Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

A STUDY ON SECURITY USING RSA PUBLIC KEY CRYPTOGRAPHY

Dr P.J. Arul Leena Rose

Associate Prof,Dept. of Computer Application, FSH, SRMIST, Chennai – 603 203.

ABSTRACT:- *Cryptography is the art of secret writing. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it.A Message in its original form is known as plain text or clear text. The mangled information is known as encryption. The reverse of encryption is called decryption.The main type of cryptographic Algorithm is Public key cryptography.*

Public key cryptography is very useful because network security based on Public key technology tends to be more easily configurable. Public key cryptography might be used in the beginning of communication for authentication and to establish a temporary shared secret key, then the secret key is used to encrypt the remainder of the conversation using secret key technology.

RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The Key-pair is derived from a large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n from this information alone and that is what makes the RSA algorithm so secure.

Keywords: *RSA, Public key, Authentication*

1. INTRODUCTION

When the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce and communication, security becomes a tremendously issue to deal with.

1.1. The purpose of Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.Within the context of any application-to-application communication, there are **some specific security requirements,** including:
Authentication : The process of proving one's identity.
Privacy/confidentiality : Ensuring that no one can read the message except the intended receiver.
Integrity : Assuring the receiver that the received message has not been altered in any way from the original.
Non-repudiation : A mechanism to prove that the sender really sent this message.
Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

2. PUBLIC KEY CRYPTOGRAPHY

Public-key cryptography[1] has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.
PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute.

2.1. Cryptographic Algorithm

There are several ways of classifying cryptographic algorithms. Here, they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

Public Key Cryptography (PKC) : Uses one key for encryption and another for decryption.

Plaintext → ciphertext → plaintext

Public key (asymmetric) cryptography[2]. PKC uses two keys, one for encryption and the other for decryption.

Public-key cryptography has been said to be the most significant new development cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute.

The mathematical "trick" in PKC is to find a trap door in the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher text. The important point here is that it **does not matter which key is applied first,** but that both keys are required for the process to work (Figure 1). Because a pair of keys are required, this approach is also called asymmetric cryptography.

In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to sent messages under this scheme.

DIFFIE AND HELMAN

D-H is used for secret-Key Key exchange only, and not for authentication or digital signatures
Overview of Diffie-Hellman

The first published public-key crypto algorithm was Diffie-Hellman.The mathematical "trick" of this scheme is that is relatively easy to compute exponents compared to computing discrete logarithms. Diffie-Hellman allows two parties – the ubiquitous Alice and Bob – to generate a secret key; they need to exchange some information over an unsecure communications channel to perform the calculation but an eavesdropper cannot determine the shared key based upon this information.

Diffie-Hellman works like this. Slice and Bob start by agreeing on a large prime number, n. They also have to choose some number g so that g<n.

There is actually another on g, Specifically that it must be primitive with respect to n. Primitive is a definition that is a little beyond the scope of our discussion but basically g is primitive to n if we can find integers I so that gI = j mod n for all values of j from 1 to n-1. As an example, 2 is not primitive to 7because the set of powers of 2 from 1 to 6, mod 7 = {2,4,1,2,4,1}. On the other hand, 3 is primitive to 7 because the set of powers of 3 from 1 to 6, mod 7 = {3,2,6,4,5,1}.

(The definition of primitive introduced a new term to some readers, namely mod. The phrase x mod y (and read as written!) means "take the reamainder after dividing x by y". Thus, 1 mod 7 = 1, 9 mod 6=3, and 8 mod 8 = 0.)

Anyway, either Alice or Bob selects n and g; they then tell the other party what the values are. Alice and Bob then work independently:

Alice	**Bob**
Choose a large random number, x	Choose a large random number, y
Send to Bob: X = gx mod n	Send to Alice: Y= gy mod n
Compute: KA= Yx mod n	Compute: KB = Xy mod n

Note that x and y are kept secret while X and Y are openly shared; these are the private and public keys, respectively. Based on their own private key and the public key learned from the other party, Alice and Bob have computed their secret keys, KA and KB, respectively, which are equal to gxy mod n.

Perhaps a small example will help here. Although Alice and Bob will really choose large values for n and g, I will use small values for example only; let's use n=7 and g=3.

Alice	Bob
Choose x = 2	Choose y = 3
Send to Bob: X = 32 mod 7=2	Send to Alice: y=33 mod 7=6
KA = 62 mod 7=1	KB = 23 mod 7=1

In this example, then, Alice and Bob will both find the secret key 1 which is, indeed, 36 mod 7. If an eavesdropper (Mallory) was listening in on the information exchange between Alice and Bob, he would learn g, n, X, and Y which is a lot of information but insufficient to compromise the key; as long as x and y remain unknown, K is safe. As said above, calculating X as gx is a lot easier than finding x as loggX!

