International Journal of Computer Systems (ISSN: 2394-1065), Volume 02– Issue 06, June, 2015
Available at http://www.ijcsonline.com/

Quadratic Residuosity based Encryption Algorithm (QREA) and its Comparative Study with RSA

Indumati Sharma[A], Sushila Vishnoi[B]

[A]Department of Computer Science, Rajasthan Technical University, Kota, India
[B]Department of Computer Science, Swami Keshvanand Institute of Technology, M & G, Jaipur, India

Abstract

RSA (Rivest, Shamir and Adleman), a popular current-day public-key cryptosystem (cryptosystems that use different keys to encrypt and decrypt data, and whose key is globally available), is widely used for securing sensitive data over an insecure network such as the Internet. Based on its assumption that a large number cannot be easily factored, it can easily be understood that if the resulting modulus in some implementation of the algorithm is factored into its prime numbers then the key can also be obtained easily. To avoid such conditions, the following dissertation serves to present a modified algorithm titled Quadratic Residuosity based Encryption Algorithm (QREA). The security of the RSA system is based on the assumption that factoring of large number is difficult. In RSA algorithm, if one can factor modulus (n) into its prime numbers then it is easy to obtain the private key too. Quadratic Residuosity based Encryption Algorithm (QREA) algorithm is more secure compared to RSA algorithm as it bases its logic on intractability of the quadratic residuosity problem integer factorization. To break the algorithm, an attacker will have to find the prime factors of a number as well as solution of quadratic residuosity problem. Hence a QREA system is more secure for mathematical attacks.

Keywords: *Quadratic Residuocity, Cryptosystem, Public key System, encryption, decryption.*

I. INTRODUCTION

Symmetric-key cryptography is based on the sender and receiver of messages knowing and using the same secret key. The sender uses the secret key to encrypt the message and the receiver uses the same secret key to decrypt it. The main problem of symmetric key cryptography is getting the sender and receiver to agree on the same secret key without anyone else knowing it. As all the keys in a symmetric key cryptosystem must remain secret, symmetric key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users.

To solve this problem, Diffie and Hellman introduced a new approach to cryptography and, in effect, challenged cryptologists to come up with a cryptographic algorithm that met the requirements for public- key systems [5].Public key cryptography uses a pair of related keys, one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed and this eliminate the need for the sender and the receiver to share secret key. The only requirement is that public keys are associated with the users in a trusted (authenticated) manner through a public key infrastructure (PKI). The public key cryptosystems are the most popular, due to both confidentiality and authentication facilities [1].The message is encrypted with public key and can only be decrypted by using the private key. So, the encrypted message cannot be decrypted by anyone who knows only the public key and thus secure communication is possible.

In a public-key cryptosystem, the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system by deriving the private key from the public key. The defense against this is to make the problem of deriving the private key from the public key as difficult as possible. Some public-key cryptosystems are designed such that deriving the private key from the public key requires the attacker to factor a large number. The Rivest-Shamir-Adleman (RSA) public key cryptosystem is a best known example of such a system [2, 6].The main arithmetic operation in the RSA Cryptosystem is modular exponentiation defined as $C = Me \mod n$ for encryption and $M = Cd \mod n$ for decryption, where C is the cipher, M is the message, e is the public key, d is the private key, and n is the modulus[3,4].

RSA algorithm has some important parameters affecting its level of security and speed [7]. By increasing the modulus length plays an important role in increasing the complexity of decomposing it into its factors. This also increases the length of private key and hence difficulty to detect the key. Another parameter is the length of message to be encrypted at a time (chunk size). When the length of message is changed then the length of encrypted message will proportionally change, hence larger chunks are selected to obtained larger encrypted message to increase the security of the data in use [4]. RSA -1024 bits (modulus size) has been good for last 20 years but recently Bernstain has described circuitry for fast factorization. Now It is entirely possible that an organization with sufficiently deep pockets can build a large scale version of his circuits and effectively crack an RSA 1024 bit message in a relatively short period of time,

ranging any where from a few minutes to some days [8].So to improve security a Quadratic Residuosity based Encryption Algorithm (QREA) is presented. QREA algorithm is more secure compared with RSA algorithm as it uses double encryption and decryption using double private and public keys to provide security against Brute-force attacks. Hence if an eavesdropper or intruder detects a single key of QREA cryptosystem even that it is not possible to decrypt the message.

II. RSA CRYPTOSYSTEM

RSA is based on the principle that some mathematical operations are easier to do in one direction but the inverse is very difficult without some additional information. In case of RSA, the idea is that it is relatively easy to multiply but much more difficult to factor. Multiplication can be computed in polynomial time whereas factoring time can grow exponentially proportional to the size of the number.

