International Journal of Theoretical & Applied Sciences, 12(1): 37-42(2020)

ISSN No. (Print): 0975-1718
ISSN No. (Online): 2249-3247

Digital Signatures using RSA Public Key Cryptosystem Scheme

Arun Kumar Sharma[1] and Nikhlesh Kumar Badoga[2]
[1]Department of Computer Science & Engineering, NIT Hamirpur, India.
[2]Department of Computer Science & Engineering, Thapar Institute of Engineering and Technology, India.

(Corresponding author: Arun Kumar Sharma)
(Received 07 April, 2020, accepted 22 June, 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In the present era which pertains mainly to information technology, the data travels through various communication channels that are insecure. Security issues of such data are very important. During communication over any network the issues of confidentiality, integrity and authenticity of data arise. The confidentiality is ensured by the methods of cryptography whereas the various techniques of digital signatures are used to ensure integrity and authenticity of data. The security issues regarding e-commerce, e-mail, internet banking, ATM etc. are addressed by the techniques of cryptography. Here, we discuss in detail the RSA public key cryptosystem and the digital signatures using the RSA technique. Further, we explain the digital signature scheme using RSA with the help of an illustration.

Keywords: Cryptosystem, Digital Signature, Public Key, Encryption, Decryption, Confidentiality, Authenticity, Integrity.

I. INTRODUCTION

In 1976, Whilfield Diffie and Martin Hellman first time describe the concept of digital signature, [3, 6, 7, 9, 11, 13, 19]. The electronic documents are signed using Digital Signature. Digital signature have similar properties to handwritten signature. Handwritten signature are called conventional signature. A "conventional" signature which is attached to a document, associates the responsibility of person pertaining to the signature. A signature is used very frequently in everyday life. For example writing a letter, signing a contract, withdrawing money from a bank etc. In other words, a verified signature on a document, is a sign of authentication, which tells that the document is authentic.

Electronic documents need to be duly signed in most situations. For example, electronic bank transactions, electronic contracts and binding electronic mail. The receiver needs to ensure that the message is only from the intended recipient and not the third person. In order to find required information filtering is utmost essential, see [14, 16]. Electronically signing the message plays a vital role in ensuring the correct sender. In other words, the authenticity of the sender can be verified or proved with the help of electronic signature. This type of signature is referred to as Digital Signature.

In the present era of web-commerce Digital signatures are of great importance. The provisions have been already made for valid authorization procedure in order to recognize a Digital Signature similar topaper-based signature. Legal status has now been achieved by Digital signatures.

RSA Cryptosystem:

Ron Rivest, Adi Shamir and Len Adleman at MIT made many attempts during entire year in order to create a one-way function which is difficult to inverse, Rivest and Shamir, as computer scientists, proposed a variety of potential functions while Adleman, being a mathematic can, developed first major asymmetric key cryptography system and the final result was published in 1978,which is known as RSA cryptosystem. It solves the problem of key agreements and distributions, [1, 2, 4, 5, 8, 10, 12, 15, 17, 18, 20, 21].

The RSA cryptosystem is the most popular and proven asymmetric key cryptographic cryptosystem.

Implementation of RSA Cryptosystem:

The RSA Cryptosystem involves mainly three steps: **Key-Generation**, **Encryption** and **Decryption**, which are discussed below.

1) RSA Key Generation: RSA Cryptosystem uses a public key. The message is encrypted with the help of public key and is known to everyone. The encryption of message which is done with the help of public key can be decrypted only using the private key. The keysto be used for RSA algorithm are created using following steps:

1. Choose two large prime, p *and* q, of equal size approximately so that the product $n = p \times q$ is of 1024 bits.
2. Calculate $n = p \times q$ *and* $\varphi(n) = (p-1)(q-1)$.
3. Choose an integer $e, 1 < e < \varphi(n)$, so that gcd $(e, \varphi(n)) = 1$.

4. Calculate the secret exponent d, such that $ed \equiv 1(mod\varphi(n))$.
5. The public key is (n, e) and the private key is (n, d).All the values d, p, q and $\varphi$are kept secret.

