International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 10 157 - 160

Randomized Encryption Cryptosystem

[1.]R. Sivaraman
Ph.D. Research Scholar in Mathematics
Sri Satya Sai University of Technology and Medical Sciences, Bhopal, Madhya Pradesh
National Awardee for Popularizing Mathematics among masses, Chennai – 600 094
Email: rsivaraman1729@yahoo.co.in

[2.] Dr. Sonal Bharti
Head, Department of Mathematics
Sri Satya Sai University of Technology and Medical Sciences
Bhopal, Madhya Pradesh
Email: sbsonalbharti6@gmail.com

Abstract

Abstract: - Cryptography is the art of secret writing. There are essentially two types of cryptosystems.

(i) Secret-key cryptosystems also called symmetric cryptosystems

(ii) Public-key cryptosystems also called asymmetric cryptosystems.

In this paper, we shall consider a Public-key cryptosystem whose security is based on the infeasibility of the Quadratic Residuosity Problem (QRP)

Keywords: *Cryptosystem, Quadratic Residues, Legendre Symbols, Algorithms*

*****

1. WE SHALL CONSIDER THE FOLLOWING ALGORITHM

RANDOMIZED ENCRYPTION ALGORITHM
Algorithm:

This algorithm uses the randomized method to encrypt messages and is based on the Quadratic Residuosity Problem (QRP) [1]. The algorithm is given in three steps, namely key generation, Message encryption and Decryption

Step I <u>Key Generation</u>

Consider two persons say Ram and shyam. Both Ram and Shyam should do the following to generate their public and secret Keys:

(i) Select two large distinct primes p and q, each with roughly the same size, say, each with β bits.

(ii) Compute n = pq

(iii) Select a $y \in Z / nZ$, such that $y \in \overline{Q_n}$ and $\left(\frac{y}{n}\right) = 1$ (i.e. y is a pseudo square modulo n) Q_n is the set of all quadratic residues modulo n. Q_n is the set of all pseudosquares modulo n

(iv) Make the Key (n,y) public, but keep the Key (p,q) secret.

Step II <u>Encryption:</u>

To send a message (the cipher text) Ram should do the following:

(i) Obtain shyam's Public key (n,y)

(ii) Represent the message **m** as a binary string **m** = $m_1\ m_2\ m_3 \ldots m_k$ of length k.

(iii) For i = 1 to k do
Choose at random an x Є $(Z/nZ)^*$ call it x_i. Compute $\mathbf{c_i}$ from

$$c_i = \begin{cases} x_i^2 \mod n, \text{ if } m_i=0 \text{ (Random square)} \\ yx_i^2 \mod n, \text{ if } m_i=1 \text{ (Random pseudo square)} \end{cases} \quad \ldots (1)$$

(iv) Send the k-typle $\mathbf{c} = (c_1, c_2, \ldots c_k)$ to shyam. Each $\mathbf{c_i}$ is an integer such that $1 \leq \mathbf{c_i} < n$. Note also that since n is a 2 β bit integer it is clear that the cipher text **c** is a much longer string than the original plain text **m**.

Step III <u>Decryption:</u>

To Decrypt Ram's message (i.e the cipher text **c** constructed above), shyam should do the following

(i) For i = 1 to k do
Evaluate the Legendre symbols

$$\left.\begin{aligned} e_i' &= \left(\frac{c_i}{p}\right) \\ e_i'' &= \left(\frac{c_i}{q}\right) \end{aligned}\right\} \quad \ldots (2)$$

(ii) Compute m_i from

$$m_i = \begin{cases} 0, & \text{if } e_i' = e_i'' = 1 \\ 1, & \text{if otherwise} \end{cases} \quad \ldots (3)$$

That is, $m_i = 0$ if $c_i \in Q_n$, otherwise $m_i = 1$. Otherwise, set $m_i = 1$.

(iii) Finally, get the decrypted message $\mathbf{m} = m_1 m_2 \ldots m_k$
This completes the algorithm.