A short digression on modulo arithmetic. In the paragraph above, we noted that 36 mod 7=1. This can be confirmed, of course, by nothing that:
36 = 729 = 104*7+1
There is a nice property of modulo arithmetic, howerve4r, that makes this determination a little easier, namely: (a mod x)(b mod x). Therefore, one possible shortcut is to note that 36 = (33)(33). Therefore, 36 mod 7 = (33 mod 7)(33 mod 7) = (27 mod 7)(27 mod 7) = 6*6 mod 7= 36 mod 7 = 1.

Diffie-Hellman can also be used to allow key sharing amongst multiple users. Note again that the Diffie-Hellman algorithm is used to generate secret keys, not to encrypt and decrypt messages.

RSA
RSA: The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it – Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signature, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure. (Some descriptions of PKC erroneously state that RSA's safety is due to the difficulty in factoring large prime numbers. In fact, large prime numbers, like small prime numbers, only have two factors!) The ability for computers to factor large numbers, and therefore attack schemes such as RSA, is rapidly improving and systems today can find the prime factors of numbers with more than 200 digits. Nevertheless, if a large number is created form two prime factors that are roughly the same size, there is no known factorization algorithm that will solve the problem in a reasonable amount of time; a 2005 test to factor a 200-digits number took 1.5 years and over 50 years of compute time (see the Wikipedia article on integer factorization.) Regardless, one presumed protection of RSA is that users can easily increase the key size to always stay ahead of the computer processing curve. As an aside, the patent for RSA expired in September 2000 which does not appear to have affected RSA's popularity one way or the other.

Overview of RSA Public-Key Cryptography

RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data. Today, RSA is primary used to encrypt the session key used for secret key encryption (message integrity) or the message's hash value (digital signature). RSA's mathematical hardness comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers. Although embloyed with numbers using hundreds of digits, the math behind RSA is relativelystraigh-forward.

3. PROBLEM DESCRIPTION

Main objectives
The main objective of the system is to provide a secured communication. There are may aspects to security and many applications ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secured communication is that of cryptography.

Public key cryptography has been said to be the most significant new dev3lopment in cryptography. Two important Public key Cryptographic algorithms that are in use today for key exchange or digital signatures are RSA and DIFFIE and HELLMAN.

RSA is the first and still most common PKC implementation. It is a PUBLIC key cryptographic algorithm that does encryption as well as decryption. The key length is variable. For enhanced security a long key should be chosen. For efficiency a short key should be chosen. The most commonly used key length for RSA is 512 bits.

The block size in RSA is also variable. The plain text block must be smaller than the key length. The cipher text block will be the length of the key.

Key issues and challenges
Any one using RSA can choose a long key for enhanced security, or a short key for efficiency. The most commonly used key length for RSA is 512 bits. The block size in RSA is also variable. The plain text block must be smaller than the key length. The cipher text block will be the length of the key.

System Methodology
Unlike secret key Cryptography, keys are not shared. Instead each individual has two keys: a private key that need not be revealed to any ne and a public key that is preferably known to the entire world. The operations that need to be3 routinely performed with RSA are

1. Encryption
2. Decryption
3. Generating a signature
4. Verifying a signature

A digital Signature is a number associated with a message. A digital Signature can be generated by some one knowing the private key. Verification of the signature only requires the knowledge of the public key.

4. SYSTEM DESIGN AND IMPLEMENTATION

The operations that need to be routinely performed with RSA are encryption, decryption, generating a signature and verifying a signature.

Encryption and Decryption
Public key Cryptography, also known as asymmetric Cryptography[3], is a form of cryptography in which a user has a pair of cryptographic keys – a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but he private key cannot be practically derived from the public key. A message encrypted with the public key can decrypted only with the corresponding private key.

A message encrypted with a recipients public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.

Conversely, Secret key Cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption.

Signing and Verifying the message

A message signed with a senders private key can be any one who has access to the senders public key,there by proving that the sender signed it and that the message has not been tampered.This is used to ensure authenticity.

For signing the sender produces a hash value of the message ,raises it to the power of d mod n and attaches it as a “signature” to the message. When the receiver receives the signed message, he raises the signature to the power of e mod n(as the sender does when encrypting a message),and compares the resulting hash value with the message’s actual hash value. If the two agree ,then the message has not been tampered.

Note that secure padding schemes such as RSA-PSS are as essential for the security of message signing as they are for message encryption, and that the same key should never be used for both encryption and signing purposes.

Algorithm of RSA Public-Key Cryptography

To create an RSA public/private key pair,here are the basic steps:

1. Choose two prime numbers, p,q. from these numbers you can calculate the modules,n=pq.

2. Select a third number ,e ,that is relatively prime to(i.e.,it does not divide evenly into)the product(p-1)(q-1).The number e is the public exponent.
3.Calclate an integer d from the quotient(ed-1)/[(p-1)(q-1)].The number d is the private exponent.