(i) n is called as the modulus.
(ii) e is called as the public exponent or exponent or encryption exponent.
(iii) d is called as the decryption exponent or secret exponent.

2) RSA Encryption: The message is sent to Bob by Alice using his public key and the private key d is kept secret. Bob receives the message which comes from Alice. The size of the message (plaintext) must be less then n $(P < n)$. If the message (Plaintext) is large then n, it should be divided in blocks. After that Alice sends message to Bob using public key of Bwhich is announced publicly.

Steps performed by Sender A :

1. The public key (n, e) of the B's is obtained.
2. The plaintext message is represented as a positive integer m.
3. The cipher text $C \equiv m^e(mod\ n)$ is calculated.
4. The cipher text is sent from C to B.

3) RSA Decryption: Bob receives the message which comes from Alice and Bob uses his private key to decrypt the cipher text message received. Steps performed by Recipient B :

1) The private key $(n, d)$is used to calculate$m \equiv c^d(mod\ n)$.
2) The plaintext is extracted from the message representative m.

The whole process of encryption and decryption in cryptography is shown in the following diagram:

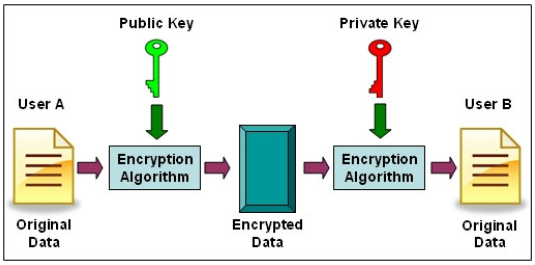

Fig. 1. RSA Encryption and Decryption.

(I) RSA Digital Signature:

Algorithm:

Key Generation : The following algorithm discusses the key generation of RSA digital signatures.

(i) Choose two large prime number p and q such that $p \neq q$.

(ii) Now, we find the product of p and q such that

$$n = p \times q.$$

(iii) Now, we calculate

$$\varphi(n) = (p-1)(q-1).$$

(iv) Selecting signing key e, such that gcd$(e, \varphi(n)) = 1$, $1 < e < \varphi(n)$.

(v) Now we find d, such that

$$ed \equiv 1(mod\ \varphi(n)).$$

Therefore, the public key is the pair (e, n), and private key is 'd'.

(I) Singing of RSA Digital Signature: We explain how Alice signs the message m.The private key is used by Alice to create a signature of the message as follows:

$s \equiv m^d(mod\ n)$, where $m = \{0,1,2, \ldots (n-1)\}$ and sends the message (encrypted as $c \equiv m^e(mod\ n)$) and signature toBob.

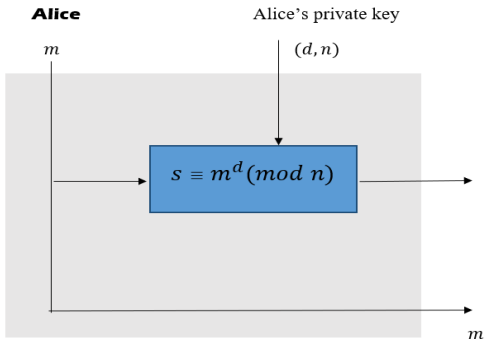

Fig. 2. Signing RSA Digital Signature.

II. VERIFYING OF RSA DIGITAL SIGNATURE

Bob wants to verify the signature $'s'$. Both m and s are received by Bob.The copy of message is created by Bob by applying the public key of Alice to signature as follows:

$$m' \equiv s^e(mod\ n)$$

and the value ofm' is compared with the value m by Bob. The message is accepted by Bob if these two are equal.

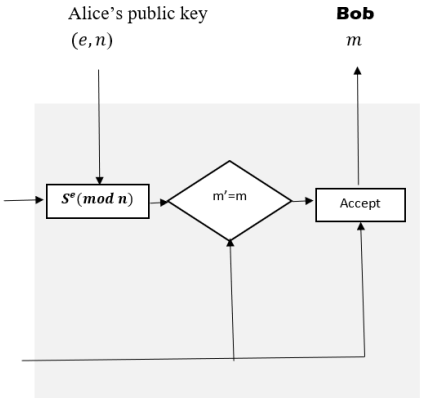

Fig: 3. Verifying RSA Digital Signature Scheme.

