,n)={23,187}
- Let, the plane message (M=88). Then,

For encryption,

$$\text{Cipher text} \quad C = M^{e} \bmod n = (88)^{7} \bmod 187$$

=888832 mod 187=1

For decryption:

$$\text{Plain text} \quad M = C^{d} \bmod n = (11)^{23} \bmod 187$$

= 79720245 MOD 187=88.

We note that, encryption with small (e) and small (M) leads to small (M^{e}), can be less than (mod n). So, Cipher text can be easily decrypted but if (M) is big, cipher text will be difficult to decrypt. Therefore it is better to use big value of (e) for security reason.

6. The security of RSA

The security of RSA cryptosystem depends upon the difficulties of factorization of large prime numbers. Private Key can be generated by using public key information, which includes n, an attacker cannot determine the prime factor of n and therefore the private key. This makes the RSA algorithm secure.

7. Conclusion and Future work

This paper shows the meaning of cryptography in general .And describe RSA algorithm as an example of public cryptographic system .Also it summarize both authenticity and secrecy are granted by using two separated keys as seen with RSA. The security of this algorithm relays on the use of complex mathematics, especially on factoring large number .In addition the performance of RSA is directly affected by chosen keys` length. That means long of the keys is critical to RSA to be more safe and secure; since large key space means more defence against such an attack. This point is strength point of RSA due to the factorization of long number is compacted. In the other hand RSA algorithm is slow of encryption text. It requires third party to verify the reliability of public keys. In conclusion asymmetric encryption technique is important in encryption of sensitive data. RSA algorithm is difficult to fracture since it requires factorization of prime numbers which are nearly impossible.

The future work would be based upon working on combination of asymmetric encryption techniques, reducing encryption time, which are not proposed in this paper.

References

[1]- Chadha,A , Mallik ,S , Johar,R and Roja ,M(2015) . Dual-Layer Video Encryption Using RSA Algorithm. International Journal of Computer Applications, Vol.116,No.1 PP.33-40

[2] Stallings,W.(2011) Cryptography And Network Security Principles And Practice.5th

New York: Prentice Hall

[3] Soriano,M.(2012) Information and Network Security. Prague :Czech Technical University

[4] Cimpa,A(2014).CompTIA Security Guide To Network Security.5th ed.USA,Boston: Cengage Learning

[5] Zotos,K.and Litke,A.(2005).Cryptography and Encryption[online].Available from: https://arxiv.org/abs/math/0510057 [acceded 01/03/2018]

[6] Steef,A , Shamma ,M ,and Alkhatib,A(2015). Rsa Algorithm With A New Approach Encryption And Decryption Message Text By Ascii. International Journal on Cryptography and Information Security, Vol. 5,No.3/4,PP.23-32

[7] Chakraborty,S ,Kumar,V(2015).Astudy and implementation of RSA Cryptosystem[online].Available from: https://arxiv.org [acceded 17/05/2018]

[8] Kumari,P.,Kumar,U. and Singh,S.(2016).Dual-Layer Video Encryption Using RSA and ECC ,Algorithm ,International Journal of Scientific and Research Publications, 6(7),pp620-625

[9]Karki,A.(2016)A Comparative Analysis of Public Key Cryptography, International Journalof Modern Computer Science,4(6),pp30-35