The public key is the number pair(n,e).Although these values are publicly known ,it is computationally infeasible to determine d from n and e if p and q are large enough[4].

To encrypt a message ,M, with the public key, create the ciphertext ,C, using the equation:

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

The receiver then decrypts the cipher text with the private key using the equation:

$$M= C^d \bmod n$$

Now, this might look a bit complex and indeed, the mathematics does take a lot of computer power given the large size of the numbers; since p and q may be 100 digits (decimal) or more, d and e will be about the same size and n may be over 200 digits. Nevertheless, a simple example may help. In this example, the values for p, q, e, and d are purposely chosen to be very small and the reader will see exactly how badly these values perform, but hopefully the algorithm will be adequately demonstrated:

1. Select p = 3 and q = 5.
2. The modulus n = pq = 15.
3. The value e must be relatively prime to (p-1)(q-1) = (2)(4) = 8. Select=11.
4. The value d must be chosen so that (ed-1)/[(p-1)(q-1) is an integer. Thus, the value (11d-1)/[(2)(4)] = (11d-1)/8 must be an integer. Calculate one possible value, d=3.
5. Let's say we wish to send the string **SECRET.** For this example, we will convert the string to the decimal representation of the ASCII values of the characters, which would be 83 69 67 82 69 84.
6. The sender encrypts each digit one at a time (we have to because the modulus is so small) using the public key value (e,n) = 11,15). Thus, each ciphertext character C I = M I 11 mod 15. The input digit string **0x836967826984** and, presumably, reassembled as the plaintext string **SECRET.**
7. The receiver decrypts each digit using the private key value (d, n) = (3, 15). Thus, each plaintext character M I = C I 3 mod 15. The input digit string **0x2c696d286924** will be converted to **0x836967826984** and, presumably, reassembled as the plaintext string **SECRET**

Again, the example above uses small values for simplicity and, in fact, shows the weakness of small values; note that 4, 6, and 9 do not change when encrypted, and that the values 2 and 8 encrypt to 8 and 2, respectively. Nevertheless, this simple example demonstrates how RSA can be used to exchange information.

RSA key lengths of 512 and 768 bits are considered to be pretty weak. The minimum suggested RSA key is 1024 bits; 2048 and 3072 bits are even better.

5.CONCLUSION

This paper has briefly described how cryptography works. Since, that there are a number of ways to attack every one of these systems; cryptanalysis and attacks on cryptosystems, however, are well beyond the scope of this paper. In the words of Sherlock Holmes (ok, Arthur Conan Doyle, really), "What one man can invent, another can discover" (The Adventure of the Dancing Men").

Public key techniques are much more computationally intensive than purely symmetric algorithms. The judicious use of these techniques enables a wide variety of applications. In practice, public key cryptography is used in combination with secret-key methods for efficiency reasons. For encryption, the message may be encrypted with secret-key algorithm using a randomly generated key, and that key encrypted with the user's public key. For digital signatures, a message is hashed (using a cryptographic has function) and the smaller "hash value" is signed; before verifying the signature, the recipient computes the hash of the message himself, and compares this hash value to check that the message has not been tampered with.

For most of the history of cryptography, a key had to be kept absolutely secret and would be agreed upon beforehand using a secure, but non-cryptographic, method; for example, a face-to-face meeting or a trusted courier. There are a number of significant practical difficulties in this approach to distributing keys. Public-key cryptography was invented to address these drawbacks – with public key cryptography, users can communicate securely over an insecure channel without having to agree upon a shared key beforehand.

The most obvious application of a public key encryption system is confidentiality; a message which a sender encrypts using the recipient's public key can only be decrypted by the recipient's paired private key.

Public-key digital signature algorithms can be used for sender authentication and non-repudiation.

To achieve authentication, non-repudiation, and confidentiality, the sender would first encrypt the message using his private key, then a second encryption is performed using the recipient's public key.

These characteristics are useful for many other, sometimes surprising, applications, like digital cash, password – authenticated key agreement, multi-party key agreement, etc.

6.FUTURE ENHANCEMENTS AND SUGGESTION

I feel it is very secure, but it will not achieve its full effectiveness without a method of re-encryption. Another addition that would enhance our program would be an advanced re-encryption process. RSA was originally considered; however, this style of encryption requires the generation and registration of keys, which would prove very difficult.

The recent emergence of practical Cryptosystems based Elliptic Curves has resulted in other potential refinements. These are mainly because Elliptic Curve

7.REFERNCES:

[1] Cryptography and Network security, seventh edition by William Stalings

[2] Guidelines on cryptographic algorithm usage and management ver 7.0 Nov 2017

[3] Douglas Stinson: Cryptography - theory and practice

[4] Practical cryptography by Al-Sakib Khan Pathan, Saiful Azad

[5] Digital Signatures-2010 Edition by Jonathan Katz