Verification Criteria:

Since, $s \equiv m^d (mod\ n)$.

Therefore,

$$m' \equiv s^e (mod\ n)$$

becomes

$m' \equiv (m^d)^e (mod\ n)$.

This gives

$$m' \equiv m^{de}\ (mod\ n),$$

that is

$m' = m$ [because $ed \equiv 1\ mod\varphi(n)$].

The following diagram shows the digital signature scheme:

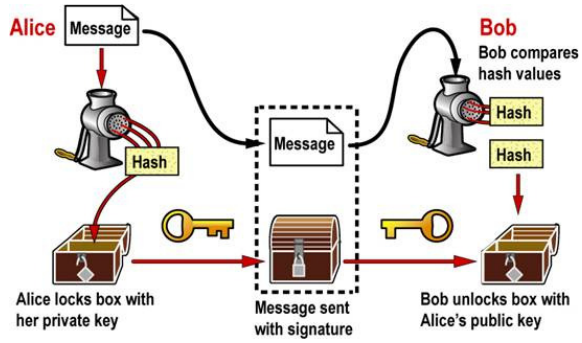

Fig. 4. Digital signature scheme.

Practical Applications:

(i) The primes p and q will be considered of equal length in bits.

(ii) Most used practical choices for e are $3, 17$ and $65537(2^{16}+1)$. These are called as Fermat primes, also rarely referred to as F_0, F_2 and F_4 respectively. The operation of modular exponentiation is made faster by choosing them. After choosing e, it is easier to check whether $gcd(e, p-1) = 1$ and $gcd(e, q-1) = 1$ while the primes are being tested and generated in step 1. Values of p and q that are not able to pass in the test can be reflected instantly.

To calculate the value of$d$, we make use of Extended Euclidean Algorithm for computing $d \equiv e^{-1} mod\ \varphi$, also written as $d \equiv \left(\frac{1}{e}\right) mod\ \varphi$. This is known as modular inversion. This is not an integer division. The modular inverse $d$is defined as the integer value such that $ed \equiv 1(\ mod\varphi(n))$. It only exists if e and φ have no common factors.

(iii) Decryption is similar to signing as far as domain of mathematics is concerned since private key is used by both of them. Similarly, the same mathematical operation is used by both encryption and verification involving the use of public key. That is, mathematically, for $m < n$

$$m \equiv (m^e\ mod\ n)^d mod\ n$$
$$\equiv (m^d mod\ n)^e mod\ n.$$

However, following significant differences of implementation are to be kept in mind:

- The message digest of the source information is used for deriving the signature. The process to be followed for deriving the message digest need to exactly same, using an identical set of data.
- The methods through which the representative integers can be derived are different for both signing and encryption.

III. ILLUSTRATION

Now we shall explain the RSA digital signature with the help of following example.

Let us take the message **"MATHEMATICS".**

STEP 1. Key Generation

Let us choose the prime numbers

$p = 47, q = 59.$

Therefore, the product of p and q is

$$n = pq$$
$$= (47)(59)$$
$$= 2773.$$

Now using Euler's totient function, we get

$$\varphi(n) = \varphi(pq)$$
$$= \varphi(p)\varphi(q)$$
$$= (p-1)(q-1).$$

This implies

$$\varphi(2773) = (47-1)(59-1)$$
$$= (46)(58) = 2668.$$

Now we choose 'e' such that $1 < e < \varphi(n)$ and

$$\gcd(\varphi(n), e) = 1.$$
$$\gcd(\varphi(n), e) = 1.$$

Let us select e = 17 such that $1 < 17 < 2668$ and gcd (2668, 17) = 1.

Now we calculate d such that

$$ed \equiv 1\ (mod\varphi(n)).$$

That is

$$17d \equiv (mod\ 2668).$$

This gives

$$d = 157.$$

STEP 2. Conversion of the English Message into the Numerical Values

Now we shall write the numerical value of the message **"MATHEMATICS"** by using the following table:

Table 1: Representation of Alphabetic and Numerical Value.

