National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)- Dec 2017

RESEARCH ARTICLE OPEN ACCESS

# Data Security in Cryptography using Mathematics

Dr.T.Logeswari
Dept of Computer Science, New Horizon College, Banglore

## Abstract:

The Network Security & Cryptography is a concept to keep network and data broadcast over wireless network. Data Security is the main aspect to make secure data transmission over changeable network. Network security involves the permission to access the data in a network, which is controlled by the network administrator. The issues of confidentiality, authenticity and anonymity have been known from long time in Security i.e. Cryptography is a method of providing security for the data including image, audio, video.. With highly advance and improved technology, there is also a need to define these methods of security under various approaches. For securing the data using cryptography uses mathematics, with number theory, linear algebra and algebraic structure etc. To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations in cryptography.

*Keywords* **— Extended Euclidean algorithm, GCD , Linear Diophantine equation.**

## I. INTRODUCTION

Cryptography is an promising knowledge, which is important for network security. The widespread use of computerized data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission[1]. Due to ongoing advancements in communications and eavesdropping technologies, business organizations and private individuals are beginning to protect their in order to computer systems and networks using cryptographic techniques, which, until very recently, were exclusively used by the military and diplomatic communities[4]. Cryptography is a essential of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages[2][3]. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorized access. techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext(ordinary text, sometimes referred to as cleartext) into ciphertext(a process called encryption), then back again (known as decryption). Individuals who apply this field are known as cryptographers[9].

## II. .Mathematics in Cryptology

### Basics → Integer Arithmetic:

Operation of modern cryptosystems is based on arithmetical computations of large integers. They must be executable quickly and efficiently. Efficiencies of algorithms are often compared using numbers of basic steps needed to execute the algorithm versus the maximum length N of the input numbers[6]. Basic step could be for example addition, subtraction or multiplication of the decimals( 0, 1, . ……, 9 )

i. Set of Integers:

It contains all integral numbers from Negativity to positive infinity

$Z=\{\ldots\ldots..,-2,-1,0,2,\ldots\ldots\ldots\}$

ii. Integer Division:

When a integer number a called the dividend is divided by another integer n called the divisor, the quotient a and remainder r are obtained. The relationship between the four integers can be shown as:

$$a = q * n + r$$

iii.The Modulo Operator:

A few words about the modulo operator (mod) are in order. Recall that a mod n is the remainder of a when divided by n. That is,

$$r = a \bmod n$$

means that $r = a - a/n\ n$.

In other words, there is some integer q, such that $a = qn + r$.

Note, in addition, that a mod n is always an integer in the set {0, 1, 2, . . . , n − 1}, even when a is negative.

It is sometimes convenient to talk about congruence modulo n. If

$$a \bmod n = b \bmod n,$$

we say that a is congruent to b modulo n, which we call the modulus, and we write

$$a \equiv b \pmod{n}.$$

Therefore, if $a \equiv b \bmod n$, then $a - b = kn$ for some integer k.

iv. Restrictions on Integer Division relation:

The divisor should be a positive integer(n>0)

The remainder should be a non-negative integer(r>=0)

v. Greatest common divisor(GCD):

The Greatest common divisor of two positive integers is the largest integer that can divide both the integers. It is also called highest common factor. The greatest common divisor (g.c.d.) of the integers' x 'and 'y' is the largest integer 'd' which divides both integers, denoted

$$d = \gcd(x, y)$$

The g.c.d. exists if at least one of the integers x and y is = 0. Note that the g.c.d. is positive.

(It's often agreed, however, that gcd(0, 0) = 0.). If gcd(x, y) = 1 then we say that x and y have no common divisors or that they are coprime.

Example:

gcd(15, 5) = 5

gcd(7, 9) = 1

gcd(12, 9) = 3

gcd(81, 57) = 3.

## VI. Euclidean algorithm for GCD

A mathematician Euclid developed an algorithm that can find the greatest common divisor of two Positive integers. The Euclidean algorithm for GCD is based on the facts.

1. gcd(a,0)=a
2. gcd(a,b) = gcd(b,r) where r is remainder of dividing a by b

### A. *Extended Euclidean algorithm*

The extended Euclidean algorithm is particularly useful when *a* and *b* are coprime, since *x* is the modular multiplicative inverse of *a* modulo *b*, and *y* is the modular multiplicative inverse of *b* modulo *a*[7,8].