2. RESULTS CONCERNING LEGENDRE SYMBOL

We shall consider the following important results for the Decryption step.
Let p,q be primes

$$\left(\frac{1}{p}\right) = 1 \quad \ldots (4)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \ldots (5)$$

$$a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \ldots (6)$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \ldots (7)$$

 ISSN: 2321-8169
157 - 160

$$\left(\frac{a^2}{p}\right) = 1 \qquad \ldots (8)$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \ldots (9)$$

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) \quad [2] \qquad \ldots (10)$$

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \quad [3] \qquad \ldots (11)$$

3. ILLUSTRATION:

Let us consider the Algorithm for the message "SPY". The binary equivalent for the letters S,P,Y are 10010, 01111, 11000 respectively. So the message space **m** is given by **m** = 10010 01111 11000

Let n = 21 = 3 * 7 so that p = 3, q = 7

Let y = 17. Let us consider the case of encrypting m_2, m_{12}

$m_2 = 0$ choose $x_2 = 5$

$c_2 = x_2^2 \bmod 21 = 5^2 \bmod 21 = 4$

The decryption is:

$$e_2' = \left(\frac{c_2}{p}\right) = \left(\frac{4}{3}\right) = 1$$

$$e_2'' = \left(\frac{c_2}{q}\right) = \left(\frac{4}{7}\right) = 1$$

Since $e_2' = e_2'' = 1$, $m_2 = 0$ form (3)

Similarly for $m_{12} = 1$, Choose $x_{12} = 9$

then $c_{12} = (17)(9)^2 \bmod 21 = 12$

$$e_{12}' = \left(\frac{12}{3}\right) = 0$$

$$e_{12}'' = \left(\frac{12}{7}\right) = \left(\frac{5}{7}\right) = -1$$

From (3), $m_{12} = 1$

Similar calculation leads shyam to the message **m**.

4. FEATURES OF THE CRYPTOSYSTEM:

(i) The encryption process in this system is random in the sense that the same bit is transformed into different strings depending on the choice of the random number x. For this reason, it is also called Probabilistic encryption [4].

(ii) Each bit is encrypted as an integer modulo n, and hence each bit is transformed in to a 2β bit string.

(iii) The Algorithm proposed in this system takes $o(\beta^2)$ time to encrypt each bit and $o(\beta^3)$ time [5] to decrypt each bit.

(iv) Solving Quadratic Residuosity Problem is equivalent to computing the prime factorization of n and so it is computationally infeasible.

(v) This system is more secure than the most famous RSA Cryptosystem [6] which is not secure for all probability distributions of the message space, in the sense that under fixed Public-key, a particular plain text **m** is always encrypted to the same cipher text **c**, where as in this system the plaintext **m** is converted into different forms of ciphertext **c**, because of the randomness in the encryption process.

References / Notes:

[1] Neal koblitz, A course in Number Theory and cryptography, **43**, 2004.

[2] C.F. Gauss Proved the stated result called Law of Quadratic Reciprocity, Disquistiones Arithmeticae, Yale university press, 1966

[3] Euler Proved an important result regarding QRP which is both necessary and sufficient.

[4] S. Goldwasser and S. Micali, "Probabilistic Encryption", Journal of computer and system sciences, **28**, 1984.

[5] Neal Koblitz, A course in Number Theory and cryptography, 7–9, 2004.

[6] Three MIT researchers, Ronald L. Rivest, Adishamir, Leonard Adleman proposed the first practical Public-key cryptosystem, now widely known as the RSA Public-key cryptosystem. There are two important References.

[7] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining Digital signatures and Public - key cryptosystems, communications of the ACM, 21, 2, (1978), 120–126

[8] R.L. Rivest, "Remarks on a proposed cryptanalytic attack on the M.I.T. Public-key cryptosystem",cryptologia, 2, 1 (1978), 62–65