International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Role of Chinese Remainder Theorem in Cryptography

Keerthika V

Abstract: ***Strength of the network security usually depends on the weakness of the link, which is the concept lies in the implementation of cryptographic algorithms. In this paper, we deal with the implementation of RSA algorithm using Chinese remainder theorem.***

Index Terms: ***Encryption, decryption, cipher text, prime numbers, Congruence, RSA algorithm etc.***

I. INTRODUCTION

Cryptology is the area which rules the modern electronic security systems, the word means the study of hidden science. The main motto of cryptology is to protect the content of message, when it was being carried from one place to other. In early stages, messages were converted into unreadable groups of figures. Egyptian scribes used hieroglyphs on BC 1900. Later, The Greek used to wrap a tape around a stick and then write the message on the wound tape, so that the messages have been kept secret. Caesar shift cipher, a method followed by the Romans, utilized the idea of shifting letters by an agreed upon number and thus writing the message using the letter-shift.

There are three basic types of cryptographic schemes typically used to accomplish these goals:

- Secret key (or Symmetric) cryptography
- Public-key (or Asymmetric) cryptography
- Hash functions

In secret or symmetric key algorithm, both Encryption and decryption use the same key to share secret between two communicating nodes. In public key or asymmetric key algorithm, a pair of keys (private and public) is used. The key used to encrypt data can be retrieved only by making use of other key. [1] Several algorithm has been developed to emphasize the mathematical relation between those two keys, so that it is practically impossible to derive the private key from the public key. The RSA algorithm is a type of this public key algorithm. This paper elucidated the concepts along with theorems used to formulate RSA algorithm.

ORIGIN

The first public-key cryptosystem came into light in a classic paper written by scientists Diffe and Hellman. However, it did not contain practical implementation. In the next few years, several methods were proposed. The most successful idea was proposed by R.L.Rivest, A.Shamir, and L.Adleman of the Mas-sachusetts Institute of Technology (MIT) in 1977 and is known as the RSA algorithm. It based on the concept that factorization of integers into their prime factors is hard [5]. The first description of the RSA cryptosystem appeared in the "Mathematical Games" column of the scientific journal in August 1977. Martin Gardner American published this with the permission of Ronald Rivest.[1]

II. METHODOLOGY

A) PRELIMINARIES

1.1 CHINESE REMAINDER THEOREM (CRT):

Suppose $m_1, m_2, \dots, m_t$ are s integers, no two of which have a common factor other than 1. Let $M = m_1 m_2 \dots m_t$ and suppose that $a_1, a_2, \dots, a_t$ are integers such that $\gcd(a_i, m_i) = 1$ for each i.

Then the system of t-congruence

$$a_1 x \cong b_1 (\text{mod } m_1)$$
$$a_2 x \cong b_2 (\text{mod } m_2)$$
$$\vdots$$
$$a_t x \cong b_t (\text{mod } m_t)$$

have a simultaneous solution that is unique modulo M.[2]

1.2 EULER's Φ-FUNCTION Φ(k):

The Euler's Φ-function Φ(k) is defined as the number of positive integers not exceeding k and are relatively prime to k. For any positive integer k,

$$\Phi(k) = k\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_n}\right),$$

Where $p_1, p_2, \cdots, p_n$ are the prime factors of k.

In particular if k is a prime, then

$\Phi(k) = k - 1$. [2]

1.3 CONGRUENCE MODULO n:

Let c, d and k be any integers with $k \neq 0$. We say that c is congruent to d modulo k if $\frac{c-d}{k}$ is an integer and is denoted by $c \cong d (\text{mod } k)$.[2]

1.4 CANCELLATION LAW:

If $bd \cong ba (\text{mod } k)$ and if b and k are relatively prime, then $d \cong a (\text{mod } k)$.

1.5 LINEAR CONGRUENCE:

A linear Congruence modulo k is an expression of the form $cx \cong d (\text{mod } k)$ and an integer x_0 is said to be the solution of the linear congruence if $ax_0 \cong b (\text{mod } n)$.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

V.KEERTHIIKA*, M.Sc., M.Phil., Assistant Professor in Sri Krishna College of Engineering and Technology, Coimbatore.

