# Modified RSA Digital Signature Scheme for Data Confidentiality

Kamal Kr. Gola
M.Tech Student at CS and E Deptt.
Uttarakhand Technical University
Uttarakhand

Bhumika Gupta
Asst. Prof., Dept. of CS and E
G.B. Pant Eng. College
Pauri Garwal, U.K., India

Zubair Iqbal
Asst. Prof., Dept. of CS and IT,
Moradabad Institute of Technology
Moradabad, U.P., India

## ABSTRACT

As we know that digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. This signature guarantees the source authenticity and integrity of a message. Digital signature provides three types of services such as authentication, message integrity and non-repudiation, but does not provide the confidentiality of data which is most important during data transfer because the data is very sensitive. In this paper, we proposed a modified RSA digital signature scheme for data confidentiality. The main purpose of this approach is to provide the data confidentiality during the data transfer. To achieve this we are using the concept of public key encryption.

## General Terms

Document Security

## Keywords

RSA digital signature scheme, Public key, private key, prime number, digital signature, public key encryption, plain text, cipher text, message (Data)

## 1. INTRODUCTION

A digital signature is a mathematical scheme for implementing the authenticity of a digital message or document. A digital signature algorithm is a public key cryptographic algorithm that is designed to protect the authenticity of a digital message or document. A message is signed by a secret key of the sender to produce a signature and the signature is verified against the message by a public key. Thus any party can verify the signatures, but only one party with the secret key can sign the messages. A valid digital signature ensures that the message was created by a known sender who have the valid secret key, and that it was not altered in transit. Digital signatures are used widely in e-commerce applications, banking applications, in software distribution, and in other cases where jurisdiction is involved and it is important to detect forgery or tampering. Thus, it is crucial to use algorithms that have been standardized by government organizations. Even though there are a numerous number of digital signature algorithms in research literature, only three algorithms have been standardized by the National Institute of Standards and Technology (NIST) and have been widely used in almost all commercial applications. These are the RSA, the DSA and the ECDSA [1] [2]. Digital signatures are strong tools applied in order to achieve the security services of authentication (proof of identity of the sender), data integrity (detection of changes to the message) and non-repudiation (prevention of denial of sending the information). They are the digital counterpart of handwritten signatures that can be transmitted over a computer network. Only the sender can make the signature, but other people can easily recognize as belonging to the sender. The sender produces a signature consisting of a number associating a message (in digital form) with a secret key. The digital signature is analogous to the handwritten. Digital signature provides three types of services such as authentication, message integrity and non-repudiation.

**Authentication:** Authentication is a procedure to verify that received messages come from the valid source. It must verify the author and the date and time of the signature.

**Message integrity:** it must authenticate the contents at the time of the signature and does not alter during data transfer. If the message has been changed, then we cannot get the same signature.

**Non-repudiation:** It means that the signer (sender) cannot claim that they did not sign the document or message.

## 2. TRADITIONAL RSA DIGITAL SIGNATURE SCHEME

The RSA digital signature scheme is an asymmetric digital signature algorithm which uses a pair of keys, one of which is used to sign the data in such a way that it can only be verified with the other key. In this scheme a pair of keys of the sender is used. The algorithm is as follows:

- Key generation process
- Signing process
- Verifying process

**In the key generation process** sender generates a pair of keys known as public key and private key. The public key is known to both (sender and receiver) while the private key is only known to sender only. The key generation process is same as in RSA algorithm.

**In the signing process** the sender generates the digital signature using own private key and send the message (data) and signature by the receiver.

**In the verifying process** the receiver receives the message (data) and the signature and perform the verifying process using the sender’s public key and compare that if the generated copy of message (data) if equal to the received message (data) then it verify the signature otherwise it reject the signature.

