ORIGINAL RESEARCH PAPER

Mathematics

Volume : 6 | Issue : 12 | December : 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 79.96

Mathematical Approach for Cryptography

KEYWORDS

Number theory, Elliptic curves,. Cryptography.

Dr .S.Vasundhara

Asst.Prof of Mathematics, G.Narayanamma Institute of Technology &science For Women) Shaikpet, Hyderabad

ABSTRACT *This paper provides an overview of elliptic curves and their use in cryptography. The focus of the paper is on the performance of mathematical background required. The main difference between RSA and Elliptic Curve Cryptography is that unlike RSA, Elliptic Curve Cryptography offers the same level of security for smaller key sizes. Elliptic Curve Cryptography is highly mathematical in nature. While conventional public-key cryptosystems (RSA, Diffie - Hellman and DSA) operate directly on large integers, an Elliptic Curve Cryptography operates over points on an elliptic curve using elliptic curve cryptography instead of traditional cryptosystemssuch as RSA. Specific applications to secure messaging and identity-based encryptionare also discussed.*

I. Introduction

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithms may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in Elliptic

History of Elliptic Curve Cryptography

Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems almost 20 years ago, independently by Victor Miller ofIBM and Neal Koblitz of the University of Washington. At that time, elliptic curves being used in various cryptographic contexts, such as integer factorization and primarily proving.

Modulo arithmetic:

Let d be an integer and let n be a positive integer. Let q and r be the quotient and remainder obtained from dividing d by n, The relationship between d,n,q, and r is

$$d=n*q+r, 0\leq r\leq n \quad (1)$$

Note that r is a non negative integer less than, d and n are the dividend and the divisor, respectively, we say "d is equal to r modulo n "if the remainder from dividing d by n is r. This is expressed as

$$r \equiv d(\text{mod } n) \quad (2)$$

for a given value of n and r there are an infinite number of (d,q) pairs that satisfy Eq.1
let n=10 and r=3
then 13,23,33 etc all satisfy with quotient 1,2,3 etc in fact each element of the set below satisfies eq(2.2)
{.....-37,-27,-17,-7, 3, 13, 23, 33, 43.....}

Congruence:

Any two numbers in the above set are said to be congruent modulo 10 and the set itself is referred to as a congruence class. It is helpful to visualize the modulo n relationship using the integers are laid out along a spiral with n integers on a single circle starting with 0 we encounter the positive integers in sequence as we traverse the spiral clockwise direction. The set of elements along a given radius constitute one of the congruence class modulo n. There is n congruence classes' mod n. It is convenient to represent a class by the smallest non-negative integer in that class.

Two distinct integers a and b that are congruent modulo n map to the same radius in the spiral counting from a to b involves one or more revolutions. it follows that :

Fact: If two integers are congruent modulo n, then they differ by an integral multiple of n algebraically, if
a mod n=r and b mod n=r,

Then $a=n*q_1+r$ and
$b=n*q_2+r$

Where q_1 and q_2 are integers.
Subtracting we get
$a-b=n(q_1-q_2)$
Since q_1 and q_2 are integers a and b differ by an integral multiple of n,
Many useful properties of modulo arithmetic can be proved using the above fact.

1.(a+b) mod n=((a mod n)+(b mod n)) mod n
2.(a-b) mod n=((a mod n)-(b mod n)) mod n
3.(a*b) mod n=((a modn) * (b mod n)) mod n

Greatest common divisor: Having introduced the concept of a divisor of an integer, we will now deal with the concept of the common divisor of two (or more) integers.

Given two integers a and b, the integer c is a common divisor of a and b, if c | a and c| b. A notion of greatest common divisor is a very important one. It is the largest possible common divisor of a and b and is formally defined as

Definition: Let a, b, c and d∈Z with d > 0. d is the greatest common divis or of a and b denoted d = gcd(a, b) if:

1. d| a and d | b
2. Whenever c | a and c | b, then c | d.

Example:
The common divisors of 12 and 18 are ±1, ±2, ±3, ±6, and gcd (12, 18) = 6. gcd(20, 30) = 10 and gcd(−12, 8) = 4.

We notice that the greatest common divisor gcd(a, b) of two integers a and b always exists and is unique. Furthermore, it can be written as a linear combination of a and b. This combination is however, not unique. For instance, $\gcd(24, 9) = 3 = 3 \cdot 9 + (-1) \cdot 24 = (-5) \cdot 9 + 2 \cdot 24$

Theorem: *If* a, b ∈ Z, are not both 0, then their greatest common

Volume : 6 | Issue : 12 | December : 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 79.96

divisor gcd (a, b) exists, is unique, and moreover can be written as linear combination of a and b, i.e. gcd(a, b) = xa + yb for some suitable integers x and y.

Euclidean Algorithm: The Euclidean algorithm is an efficient algorithm for computing the greatest common divisor of two integers that does not require the factorization of the integers. It is based on the following simple theorem

Theorem: *Let* a, b ∈ Z. *Then,*

1. if b = 0, *then* gcd(a, b) = |b|,
2. *if* b ≠ 0, *then* gcd(a, b) = gcd(|b|, a mod |b|) .