The Extended Euclidean Algorithm is just a fancier way of doing what we did Using the Euclidean algorithm above. It involves using extra variables to compute ax + by = gcd(a, b) as we go through the Euclidean algorithm in a single pass.

Algorithm: Extended Euclidean algorithm

INPUT : Two non-negative integers a and b with a ≥ b.

OUTPUT: d = gcd(a, b) and integers x and y satisfying ax + by = d.

```
1. If b = 0 then set d = a, x = 1, y = 0, and return(d, x, y).
2. Set x2 = 1, x1 = 0, y2 = 0, y1 = 1
3. While b > 0, do
      a. q = floor(a/b), r = a - qb, x = x2 - qx1, y = y2 - q y1.
      b. a = b, b = r, x2 = x1, x1 = x, y2 = y1, y1 = y.
4. Set d = a, x = x2, y = y2, and return(d, x, y).
```

1. Find gcd(81,57) by extended Euclidean algorithm

81 = 1[57]+24<br>
57= 2[24]+9<br>
24 = 2[9]+6<br>
06 =2[3]+0

from the last 6 = 24-2[9]. so 3 = 9-1[6]

line before that 9 = 57-2[24] so

3 = 9-1[24-2[9]]

= 3[9]-1[24]

line before that

24 = 81-1[57] giving us so

3 = 3[57-2[24]]-1[24]

= 3[57] - 7[24]

3 = 3[57]-7[81-1[57]]

= 10[57]-7[81]

P = -7 and S = 10

### B. *Linear Diophantine Equation*

A Diophantine equation is a polynomial equation whose solutions are restricted to integers. These types of equations are named after the ancient Greek mathematician, Diophantus[10]. A linear Diophantine equation is a first degree equation of this type. Diophantine equations are important when a problem requires a solution in whole amounts.

A linear Diophantine equation (in two variables) of the general form

ax + by =c ……………………1

where solutions are sought with a , b and c integers

A new procedure for finding the general solution of a linear diophantine equation is given. As a byproduct, the algorithm finds the greatest common divisor(gcd) of a set of integers . Related results and discussion concerning existing procedures are also given

**particular Solution**:

if d/c the particular solution to the above equation[11] can be found using following steps:

1. Reduce the equation to $a_1x+b_1y = c$, by dividing both sides of equation by d. This is possible because d divides a, b and c by assumption
2. Solve for S and T in the relation $a_1S+b_1T = 1$ using extended Euclidean algorithm
3. The Particular Solution can be found

P.S = $x_0 = [c\backslash d]_S$ and $y_0 = [c\backslash d]_T$

**General Solution**

After Particular Solution found, the next step is to find general Solution[12].

G.S = x = $x_0 + k[b\backslash d]$ and

$y = y_0 - k[a\backslash d]$ where k is an integer

## III. Implementation

### 1.The Extended Euclidean Algorithm

#### *Method 1 : Tabular Method*

The following table shows how the extended Euclidean algorithm proceeds with input 240 and 46. The greatest common divisor is the last non zero entry, 2 in the column "remainder". The computation stops at row 6, because the remainder in it is 0. Bézout coefficients appear in the last two entries of the second-to-last row. In fact, it is easy to verify that −9 × 240 + 47 × 46 = 2. Finally the last two entries 23 and −120 of the last row are, up to the sign, the quotients of the input 46 and 240 by the greatest common divisor 2.

#### *Method 2 : Back - Substitution*

m = 400 , n = 60

Step 1: The (usual) Euclidean algorithm:

(1) 400 = 6.60 + 40<br>
(2) 60 = 1.40 + 20<br>
(3) 40 = 2.20 + 0

Therefore gcd(400 , 60) = 20

Step 2: Using the method of back-substitution:

1.60 - 1.40 = 20<br>
1.60 - 1(1.400 - 6.60) = 20<br>
1.60 - 1.400 + 6.60 = 20<br>
-1.400 + 7.60 = 20

Therefore S = -1 and T = +7

Table 1.1 Extended Euclidean Algorithm

| Index i | Quotient $q_{i-1}$ | Remainder $r_i$ | $S_i$ | $t_i$ |
|---|---|---|---|---|
| 0 | | 240 | 1 | 0 |
| 1 | | 46 | 0 | 1 |
| 2 | 240+46 = 5 | 240 - 5 * 46 = 10 | 1 - 5 * 0 = 1 | 0 -5 * 1 = -5 |
| 3 | 46 + 10 = 4 | 46 - 4 * 10 = 6 | 0 - 4 * 1 = -4 | 1 - 4 * -5 = 21 |
| 4 | 10 + 6 = 1 | 10 - 1 * 6 = 4 | 1 * 1 * -4 = 5 | -5 -1 * 21 = -26 |
| 5 | 6 + 4 = 1 | 6 - 1 * 4 = 2 | - 4 - 1 * 5 = -9 | 21 -1 * -26 = 47 |
| 6 | 4 + 2 = 2 | 4 - 2 * 2 = 0 | 5 -2 * -9 = 23 | -26-2*47 = -120 |