1.6 EULER'S THEOREM:

If the integers a and m are relatively prime, then $a^{\Phi(m)} \cong 1 (\text{mod } m)$.

1.7 FERMAT'S LITTLE THEOREM:

If k is a prime, then $a^k \cong a (\text{mod } k)$.

1.8 CRYPTOSYSTEM:

An Encryption scheme or Cryptosystem is a collection of 5-tuple (P,C,E,D,K) where

- P refers the space of all plaintext.
- C refers the space of all cipher text.
- E denotes the set of encryption function.
- D denotes the set of decryption function.
- K refers the space of all keys.[1]

B) ALGORITHM

Following is the algorithm of RSA cryptographic system construction:

Step 1: Choose two large prime integers p_1 and p_2 randomly of same size, but not too close together.

Step 2: Calculate the product $k = p_1 \times p_2$.

Step 3: Choose an encryption exponent e^* randomly such that e^* is less than k and is relatively prime to $p_1 - 1$ and $p_2 - 1$ respectively. That is, gcd(e^*,($p_1 - 1$)($p_2 - 1$)) = 1.

Step 4: Calculate the decryption exponent d^* using,

$$e^* d^* \cong 1 \left(\text{mod } (p_1 - 1)(p_2 - 1)\right).$$

Step 5: If step 4 is not possible, then pick two random integers d_1^* and d_2^* such that gcd(d_1^*, $p_1 - 1$) = 1, gcd(d_2^* , $p_2 - 1$) = 1 and $d_1^* \cong d_2^* \pmod 2$.

Step 6: Find d^* such that $d^* \cong d_1^* \pmod{p_1 - 1}$ and $d^* \cong d_2^* \pmod{p_2 - 1}$ and compute $e^* = d^{*-1} \pmod{\Phi(k)}$.

Step 7: The Encryption function is $E(m) = c \cong m^{e^*} (\text{mod } k)$ and the Decryption function is $D(c) = m \cong c^{d^*} (\text{mod } k)$ for any cipher text c and message m.

Step 8: The public-key is the pair of integers (k, e^*).

Step 9: The private-key is the triple of integers (p_1, p_2, d^*).

III. RESULTS AND DISCUSSION

As a result of RSA algorithm, we obtain a set of keys on which the strength of the system based on. Even though, the algorithm portrays the step by step procedure of key generation, some of the constraints must be concentrated while creating keys to ensure the security of the cryptosystem, which we discuss below:

(i) The security of the system mentioned above lie on the fact that it is almost impossible to calculate the value of d^*, if only the public-key (k, e^*) is known. Thus the chosen prime numbers p_1 and p_2 must satisfy the following conditions:

- $p_1 - 1$ must have a large prime factor, say q_1.
- $p_1 + 1$ must have a large prime factor, say q_2.
- $q_1 - 1$ must have a large prime factor, say t.

(ii) The same restrictions were imposed on p_2. And the difference $|p_1 - p_2|$ must also be large.[5]

(iii) For solution to exists, the moduli appeared in step 6 must be relatively prime in pairs. But $p_1 - 1$ and $p_2 - 1$ are even and so we cannot apply CRT directly. We observe that gcd $\left(\frac{p_1 - 1}{2}, \frac{p_2 - 1}{2}\right) = 1$. Essentially d_1^*, d_2^* are odd integers and $d_1^* - 1$, $d_2^* - 1$ are even integers, since gcd (d_1^*, $p_1 - 1$) =1 and gcd (d_2^*, $p_2 - 1$) = 1.

(iv) Also we have gcd (d^*, $p_1 - 1$) = 1, which implies that d^* is odd and $d^* - 1$ is even.

