Indian J.Sci.Res. 17(2): 99 - 101, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

IMPLEMENTATION OF RSA WITH DIGITAL SIGNATURES USING FOUR PRIME NUMBERS

[1]A.Gayathri, [2]K.Ravisagar, [3]E.Pragnavi
[1,2,3] Department of Computer Science and Engineering, University College of Engineering, Osmania University, Hyderabad

Abstract – Digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable; if a dispute arises as to whether a party signed a document (caused by either a lying signer trying to repudiate a signature it did create, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information (private key). The first method discovered was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Sub-sequent research has resulted in many alternative digital signature techniques.RSA algorithm is used to hide and retrieve thedata in an insecure network environment. The advantage of RSAalgorithm is to increase security and accessibility. The privatekeys never required to be transferred or exposed to everybody.In a shared-key cryptographic system, the secret keys must beshared since exactly the same key is used for encryption anddecryption. So there may be a chance that an intruder can findthe secret key during the data transmission. Thecenter of this paper is to talk about how to securecorrespondences that happen in an exchange in order todirect against fraudsters and in different situations by using RSA algorithm with four prime numbers.

Keywords --Digital signature,RSA algorithm, Encryption, Decryption,Security.

Limitations in Symmetric key Cryptography:

Symmetric cryptosystems have a problem of key transportation. The secretkey is to be transmitted to

the receiving system before the actual message is transmitted. Every means of electronic communication is insecure as it isimpossible to guarantee that no one will be able to tap communicationchannels. So the only secure way of exchanging keys would be exchangingthem personally.

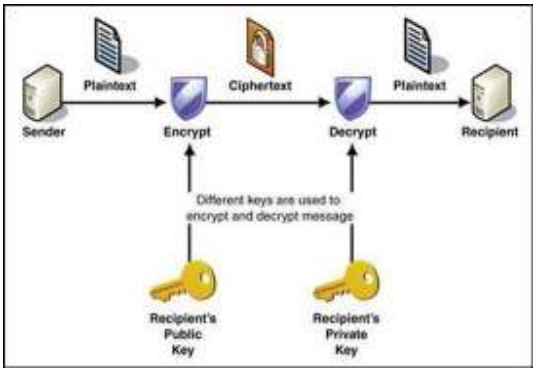


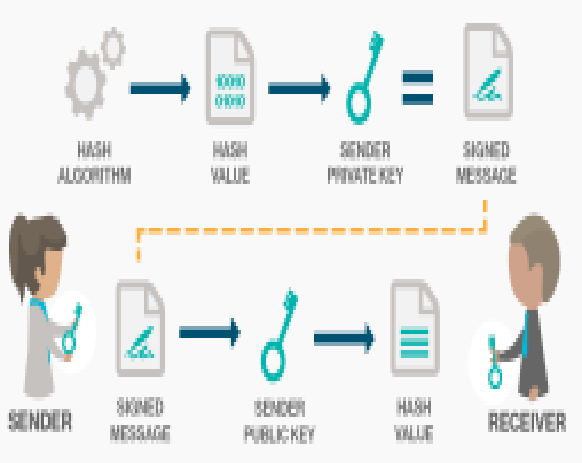
Fig-1: Process model of Asymmetric Key Cryptography

I. Introduction

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications.Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way or the signature was created with a private key that doesn't correspond to the public key presented by the signer.



Propelled check approval arranges givesecure correspondence minimum computational costfor steady applications, for instance, electronicexchange, electronic voting etc. Use ofcryptographic counts to guarantee unmistakableverification, affirmation or data stockpiling has beenthe prime focus in cryptographic field exceptionallyfor more diminutive handheld devices.

RSA is the essential estimation alluded to besensible for stamping and what's more encryption,and one of the fundamental marvelous advances outin the openkey cryptography. PropelledSignatureCalculation(DSA) which gives mechanized markcapacity to the confirmation of messages. RSA is an Open KeyCryptography(PKC) is based upon prime numbers and which is used to be expected forcontraptions with limited computation control as wellas memory, for instance, smartcards and PDAs.

To framework and change of a count forexecuting Safety efforts using Python programminglingo with online based. The computation is to beproposed for Effective Counts and Investigation. Python

Cryptography Toolbox is an aggregation ofnumber of different estimations, for instance,Encryption counts, Hash computations and open keyfiguring.Python code is to be irrelevant to supplantone computation with another which modules thatexecute a particular class of estimation offering distinct interfaces, and factors parameter zing themodule's ascribes are open to help in programmingportably.

II. Analysis of Existing Algorithms

RSA Algorithm

RSA, is a open key assume that usages simply basicnumber speculation in its delineation.

Here are a couple of things that can turn out badly.

1) Using small primes.

This one is quite obvious, if the primes used are smallenough then a computer will make easy work offactorizing.

2) Using primes that are very close.

This is quite a serious weakness because it makes abig flaw, even if you do use big enough primes.

If are relatively close then searchingfor prime factors in the vicinity of will revealeither of the factors in quite a quick time

Algorithm For The Generation of Key pair

1. Long Integer w, x , y, z; #w,x,y,z are the four prime numbers. #long integer n=0; N is any large number initialized to zero#

Long integer F(n): # productive function #integer p; # any integer between 1 and f(n) #integer d ; #any integer between 1 and f(n)#

2. Choose four large prime numbers w, x, y, z randomly and independently of each other. All prime numbers should be equivalent in length.

3. n= wxyz;

4. f(n)= (w-1)(x-1)(y-1)(z-1);

5. Choose an integer e, where 1<e<f(n) such that gcd(e, f(n))=1 and e and f(n) are co-prime

6. Compute the secret exponent d, where

1<d<f (n) such that (e*d) modf(n)=1

7.'d' should be kept private

8. Public key: (e,n);

9. Private key: (d,n);

III. Conclusion

RSA with four prime numbers gives more complex secret key and Key not decrypted by the third party and the prime numbers are low so that the memory consumption and time complexity for the algorithm is reduced compared to the existing algorithms.

References

[1] High speed efficient advanced encryption standard implementation

[2] Implementation of RSA

[3] An efficient implementation of RSA Digital signature algorithm

[4] William Stallings: Cryptography and Network Security: Principles and Practices, 4th edition

Prentice Hall

[5] Sonal Sharma, " RSA algorithm using modified subset sum Cryptosystem" Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011

[6] R. Rivest, A.Shamir and L.Adleman, " A method for obtaining digital Signatures and public key cryptosystems", "communication of the Association for computing machinery "1978,pp 120-126.

[7] M. Bishop, Introduction to Computer Security. Reading, MA:Addison-Wesley, 2005.

[8] Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model Author: Jorge L´opezHern´andez-Ardieta Supervisor: Prof. Dr. Ana Isabel Gonz´alez-TablasFerreres COMPUTER SCIENCE