A. Key Generation Process:

i. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = p x q is of the required bit length, e.g. 1024 bits.

ii. Compute n = p x q and φ = (p-1) x(q-1).

iii. Choose an integer *e*, satisfying 1<e< φ, such that gcd (e, φ) = 1.

iv. Compute the secret exponent *d*, 1 < d< φ, such that e x d ≡ 1(mod φ).

v. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and φ secret.

- n is known as the modulus.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

Public key (n, e) is published for everyone and private key (p, q, d) must be kept secret. Then by using these keys encryption, decryption, digital signing and signature verification are performed.

B. Encryption Process:

Sender A does the following: -

- Obtains the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer *m*.
- Computes the cipher text c =m^e mod n.
- Sends the cipher text C to B.

C. Decryption Process:

Recipient B does the following: -

- Uses private key (n, d) to compute m = c^d mod n.
- Extract the plaintext from the message representative m.

III. QREA ALGORITHM

The Quadratic Residuosity based Encryption Algorithm (QREA) is an extension of the RSA algorithm with the Quadratic properties. It is an asymmetric key encryption algorithm and the key generation process is same as RSA algorithm. This algorithm is developed to improve the security as compared to RSA. Following are the key generation, encryption and decryption process of RSA cryptosystem.

A. Key Generation Algorithm

i. Generate two large random primes, *p* and *q*, of approximately equal size such that p, q = 3 mod 4.

ii. Compute N = p x q and φ = (p-1) x (q-1).

iii. Choose an integer *e*, 1 < e < φ, such that gcd (e, φ) = 1.

iv. Compute the secret exponent *d*, 1< d< φ, such that e x d (mod φ) = 1.

The public key is (N, e) and the private key is (N, d). Keep all the values d, p, q and φ secret. ·

B. Encryption

1. First encodes m as a string of bits (m_1, ..., m_n).

2. For every bit m_i, Bob generates a random value y less than N. He outputs the value c_i = ((y^2 * (N-1)^ m^i (mod N))^e mod N.

3. Bob sends the ciphertext (c_1, ..., c_n).

C. Decryption

1. Compute h_i= $(c_i)^d$ mod N.

2. For each i, using the prime factorization (p, q), Alice determines whether the value hi is a quadratic residue; if so, m_i =0, otherwise m_i = 1.

3. Alice outputs the message m = (m_1, ... , m_n).

Following is a method for checking that x is a quadratic residue or not

1. Compute x_p = x mod p, x_q = x mod q.
2. If $x^{(p-1)/2}$ (mod p) = 1 and $x^{(q-1)/2}$ (mod q) = 1 then *x* is a quadratic residue mod *N*.

IV. CONCLUSION

We have presented a new universally anonymous QREA scheme, based on RSA encryption with some modifications. QREA is Quadratic Residuosity based Encryption Algorithm with double encryption and decryption keys and operations. Based on mathematical facts, it is realized that as the size of the number increases, the feasibility or easy of factoring the number decreases, even with enormously powerful computing machines, it is almost impossible to find two prime numbers which multiply to give the original given number. In RSA, if one can factorize the modulus (n) of a number into its prime number it becomes easy to obtain the private key too. To better the security prospect of RSA, QREA cryptosystem

combines quadratic residuosity property with RSA's factoring problem. The attacker is first required to factorize a large number and then solve the residuosity problem to break the QREA algorithm. Although QREA reduces the speed of encryption and decryption process, the resulting speed still remains nearly half the speed of RSA algorithm.

REFERENCES

[1] S.Goldwasser, S.Micali (1984). Probabilistic encryption". Journal of computer and system sciences 28(2); 270-299.

[2] R.L. Rivest, A.Shamir, and L.Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2):120-126, 1978.

[3] W.Diffie and M.Hellman. New directions in cryptography. Information theory, IEEE transactions on 22(6):644-654, 2002.

[4] Burnett, Steve, and Paine, Steven, RSA security official guide to Cryptography, Tata MCGraw-Hill, 2001.

[5] D. Boneh and H. Shacham. Fast variants of RSA. CryptoBytes (RSA Laboratories), 5:1(9), 2002.

[6] RSA Laboratory (2009)"RSA Algorithm security and Complexity", Retrieved from http://www.google.co.in/imgres?imgurl=http://regenet.files.wordpress.com.

[7] Bryan Poe," Factoring the RSA Algorithm", mat/csc 494, April 27, 2005,pages 1-6.

[8] Maurer, Ueli. "Constructive cryptography–a new paradigm for security definitions and proofs." Theory of Security and Applications. Springer Berlin Heidelberg, 2012. 33-56.

[9] Richard E.Smith"Internet Cryptography", ISBN 81-297-0351-3, Pearson education.

[10] Atul Khate ,"Cryptography and network Security" ,Tata MCGraw-Hill publishing company limited, India Second edition, pages 38-62,152-165,205-240,340-370.