***2. Linear Diophantine Equation***

Example 1. Let the equation be

$$60x + 33y = 9.$$

And find all solution to $60x + 33y = 9$.

So, $a = 60$, $b = 33$, $c = 9$ and $(60, 33) = 3$, we can see $3|9$. So we can search for solutions.

First, we use euclidean algorithm

$60=1.33+27$

$33=1.27+6$

$27=4.6+3$

$6=2.3+0$

We see the last nonzero remainder is 3 so $(60, 33) = 3$.

Reverse by step

$$\begin{aligned} 3 &= 27 - 4 \cdot 6 \\ &= 27 - 4 \cdot (33 - 27) \\ &= 5 \cdot 27 - 4 \cdot 33 \\ &= 5 \cdot (60 - 33) - 4 \cdot 33 \\ &= 5 \cdot 60 - 9 \cdot 33. \end{aligned}$$

So we take $u = 5$ and $v = -9$. One solution is then,

$X0=5.(9/3)=15$

$Y0=-9.(9/3) = - 27$

## IV.CONCLUSIONS

With the touchy advance in the Internet, system and information security have turned into an inevitable sympathy toward any association whose interior private system is associated with the Internet. The protection for the information has turned out to be exceptionally essential. Network security consists of the necessities made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together data safety can be done in cryptography using mathematics. Extended Euclidean algorithm is an extension to the Euclidean algorithm, which computes, the greatest common divisor of integers a and b, because the gcd is the only number that can all together satisfy this equation and divide the inputs. The extended Euclidean algorithm is particularly useful when a and b are co prime. Finding the extended Euclidean algorithm is a lengthy process in the tabular method is a complicated method when compared to Back-substitution method. The simplest linear Diophantine equation takes the form ax + by = c, where a, b and c are given integers. A linear Diophantine equation is an equation that sums two monomials of degree zero or one. it involves a simple procedure as well as it provides particular and general solutions. it is easy to compute.

## REFERENCE

*1. Lehmer, D. H. (1938). "Euclid's Algorithm for Large Numbers". The American Mathematical Monthly. 45 (4): 227–233. doi:10.2307/2302607. JSTOR 2302607.*

*2. Sorenson J (1995) An analysis of Lehmer's euclidean GCD algorithm. In: Proceedings of the 1995 international* *symposium on Symbolic and algebraic computation. ACM Press, New York, pp 254–258CrossRef*

*3. Euclid (1986) Thirteen books of Euclid's elements, 2nd edn. Dover, New York*

*4. Cohen H (1993) A course in computational algebraic number theory. Springer, BerlinMATH*

*5. Knuth, Donald. The Art of Computer Programming. Addison-Wesley. Volume 2, Chapter 4.*

*6. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Pages 859–861 of section 31.2: Greatest common divisor.*

*7. Greatest Common Measure: The Last 2500 Years, by Alexander Stepanov*

*8. Saunders MacLane and Garrett Birkhoff. A Survey of Modern Algebra, Fourth Edition. MacMillan Publishing Co., 1977. ISBN 0-02-310070-2. 1–7: "The Euclidean Algorithm."*

*9. M.R.K. Ariffin and N.A. Abu, -cryptosystem: "A chaos based public key crypto-system", Int. Jour. Cryptology Research, vol. 1, no. 2, pp. 149 – 163, Dec. 2009.*

*10. M.R.K. Ariffin, N.A. Abu and A. Mandangan, "Strengthening the-cryptosystem" Proc. Second International Cryptology Conference 2010, pp. 16 - 26, 2010.*

*11. S.R. Blackburn, " The Discrete Log Problem Modulo 1: Cryptanalyzing the Ariffin – Abu cryptosystem," J. Mathematical Cryptology, vol. 4, pp. 193-198, 2010.*

*12. R. Bose, "Novel Public Key Encryption Techniques Based on Multiple Chaotic Systems",Physic Review Letters, vol. 95, issue 9, id. 098702. 2005.*