Alphabetical value	A	B	C	D	E	F	G	H	I	J	K	L	M
Numerical value	00	01	02	03	04	05	06	07	08	09	10	11	12
Alphabetical value	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical value	13	14	15	16	17	18	19	20	21	22	23	24	25

The numerical value of the message **"MATHEMATICS"** is **1200 1907 0412 0019 0802 18**.

We add slack variable "A" to make pair message "MATHEMATICSA" and its numerical value is

$$M = 1200\ 1907\ 0412\ 0019\ 0802\ 1800$$
$$= M_1M_2M_3M_4M_5M_6 \text{ (say)}.$$

STEP 3. Signing Process

We apply the signing algorithm to the message pairs and find the signature 'S' from the message.

We start with message packet M_1, thus we have

$$M_1 = 1200, \quad d = 157, \quad n = 2773.$$

Therefore,

$$S_1 \equiv M_1^d (mod\ n).$$

That is

$$S_1 \equiv (1200)^{157} (mod\ 2773).$$

Since

$$(1200)^2 \equiv 813 (mod\ 2773).$$

Therefore,

$$((1200)^2)^2 \equiv 813 \times 813 (mod\ 2773),$$

this implies

$$(1200)^4 \equiv 995 (mod\ 2773).$$

Now

$$((1200)^4)^2 \equiv 995 \times 995 (mod\ 2773)$$

gives

$$(1200)^8 \equiv 64 (mod\ 2773).$$

Therefore,

$$((1200)^8)^2 \equiv 64 \times 64 (mod\ 2773),$$

which gives

$$(1200)^{16} \equiv 1323 (mod\ 2773).$$

Now

$$((1200)^{16})^2 \equiv 1323 \times 1323 (mod\ 2773),$$

which gives

$$(1200)^{32} \equiv 566 (mod\ 2773).$$

Therefore,

$$((1200)^{32})^2 \equiv 566 \times 566 (mod\ 2773),$$

which gives

$$(1200)^{64} \equiv 1461 (mod\ 2773).$$

Now

$$((1200)^{64})^2 \equiv 1461 \times 1461 (mod\ 2773),$$

which gives

$$(1200)^{128} \equiv 2084 (mod\ 2773).$$

Therefore

$$(1200)^{128}(1200)^{16} \equiv 2084 \times 1323 (mod\ 2773)$$

gives

$$(1200)^{144} \equiv 770 (mod\ 2773).$$

Now

$$(1200)^{144}(1200)^8 \equiv 770 \times 64 (mod\ 2773)$$

gives

$$(1200)^{152} \equiv 2139 (mod\ 2773).$$

Therefore

$$(1200)^{152}(1200)^4 \equiv 2139 \times 995 (mod\ 2773)$$

gives

$$(1200)^{156} \equiv 1414 (mod\ 2773).$$

Now

$$(1200)^{156}(1200)^1 \equiv 1414 \times 1200 (mod\ 2773).$$

This implies

$$(1200)^{157} \equiv 2497 (mod\ 2773).$$

Therefore, the value of signature for the message packet M_1 is

$$S_1 = 2497.$$

Now we shall take the next pair of the message M.

Thus we have $M_2 = 1907,\ d = 157,\ n = 2773$.

Therefore,

$$S_2 \equiv M_2^d (mod\ n)$$

becomes

$$S_2 \equiv (1907)^{157} (mod\ 2773).$$

This gives

$$S_2 = 0239.$$

Now we shall take the third pair to find its equivalent signature value. Thus we have

$M_3 = 0412,\ d = 157,\ n = 2773$.

Therefore,

$$S_3 \equiv M_3^d (mod\ n)$$

becomes

$$S_3 \equiv (0412)^{157} (mod\ 2773).$$

This gives

$$S_3 = 0707.$$

Further, we have the fourth pair of the message to obtain its signature value. Thus we have

$M_4 = 0019,\ d = 157,\ n = 2773$.

Therefore,

$$S_4 \equiv M_4^d (mod\ n)$$

becomes

$$S_4 \equiv (0019)^{157} (mod\ 2773).$$

This gives

S_4=1537

Now we consider the fifth pair for its equivalent signature value. Thus we have

$M_5 = 0802,\ d = 157,\ n = 2773$.