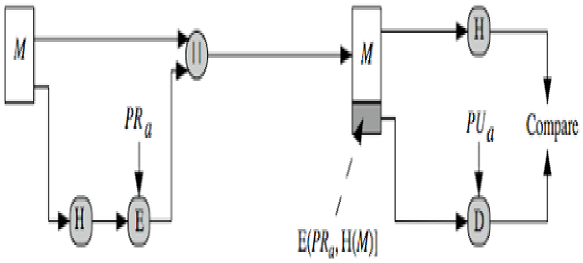


**Fig 1: RSA Digital Signature Scheme**

## 3. LITERATURE REVIEW

In the RSA Digital Signature Scheme proposed combined signing and public-key encryption. For example, Alice wishes to send a signed, encrypted message to Bob. Given a plaintext x, Alice would compute her Signature y = sig Alice(x), and then encrypt both x and y using Bob‟s public encryption function eBob, obtaining z = eBob (x, y). The ciphertext z would be transmitted to Bob. When Bob receives z, he first decrypts it with his decryption function dBob to get (x, y). Then he uses Alice‟s public verification function to check that ver Alice(x,y) = true[3] [4].

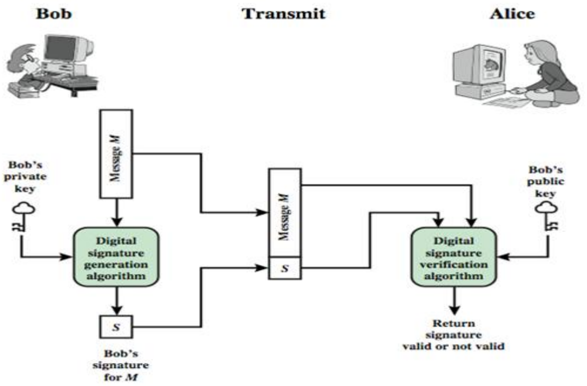

Bob
Transmit
Alice
Bob's private key
Message M
Digital signature generation algorithm
S
Bob's signature for M
Message M
S
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

**Fig 2: RSA Digital Signature Scheme**

ElGamal Signature Scheme, described in a 1985 paper. A modification of this scheme has been adopted as a digital signature standard by the National Institute of Standards and Technology (NIST). The ElGamal Scheme is designed specifically for the purpose of signatures, as opposed to RSA, which can be used both as a public-key cryptosystem and a signature scheme. The ElGamal Signature Scheme is non-deterministic, as was the ElGamal Public-key Cryptosystem. This means that there are many valid signatures for any given message. [5]

Aqeel Khalique Kuldip Singh Sandeep Sood in 2010 proposed the implementation of ANSI X9.62 ECDSA over elliptic curve and discusses related security issues. The main reason for the attractiveness of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. Hence, it takes full exponential time to solve while the best algorithm known for solving the underlying integer factorization of RSA and discrete logarithm problems in DSA both take sub exponential time. The key generated by the implementation is highly secured and it consumes lesser bandwidth because of small key size used by the elliptic curves. Significantly smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA but with equivalent levels of security.[6]

Sushila Vishnoi, Vishal Shrivastava in 2012 has been proposed a new variant of digital signature algorithm which is based on two hard problems, one is prime factorization and other is discrete logarithm. It is shown that one has to solve both the problems simultaneously for cryptanalysis of this algorithm. The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems. [7]

Mr. Hemant Kumar, Dr. Ajit Singh proposed in June 2012 has been proposed an algorithm which is based on the RSA algorithm with some modification and included more security. In this algorithm authors have an extremely large number that has two prime factors that are not equal to each other (similar to RSA). In addition to this authors have also used two natural numbers in pair of keys (public, private) with the help of these natural number authors increases the security of the cryptosystem. If the security of this method proves to be adequate, it permits secure communication to be established without the use of carriers to carry keys. In this paper, a new algorithm has been designed for generating signature that overcomes the Shortcomings of the RSA system, also the new algorithm can be achieved high security for digital signature. [8]

Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidithis has been proposed a new variant of digital signature algorithm which is based on linear block cipher or Hill cipher initiate with Asymmetric algorithm using mod 37. In this author discuss various several signature schemes. First is the question of signing a document. With a conventional signature, a signature is physically part of the document being signed. However, a digital signature is not attached physically to the message that is signed, so the algorithm that is used must somehow "bind" the signature to the message. Second is the question of verification. A conventional signature is verified by comparing it to other, authentic signatures [9].

