Geo Location Based RSA Encryption Technique

Ayesha Khan

Department of Computer Science and Engineering
Abha College of Engineering
E-mail : ayeshak1989@gmail.com

Abstract – **The RSA cryptosystem was first published more than 25 years ago by Ronald Rivest, Adi Shamir and Leonard Adleman in 1997. It has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions. This paper discusses yet another use of RSA algorithm that is using designing of an encryption technique using RSA algorithm. We will use geo-location (latitude and longitude of source and destination) as keys along with the public and private keys of RSA algorithm**

Keywords – Public key cryptography, Factoring problem, n prime numbers, encryption, decryption, RSA Cryptosystem

I. INTRODUCTION

This Ronald Rivest, Adi Shamir and Leonard Adleman in 1997 provided maximum security for the data over network by giving this RSA algorithm. This security system is composed of three phases namely Key Generation, Encryption and Decryption. Also we can note that many security systems are built using this three phase scheme. In this method there are two keys Private Key and Public Key. Public Key is used to encrypt the message and can be seen by all, where as the private key also called as the secret key is used to decrypt the messages.

Also there are methods to break RSA security [1] Public key cryptography is one of the system which is not very secure because it is very much prone to insecurities while sending which is seen in the internet today. But, there are many algebraic assumptions which we have considered as an important key in this issue. For example, integer factoring problem and finding out prime numbers. To find out n in RSA we have to find out p and q which are prime numbers. Also , modulo n is a NP hard problem and many of the Public key cryptography are relied upon it[2] but it is not practically possible because the quadratic sieve is used for factorizing RSA-120 by Thomas, Bruce, Arjen and Mark[3] . Also, the RSA-140 is factored using number field sieve by Cavallar, Dodson, Lenstra, Leyland, Lioen, Montgemery, Murphy and Zimmermann [4]. While RSA-155 is factored in 1999, also, the RSA-160 is factored in April 2003, and the RSA-576 is factored in December 2003 by Eric [5]. The RSA-200 is factored in 2004; the RSA-640 is factored in November 2, 2005 by Bahr, Boehm, Franke and Kleinjung [6] and verified by RSA Laboratories. The relation between factoring and the public key encryption schemes is one of the main reasons that researchers are interested in factoring algorithms [7]. In 1976 Diffie-Hellmam [8] creates the first revolutionary research in public key cryptography via presented a new idea in cryptography and to challenge experts to generate cryptography algorithms that faced the requirements for public key cryptosystems. However, the first reaction to the challenge is introduced in 1978 by RSA [9].

II. RSA ALGORITHM

RSA has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions [10]. After seeing several examples of “classical" cryptography, where the encoding procedure has to be kept secret (because otherwise it would be easy to design the decryption procedure), we turn to more modern methods, in which one can make the encryption procedure public, without sacrifice of security: knowing how to encrypt does not enable you to decrypt for these public key systems [11].

To understand how the algorithm was designed, and why it works, we shall need several mathematical ingredients drawn from a branch of mathematics known as Number Theory, the study of whole numbers. In recent times it has been found very useful, as we shall see. Here are the ingredients we will draw from number theory:

- Modular arithmetic
- Fermat's “little" theorem
- The Euclidean Algorithm

A. Public key encryption

This idea omits the need of a carrier to deliver keys to recipients over another secure channel before transmitting the originally intended message. In RSA encryption keys are public, while the decryption keys are not, so only the person with the correct decryption keys can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key cannot be easily deduced from the public encryption key

III. GEO-LOCATION

The longitude and latitude location of source and destination will be given with the prime numbers used in the RSA algorithm for processing of public key on source side for encryption and also for the decryption of the text on the destination side.

IV. LITERATURE SURVEY

A. RSA Algorithm

Ronald Rivest, Adi Shamir and Leonard Adleman in 1997 also proposed a method for digital signatures and RSA cryptosystems. A digital signature is mathematical scheme which provides authenticity of a digital message and assures the recipient that the message was created by an authorized sender and was not modified in transit[12]. Generally, digital signature algorithms are based on a single hard problem like problem like prime factorization problem or discrete logarithmic or elliptic curve problem. If we can find the solution of any of one of these NP Hard problem then we can easily tamper with the security of the RSADSA (RSA Digital Signature Algorithm). The RSADSA is an asymmetric cryptographic technique, whose security is based on the level in which we are factorizing [13]

B. Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encryption of message. Messages encrypted with the public key can only be decrypted using the private key. The key for the RSA algorithm are generated the following way

1. Choose 2 distinct prime numbers p and q

   For security purpose the integers p and q should be chosen at random and should be of similar bit length. Prime integers can be efficiently found using a primality test.