Therefore,

$$S_5 \equiv M_5^d (mod\ n)$$

becomes

$$S_5 \equiv (0802)^{157} (mod\ 2773).$$

This gives

$$S_5 = 0723.$$

Further, we take the last pair of the message to obtain its corresponding signature value. Thus we have

$M_6 = 1800,\ d = 157,\ n = 2773$.

Therefore,

$$S_6 \equiv M_6^d (modn)$$

becomes

$$S_6 \equiv (1800)^{157} (mod\ 2773).$$

This gives

$$S_6 = 0741.$$

Now we shall show the signature of different packet of the message in the following table

Table 2: Representation of Signature.

Message Packet Value	Private Key d	ModulusValue n	Corresponding Signature Packets Value
$M_1 = 1200$	157	2773	$S_1 = 2497$
$M_2 = 1907$	157	2773	$S_2 = 0239$
$M_3 = 0412$	157	2773	$S_3 = 0707$
$M_4 = 0019$	157	2773	$S_4 = 1537$
$M_5 = 0802$	157	2773	$S_5 = 0723$
$M_6 = 1800$	157	2773	$S_6 = 0741$

Hence, we get signature

$$S = (2497\ 0239\ 0707\ 1537\ 0723\ 0741)$$

from the message.

STEP 4. Verifying Process

Now the receiver will verify the obtain signature string of numerical values.

The receiver has the signature string as follows

$$S = (2497\ 0239\ 0707\ 1537\ 0723\ 0741)$$
$$= S_1S_2S_3S_4S_5S_6.$$

We start with the first packet of signature S. Thus we have

$$S_1 = 2497, \quad e = 17, \quad n = 2773.$$

Therefore,

$$M_1 \equiv S_1^e (mod\ n)$$

becomes

$$M_1 \equiv (2497)^{17} (mod\ 2773).$$

Since

$$(2497)^2 \equiv 1305 (mod\ 2773).$$

Therefore

$$((2497)^2)^2 \equiv 1305 \times 1305 (mod\ 2773)$$

gives

$$(2497)^4 \equiv 403\ (mod\ 2773).$$

Now

$$(2497)^4)^2 \equiv 403 \times 403 (mod\ 2773)$$

gives

$$(2497)^8 \equiv 1575 (mod\ 2773).$$

Now

$$(2497)^8)^2 \equiv 1575 \times 1575 (mod\ 2773),$$

which gives

$$(2497)^{16} \equiv 1563 (mod\ 2773).$$

Therefore

$$(2497)^{16}(2497)^1 \equiv 1563 \times 2497 (mod\ 2773)$$

gives

$$(2497)^{17} \equiv 1200 (mod\ 2773).$$

Thus the value of

$$M_1 = 1200.$$

Now we take the second pair S_2 to verifying the message. Thus, we have

$$S_2 = 239, \quad e = 17, \quad n = 2773.$$

Therefore,

$M_2 \equiv S_2^e (mod\ n)$f

becomes

$$M_2 \equiv (0239)^{17} (mod\ 2773).$$

which gives

$$M_2 = 1907\ .$$

Now we consider the third pair S_3 of the signature to verify the message. Thus, we have

$$S_3 = 0707, \quad e = 17, \quad n = 2773$$

Therefore,

$$M_3 \equiv S_3^e (mod\ n)$$

becomes

$$M_3 \equiv (0707)^{17} (mod\ 2773).$$

This gives

$$M_3 = 0412.$$

Now we shall obtain the message of the fourth signature packets. Thus, we have

$$S_4 = 1537, \quad e = 17, \quad n = 2773$$

Therefore,

$$M_4 \equiv S_4^e (mod\ n)$$

becomes

$$M_4 \equiv (1537)^{17} (mod\ 2773).$$

This gives

$$M_4 = 0019.$$

Further, we take the next pair of signature to obtain its equivalent original message. Thus, we have

$$S_5 = 0723, \quad e = 17, \quad n = 2773$$

Therefore,

$$M_5 \equiv S_5^e (mod\ n)$$

becomes

$$M_5 \equiv (0723)^{17} (mod\ 2773).$$

This gives

$$M_5 = 0802.$$

Now we verify the final packet of the signature. Here, we have

$$S_6 = 0741, \quad e = 17, \quad n = 2773.$$

Therefore,

$$M_6 \equiv S_6^e (mod\ n)$$

becomes

$$M_6 \equiv (0741)^{17} (mod\ 2773).$$

This gives

$$M_6 = 1800.$$

The values obtain of the message packets for the corresponding signatures packets is shown in the following table.