## 4. PROPOSED ALGORITHM

**Key generation process (at Sender side)**

i) Select p and q with the condition that p and q both prime and p does not equal to q.

ii) Calculate n=p*q

iii) Calculate Ø (n) = (p-1)*(q-1)

iv) Select integer e gcd (Ø (n), e) =1; 1<e<Ø (n)

v) Calculate d e*d=1 mod Ø (n)

vi) Public key (e, n)

vii) Private Key (d, n)

**Key generation process (at Receiver side)**

i) Select p1 and q1 with the condition that p1 and q1 both prime and p1 does not equal to q1.

ii) Calculate n1=p1*q1

iii) Calculates Ø (n1) = (p1) -1 * (q1) -1

iv) Select integer e1 gcd (Ø (n1), e1) =1; 1<e1<Ø (n)

v) Calculate d1 e1*d1=1 mod Ø (n1)

vi) Public key (e1, n1)

vii) Private Key (d1, n1)

**Signing process**
Signer using his/her private key to create a signature S is using S =M$^d$ mod n and send the data and the signature (S) to the receiver.

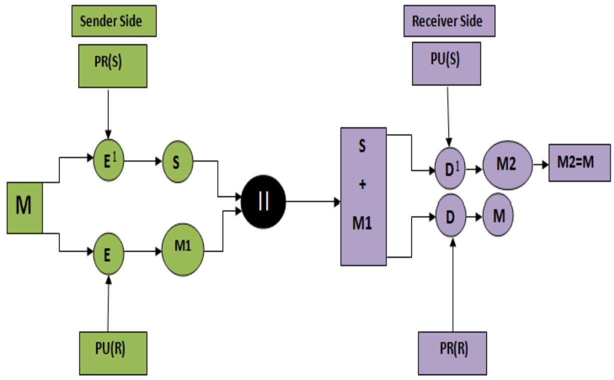
**Encryption process**

i) Before sending the data and signature to the receiver, the sender encrypts the data using K=M$^{e1}$ mod n where M is data and e1 is the public key of the receiver.

ii) Now sender sends the encrypted data and signature to the receiver.

**Decryption process**
Now Receiver receives the data and the signature and perform the decryption process using M=K$^{d1}$ mod n where M is the original data, d1 is the private key of the receiver and k is the encrypted data.

**Verifying process**
Now receiver performs the verifying process using M1= S$^e$ mod n. Where M1 is a copy of the data, S is the signature and e is the public key of the sender. If M1=M then the signature is verified.



Where M=Message(Data) , E=Encryption , PR(S)=Sender 's Private Key , PU(R)=Receiver 's Public Key S=Signature , M1=Encrypted Message(Data) , PU(S)=Sender 's Public Key , D=Decryption , M2=Copy of Message(Data) , PR(R)=Receiver 's Private Key , E$^1$=Digital Signature Generation Algorithm , D$^1$= Digital signature verification algorithm

**Fig 3: Proposed Model of Modified RSA Digital Signature Scheme for data confidentiality**

## 5. IMPLEMENTATION

**Key generation process (at sender side)**

The first sender selects two prime numbers given as p and q that are known to sender only.

P=7 and q=17

Now it will calculate the value of n and Ø (n)

Values of n will be calculated by n=p * q.

n=7*17=119

Now calculate the value of Ø (n) = (p-1) * (q-1).

Ø (n)=6 * 16=96

Now the sender will choose public key e such that e < Ø (n) and GCD (e, Ø (n)) =1.

e =5.

Now sender calculates the private key d using given expression.

e*d=1modØ (n)

(5 * d) mod 96=1

d=77.

**Key generation process (at receiver side)**
Now the receiver selects two prime numbers p1 and q1 that are only known to the receiver only.

p1=17 and q1=11

Now it will calculate the value of n1 and Ø (n1)

Values of n will be calculated by n1=p1 * q1.

n1=17*11=187

Now calculate the value of Ø (n1) = (p1) -1 * (q1) -1.