   Compute n = pq.

   n is used as the modulus for both the public and private keys

   Compute φ (n) = (p – 1)(q – 1), where φ is Euler's totient function.

   Choose an integer e such that 1 < e < φ (n) and greatest common divisor of (e, φ(n)) = 1; i.e., e and φ (n) are coprime.

   e is released as the public key exponent.

   e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of e (such as 3) have been shown to be less secure in some settings.[4]

   Determine d as:

   $$d \equiv e^{-1} \pmod{\varphi(n)}$$

   i.e., d is the multiplicative inverse of e mod φ(n).

   This is more clearly stated as solve for d given (de) = 1 mod φ (n)

   This is often computed using the extended Euclidean algorithm.

   d is kept as the private key exponent.

C. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that 0 ≤ m < n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c = m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Note that at least nine values of m could yield a ciphertext c equal to m,[5] but this is very unlikely to occur in practice.

D. Decryption

Alice can recover m from c by using her private key exponent d via computing

$$m = c^d \pmod{n}$$

Given m, she can recover the original message M by reversing the padding scheme

V. GEOENCRYPTION

Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing. The term "location-based encryption" is used here to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext [13]. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system. Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, at a particular theatre, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location.

VI. PROPOSED WORK

Along with the public and private keys involved in RSA algorithm. We are implementing two more keys.

Geo location key : It will check the location of the sender and the receiver i.e the latitude and the longitude positions of both and then only the message will be decrypted. For eg. If the sender is at (x,y) location and the receiver is at (a,b) location then we will use a hash function to convert the values of (x,y) and (a,b) into an integer and multiply it with the RSA formula for encryption

Suppose hash [(x,y)] = p

And hash [(a,b)] = q

Then, c = [me (mod n)] × (p / q)

And at the receiver side we will implement

c = [me (mod n)] × (q / p)

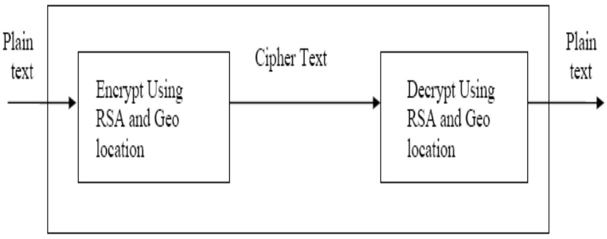
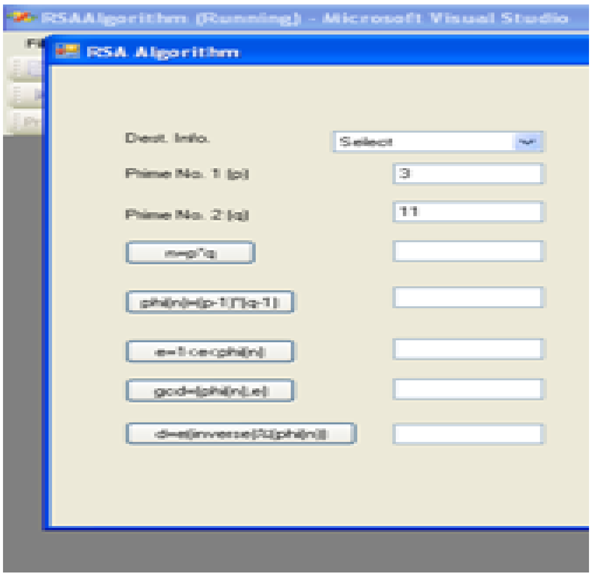

Plain text
Encrypt Using RSA and Geo location
Cipher Text
Decrypt Using RSA and Geo location
Plain text

