UGC Approved Journal
Research Link

Since March 2002

An International, Registered & Refereed Monthly Journal : Computer Science
Research Link - 170, Vol - XVII (3), May - 2018, Page No. 11-12
ISSN - 0973-1628 ■ RNI - MPHIN-2002-7041 ■ Impact Factor - 2015 - 2.782

RSA Algorithm in Cryptography

One of the main challenges of resource sharing on data communication network is its security. This is premised on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. This paper presents a design of data encryption and decryption in a network environment using RSA algorithm. The algorithm allows a message sender to generate a public key to encrypt the message and the receiver is sent a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message but to a form different from the original message. Key Words : Encryption, Decryption, Key.

Ms. Neena

Introduction :

Cryptography a playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day to day life because thousands of people interact electronically every day through e-mail,e-commerce, ATM machines,cellular phones etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users.

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Terminology used in cryptography :

(1) Plaintext (Clear text) : The intelligible message which will be converted into an unintelligible (encrypted) message.

(2) Cipher text : A message in encrypted form.

(3) Encryption : The process of converting a plaintext message into a cipher text message.

(4) Decryption : The process of converting a cipher text message into a plaintext message.

(5) Key : A parameter used in the encryption and decryption process.

(6) Cryptosystem : A system to encrypt and decrypt information.

(7) Symmetric Cryptosystem : A cryptosystem that uses the same key to encrypt and decrypt information.

(8) Asymmetric Cryptosystem : A cryptosystem that uses one key to encrypt and a different key to decrypt.

(9) Cryptography : The use of cryptosystems to maintain the confidentiality of information.

(10) Cryptoanalysis : The study of breaking cryptosystems.

Cryptography is also known as cryptology.

Modern cryptography concerns itself with the following four objectives :

(1) Confidentially : The information cannot be understood by anyone for whom it was unintended.

(2) Integrity : The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

(3) Non-repudiation : The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

(4) Authentication : The sender and receiver can confirm each other's identity and the origin/destination of the information.

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

(a) Secret Key Cryptography (SKC) : Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption/private key cryptography.

(b) Public Key Cryptography (PKC) : Here two keys are used. This type of encryption is also called asymmetric

Assistant Professor (Department of Computer Science), S.D. College, Hoshiarpur (Punjab)

encryption. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver's public key. The receiver decrypts the message using his/her private key. For nonrepudiation, the sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows who sent it.

(c) Hash Functions : These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

The growth of the Internet and electronic commerce have brought to the forefront the issue of privacy in electronic communication. Large volumes of personal and sensitive information are electronically transmitted and stored every day. For this purpose, I described about RSA Algorithm.The RSA Algorithm is named after Ron Rivest,Adi Shamir and Leonard Adleman who inverted it in 1977, MIT (MASSACHUSELTS INSTITUTE OF TECHNOLOGY). It is asymmetric cryptography algorithm .It is normally used for encrypt and decrypt messages.RSA is a cryptosystem for public key encryption and is widely used for securing sensitive data.

Some of the famous security system which is composed of three faces, such as :

(A) RSA Key Generation Algorithm.

(B) Encryption Algorithm.

(C) Decryption Algorithm.

(A) RSA Key Generation Algorithm :

(1) Generate two large random primes p,and q

(2) Compute n=p*q

(3) Phi=(p-1)(q-1)

(4) Choose an integer e , 1<e<phi such that gcd(e,phi)=1

(5) Compute the secret exponent d, 1<d<phi such that ed=1(mod phi).

(6) The public key is (n,e) and the private key is (n,d). keep all the d,p,q and phi secret.

(i) n is known as the modulus.

(ii) e is known as the public exponent or encryption exponent or just the exponent.

(iii) d is known as the secret exponent or decryption exponent.

(B) Encryption Algorithm :

Sender a does the following :

(1) Obtains the recipient B's public key(n,e).

(2) Represents the plaintext message as a positive integer m.

(3) Computes the cipher text c=me mod n.

(4) Sends the cipher text c to B

(C) Decryption Algorithm :

Recipient B does the following:-

(1) Uses his private key (n,d) to compute m=cd mod n.

(2) Extracts the plaintext from the message representative m.

(A) working example :

(1) Choose two random prime numbers

(2) P=11,q=3 compute n=p*q

(3) n =11*3=33

(4) compute phi=(p-1)(q-1)

(5) phi=(11-1)(3-1)=10*2=20

(6) choose an integer 'e' 1<e<phi or gcd(e,phi)=1 , 1<e<20

choose e=3

Checkgcd(e,p-1)=gcd(3,10)= (3 and 10 have no common factors except 1)

Checkgcd(e,q-1)=gcd(3,2) = 1

therefore gcd(e,phi)=gcd(e,(p-1)(q-1))=gcd(3,20)=1

(7) calculate d such that ed=1 (mod phi)

compute d=e-1 mod phi = 3-1 mod 20

find a value of d such that phi divides (ed-1)

find d such that 20 divides 3d-1

simple testing (d = 1,2,…) gives d=7

check ed-1 =3*7-1=20 which is divisible by phi

(8) public key =(n,e)=(33,3)

private key = (n,d)=(33,7)

This is actually the smallest possible value for the modulus n for which the RSA

Algorithm works Now we want to encrypt the message m=7,

C=me mod n=73 mod 33=343 mod 33=13

Hence cipher text c=13

(9) To check decryption we compute :

m=memod n=137 mod 33=7

Compute m=cd mod n.

Note that we don't have to calculate the full value of 13 to the power 7 here.

Make use of fact that a=bc mod n=(b mod n).(c mod n) mod n

So we can break down a potentially large number into its components and combine the results of easier,smaller calculations to calculate the final value.

m = 137 mod 33=13(3+3+1) mod 33=133.133.13 mod 33

=(133 mod 33).(133 mod 33).(13 mod 33) mod 33

=(2197 mod 33).(2197 mod 33).(13 mod 33) mod 33

= 19.19.13 mod 33= 4693 mod 33

=7

References :

__(1)__ M.Preethaeral.International Journal of Computer Science and Mobile Computing Vol 2 issue 6, june,2013 pg 126-139. __(2)__ American Journal of Engineering Research (AJER) 2015 (www.ajer.org) __(3)__ International Journal of Engineering And Computer Science ISSN:2319-7242 vol issue 2 nov, 2012 page no 63-66 www.ijecs.in __(4)__ IJCSNS International Journal of Computer Science and Network Security vol 13 no 7 july 2013. __(5)__ https://simple.wikipedia.org/wiki/RSA_algorithm