Ø (n1) =16 * 10=160

Now the receiver will choose public key e1 such that e1 < Ø (n1) and GCD (e1, Ø (n1)) =1.

e1 =7.

Now receiver calculates the private key d1 using given expression.

e1*d1=1modØ (n)

(7 * d1) mod 60=1

d1=23.

In proposed technique public key of both (sender and receiver) are known to each other. Now sender generate the digital signature using own private key (d).

**Signing Process**
S=M$^d$ mod n

Where S is a digital signature at the sender side.

M is the data

d is a private key

n is the multiplication of two prime numbers.

For implementation purposes lets M=88

S=88$^{77}$ mod 119

= (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (88$^5$ mod 119) * (885 mod 119) * (885 mod 119) * (885 mod 119) * (88$^5$ mod 119) * (88$^2$ mod 119)

= (107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 107 * 9) mod 119

= (30 * 30 * 30 * 37) mod 119

= 999000 mod 119

**S= 114 (Digital signature at sender side)**

**Encryption process**
Before sending the data and signature to the receiver, the sender encrypts the data using receiver's public key.

K=M$^{e1}$ mod n where M is data and e1 is the public key of the receiver.

K=$88^7$ mod 187

= ($88^3$ mod 187) * ($88^3$ mod 187) * (88 mod 187)

= (44 * 44 * 88) mod 187

= 170368 mod 187

**K = 11(Encrypted data at sender side)**

**Decryption process**
Now Receiver receives the data and the signature and perform the decryption process using M=Kd1 mod n where M is the original data, d1 is the private key of the receiver and k is the encrypted data.

M= $11^{23}$ mod 187

= ($11^4$ mod 187) * ($11^4$ mod 187) *($11^4$ mod 187) *(114 mod 187) *($11^4$ mod 187) *($11^3$ mod 187)

= (55 * 55 * 55 *55 *55) mod 187 *(113 mod 187)

= (33 *33*55*11*11*11) mod 187

**M=88 it proved that data is confidential.**

**Verifying process**
Now receiver performs the verifying process using M1= $S^e$ mod n. Where M1 is a copy of the data, S is the signature and e is the public key of the sender. If M1=M then the signature is verified.

M1= $114^5$ mod 119

= ($114^2$ mod 119) * ($114^2$ mod 119) * (114 mod 119)

= (25 * 25 * 114) mod 19

= 71250 mod 119

**M1= 88=M its provide the authentication.**

## 6. CONCLUSION

In this work a modified RSA digital signature scheme for data confidentiality based on public key encryption has been proposed. By doing implementation this scheme showed that the proposed technique provides the security during data transfer as compared to existing RSA digital signature scheme. The important concept of any algorithm satisfying security, it is one of the most important goals of the digital signature scheme. In the existing scheme, there is no security for the data, it only provides the user authentication, but the proposed scheme provides data security. Also, it ensures the data confidentiality, integrity of data and user authentication. The implementation results show that the proposed method has improved the security and performance of digital signature, while providing high quality of service and security for desired digital signature scheme.

## 7. REFERENCES

[1] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards 186–3.

[2] National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards 180–3.

[3] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition 2007, Tata McGrawHill Publishing Company Limited, New Delhi.

[4] William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Pearson Education.

[5] Douglas Stinson, Cryptography Theory and Practice, by CRC Press, 1995.

[6] Aqeel Khalique, Kuldip Singh Sandeep Sood, Implementation of Elliptic Curve Digital Signature Algorithm, International Journal of Computer Applications, May 2010.

[7] Sushila Vishnoi, Vishal Shrivastava, International Journal of Computer Trends and Technology, ISSN: 2231-2803, 2012.

[8] Mr. Hemant Kumar, Dr. Ajit Singh, An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography, IJRREST, June 2012.

[9] Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidithis, A new efficient digital signature scheme algorithm based on block ciphers, IOSR Journal of Computer engineering (IOSRJCE) ISSN: 227s8-0661, ISBN: 2278-8727Volume 7, Issue 1 (Nov. - Dec. 2012), PP 47-52