Fig. 1 : Diagrammatic representation of the proposed algorithm


RSAAlgorithm (Running) - Microsoft Visual Studio

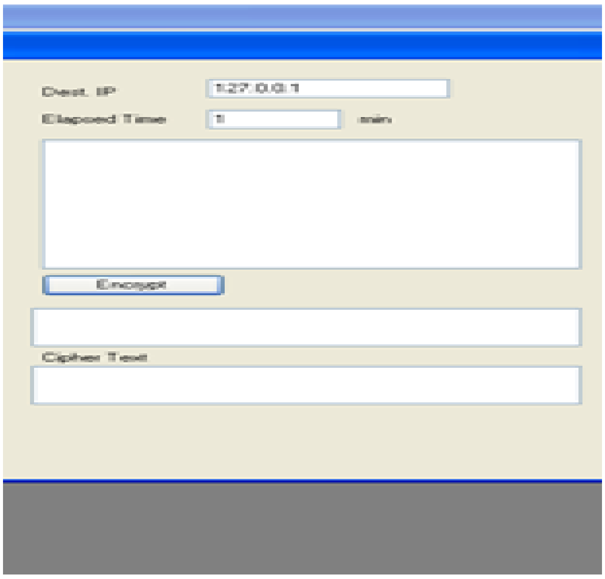
RSA Algorithm

Dest. Info. Select

Prime No. 1 (p) 3

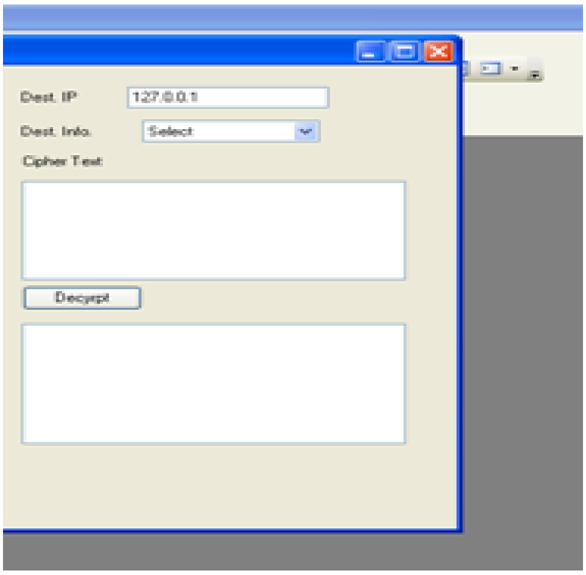
Prime No. 2 (q) 11

Fig. 2: Screen-shot representing the calculation part of the algorithm.


Dest. IP 127.0.0.1

Elapsed Time 1 min

Fig. 3 : Screen-shot representing sender side GUI



Dest. IP 127.0.0.1

Dest. Info. Select

Cipher Text

Fig. 4 : Screen-shot representing receiver side GUI

Time: This key will be optional. This will check the time barrier. For eg, if it takes 30 mins for the data to travel from dest1 to dest2 then the message cannot be decrypted before 30 mins. Due to network delay involved in real time systems, un-synchronized clocks and data traffic, this key is kept optional

VII. REFERENCES

[1] Vibhor Mehrotra and Dr. K. C. Joshi “A Method for Breaking RSA Security”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 2 , Issue 9, September 2012 ISSN: 2277128X Page 289-292

[2] Bonteh S, “Twenty Years of Attacks on the RSA Cryptosystem”, Notices of the American Mathematical Society, 46(2):203-213, 1999

[3] Thomsan D. Bruce D. Arjen L. and Mark M.,“On the Factoring of RSA-120”, (169), pp.166-174, 1994

[4] Cavallar S, Dodson B, Lenstra A, Leyland P,Lioen W, Montgemery P, Murphy B, and Zimmermann P, “Factoring of RSA-140 using the number field sieve”, 1999

[5] Eric W “Prime Factorization Algorithm”, Mathworld.woiframe.com/news/ 2003

[6] Bahr F, Boehm M, Franke J and Kleinjung T, “For the Successful Factorization of RSA-200” www.rsasecurity.com

[7] Douglas Stinson “Cryptography Theory and Practice”, CRC Press, 3rd Edition, pp. 211-214, 2006

[8] Diffie W and Hellman M, “New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[9] Rivest R, Shamir A and Adelman L, “A Method for Obtaining Digital Signature and Public Key Cryptosystems”, Communications of the ACM, 21, pp. 120-126, 1978

[10] William Stallings, ―Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition (2009).

[11] Edmund Landau, Vorlesungen, Uber Zahlentheorie - Lectures on Number Theory (1927)

[12] Logan Scott, GeoCodex LLC, LS Consulting, Dorothy E. Denning, GeoCodex LLC - Location Based Encryption & Its Role In Digital Cinema Distribution

[13] Ashish Vijay, Priyanka Trika and Kapil Madhur “A New Variant of RSA Digital Signature”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 2 , Issue 10, October 2012 ISSN: 2277128X Page 366-371

❖❖❖