Table 3: Representation of Original Message.

Signature Packets Value	Public Key Value e	Modulus Value n	Corresponding Message Packets Value
$S_1 = 2497$	17	2773	$M_1 = 1200$
$S_2 = 0239$	17	2773	$M_2 = 1907$
$S_3 = 0707$	17	2773	$M_3 = 0412$

$S_4 = 1537$	17	2773	$M_4 = 0019$
$S_5 = 0723$	17	2773	$M_5 = 0802$
$S_6 = 0741$	17	2773	$M_6 = 1800$

Hence, we get a message

1200 1907 0412 0019 0802 1800.

which is same as the numerical value of the original message

"MATHEMATICS".

Therefore, the message has been verified by the digital signature.

IV. CONCLUSION

In the present scenario we discussed the RSA Cryptosystem and the Digital Signature schemes. The RSA public key cryptosystem is more useful for the digital signatures scheme. Further, we explained the digital signature scheme and mathematical structure of RSA.

REFERENCES

[1]. Bakhtiari, S., Safavi-Naini, R., &Pieprzyk, J. (1995). *Cryptographic hash functions: A survey* (Vol. 4). Technical Report 95-09, Department of Computer Science, University of Wollongong.

[2]. Brickell, E. F. (1989, August). A survey of hardware implementations of RSA. In *Conference on the Theory and Application of Cryptology* (pp. 368-370). Springer, New York, NY.

[3]. Buchmann, J. A., Karatsiolis, E., &Wiesmaier, A. (2013). *Introduction to public key infrastructures.* Springer Science & Business Media.

[4]. Davida, G. I. (1982). *Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem.* Department of Electrical and Computer Science, College of Engineering and Applied Science, University of Wisc.

[5]. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[6]. Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security*. Mc Graw Hill Education (India) Private Limited.

[7]. Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.

[8]. Lipton, S. M., & Matyas, S. M. (1978). Making the digital signature legal--and safeguarded. *Data Communications*, *7*, 41-52.

[9]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

[10]. Potter, R. J. (1977). Electronic mail. *Science*, 195(4283), 1160-1164.

[11]. Preneel, B., Govaerts, R., & Vandewalle, J. (1989). *Cryptographically secure hash functions: an overview.* In: ESAT Internal Report, KU Leuven.

[12]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[3]. Schneier, B., & Kelsey, J. (1998, January). Cryptographic support for secure logs on untrusted machines. In *USENIX Security Symposium* (Vol. 98, pp. 53-62).

[14]. Sharma, A. K. (2018). Content-Based Filtering in MovieRecommendation. *International Journal of Electrical, Electronics and Computer Engineering*, *7*(2): 106-109.

[15]. Sharma, A. K. (2019). Design and Mathematical Structure of Cryptographic Hash Function SHA-512. *International Journal of Theoretical & Applied Sciences, 11*(2): 41-47.

[16]. Sharma, A. K. (2019). Safety Application in Android. *International Journal on Emerging Technologies, 10*(1): 234-238.

[17]. Sobti, R., & Geetha, G. (2012). Cryptographic hash functions: a review. *International Journal of Computer Science Issues (IJCSI)*, *9*(2), 461.

[18]. Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

[19]. Stinson, D. R., & Paterson, M. (2018). Cryptography: Theory and practice. CRC press.

[20]. Stinson, D. R. (2006). Some observations on the theory of cryptographic hash functions. *Designs, codes and Cryptography, 38*(2), 259-277.

[21]. Trappe, W. (2006). *Introduction to cryptography with coding theory*. Pearson Education India.