Thus to find a solution for the system of congruence,

$$d^* \cong d_1^* (\text{mod } p_1 - 1)$$
$$d^* \cong d_2^* (\text{mod } p_2 - 1)$$

It is enough to find a solution to the system

$$d^* - 1 \cong d_1^* - 1 (\text{mod } p_1 - 1)$$
$$d^* - 1 \cong d_2^* - 1 (\text{mod } p_2 - 1)$$

By applying the cancellation law and taking 2 out as the common factor, we have

$$d \cong \frac{d_1^* - 1}{2} \left(\text{mod } \frac{p_1 - 1}{2}\right)$$
$$d \cong \frac{d_2^* - 1}{2} \left(\text{mod } \frac{p_2 - 1}{2}\right)$$

Where $d = \frac{d^* - 1}{2}$.

Using CRT, we can find d such that $d = (2 \times d^*) + 1$. Knowing d, p_1 and p_2, calculate

$$m_1 \cong c^d (\text{mod } p_1)$$
$$m_2 \cong c^d (\text{mod } p_2)$$

Then, using CRT, solve

$$x \cong m_1 (\text{mod } p_1)$$
$$x \cong m_2 (\text{mod } p_2)$$

to get the solution x.

C) ILLUSTRATION

Suppose that p_1 =97, p_2 =167, k=26, l=2 and e=797, in the RSA Cryptosystem and assume that the following are the cipher text message units obtained: 2684, 7052, 0, 2684, 14560, 3314, 2444, 14238, 14238, 10952. Decipher to give the English Plaintext.

Solution:

Since given values of p_1 and p_2 are relatively prime, we have

$\Phi(k) = \Phi(97 \times 167) = 96 \times 166 = 15936$.

Using Extended Euclidean Algorithm, we have

$$e^* d^* \cong 1 \left(\text{mod } (p_1 - 1)(p_2 - 1)\right).$$

$\Rightarrow \quad 797 d^* \cong 1 (\text{mod } 15936)$,

$\Rightarrow \quad 1 = 797 d^* + 15936x$,

$\Rightarrow \quad d^* = 11957$ and x = -598:

Hence by computing $c^{d^*} \cong m (\text{mod } k)$, we have

$2684^{11957} \cong 02 (\text{mod } 16199)$,

$7052^{11957} \cong 14 (\text{mod } 16199)$,

$0^{11957} \cong 00 (\text{mod } 16199)$,

$2684^{11957} \cong 02 \pmod{16199}$,
$14560^{11957} \cong 07 \pmod{16199}$,
$3314^{11957} \cong 06 \pmod{16199}$,
$2444^{11957} \cong 20 \pmod{16199}$,
$14238^{11957} \cong 13 \pmod{16199}$,
$14238^{11957} \cong 13 \pmod{16199}$,
$10952^{11957} \cong 24 \pmod{16199}$.

Thus, M = {02, 14, 00, 02, 07, 06, 20, 13, 13, 24}. Transferring into corresponding English alphabets starting with a = 00 and so on, we get the plaintext as COACH GUNNY.

IV. CONCLUSIONS

Chinese remainder theorem plays a vital role in the security loop of electronic gadgets developed based on RSA algorithm. The key fact lie on the concept which will be implemented to create public and private keys. Several algorithm has been developed in recent days based on different concepts for efficient key creation. This paper demonstrate how Chinese remainder theorem have been applied to construct keys which provide a pathway for secured encryption and decryption process. Deciphering the text has been illustrated using an example.

REFERENCES

1. A. Buchmann, Introduction to Cryptography, Second Edition, Springer-Verlag New York, Inc.
2. George E. Andrews, Number Theory, Dover Publications, Inc., New York.
3. Johann Groschadl, Graz University of Technology, the Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip.
4. Law Huong Ing, The history of THE CHINESE REMAINDER THEOREM, volume 30, no. 1, June 2003.
5. Neal Koblitz, A Course in Number Theory and Cryptography, volume 114 of Graduate texts in mathematics, Springer-Verlag, Berlin, Germany, second edition, 1994.
6. ZIHAO JIANG, Applications of number theory in cryptography

AUTHORS PROFILE

V.KEERTHIIKA, M.Sc., M.Phil. I'm working as Assistant Professor in Sri Krishna College of Engineering and Technology, Coimbatore. I have passed SLET and NET and have 3 year experience in research field.