The previous theorem enables the computation of the greatest common divisor gcd(a, b) as follows:
We suppose r_0 = a, r_1 = b and a > b > 0, then we introduce the notation
r_i+1 = r_i−1 mod r_i for each integer i ≥ 1 and r_i ≠ 0

Then, we compute r_i+1 = r_i−1 mod r_i for i = 1, 2, 3 . . . until we obtain for a fixed
i_o ≥ 1:
r_i+1 = 0.
Then, the greatest common divisor is ri0.
If a = 0 resp. b = 0, then gcd(a, b) = b resp. gcd(a, b) = a.

Example:
We want to determine gcd (110, 40). Using the notation introduced above, we Obtain the following table

Table: 2.3

I	0	1	2	3	4
r_i	110	40	30	10	0

From the table we get r_4 = 0, i.e. i_0 = 3 and r_3 = 10 is the greatest common divisor of 110 and 40, i.e. gcd(110, 40) = 10.

Extended Euclidean Algorithm:
The Euclidean algorithm can be extended so that it not only yields the greatest Common divisor of two integers a and b, but also integers x and y satisfying the
Linear combination:
ax+ by = gcd(a, b).

This algorithm is called the Extended Euclidean algorithm and is very Important, since it can be used to compute a multiplicative inverse in Groups.

Corollary: For all a, b, n ∈ N, the equation ax + by = n has two integers xand y as solution if gcd (a, b) divides n.

This corollary means that the equation ax + by = gcd (a, b) is always solvable. Given two integers a and b as input, with the Extended Euclidean algorithm the two Unknown integers x and y as well as the greatest common divisor of a and b can be determined so that
ax+ by = gcd(a, b).

This will be illustrated in what follows
Let r_0 = a, r_1 = b, r_2 = a mod b and $q_1 = \frac{a}{b}$.

If r_2 ≠0, then:

$r_3 = r_1 \bmod r_2$ and $q_2 = \frac{r1}{r2}$

Generally, we continue with this notation until r_i= 0:
$r_{i+1} = r_{i-1} \bmod r_i$ and q_i = ri|, 1 ≤ i ≤ n.
We start with x_0 = 1, y_0 = 0, x_1 = 0, y_1 = 1 and compute in every further iterate

Euler's phi-function
Euler's phi-function, φ(n), which is some times called the Euler's totient function plays a very important role in cryptography. The function finds the number of integers that are both smaller 23than n and relatively primes to n. The set Z_n* contains then number of elements in this set. The following helps to find the value of φ(n).

1. φ(1)=0.
2. φ(p)=p-1 if p is prime.
3. φ(mxn)=φ(m)xφ(n) if m and n are relatively prime.
4. $\varphi(p^c)=p^c-p^{c-1}$ if p is a prime.

We can combine the above four rules to find the value of $n=p_1^{e_1}Xp_2^{e_2}p_3^{e_3}X.....p_k^{e_k}$, then we combine the third and the fourth rule to find $\varphi(n)= (p_1^{e_1}-p^{e1-1}{}_1)$ X $(p_2^{e_2}-p^{e_2-1}{}_2)$..... $(p_k^{e_k}-p^{e_{k-1}}{}_k)$ it is very important to notice that the value of φ(n for large composites can be found only if the number n can be factored into primes. In other words the difficulty of finding φ(n) depends on the difficulty of finding the factorization of n.

Fermat's little theorem: Fermat's little theorem plays a very important role in number theory and cryptography. We introduce two versions of the theorem here.

First version: The first version says that if p is a prime and a is an integer such that p does not divide a , then ap-1≡ 1 mod p.

Second version The second version removes the condition on a. It says that p is a prime and a is an integer, then ap≡a mod p.

Exponentiation Fermat's little theorem sometimes is helpful for quickly finding a solution to some exponentiations. The following examples show the idea.

Example. Find the result of 610 mod 11=1.This is the first version of Fermat's little theorem where p=11.

Find the result of 3^{12} mod 11.
Here the exponent (12) and the modulus (11) are not the same. With substitute this can be solved using Fermat's little theorem.
3^{12} mod 11=(3^{11}x3) mod 11=(3^{11} mod 11)(3 mod 11)=(3x3)mod 11=9
Multiplicative inverse. A very interesting application of Fermat's little theorem is in finding some multiplicative inverses quickly if the modulus is a prime .If p is a prime and a is an integer such that p does not divide a (p/a), then a^{-1} mod p=a^{p-2} mod p.
This can be easily proved if we multiply both sides of the equality by a and use the first version of Fermat's little theorem:
aa^{-1} modp= aa^{p-2} mod p=a^{p-1} mod p=1 mod p
Example. The answers to multiplicative inverses modulo prime can be found without using the extended algorithm:

a. 8^{-1} mod 17=8^{17-2} mod 17=8^{15} mod 17=15 mod 17
b. 5^{-1} mod 23=5^{23-2} mod 23=5^{21} mod 23=14 mod 23
c. 60^{-1} mod 101=60^{101-2}mod 101=60^{99}mod 101=32 mod 101
d. 22^{-1}mod 211=22^{211-2}mod 211=22^{209}mod 211=48 mod 211

References

1. Alfred J. Menezes, Paul C. van Oorschotand Scott A. Vanstone, Guide to Elliptic curve Cryptography, 1996.
2. Certicom, Standards for EfficientCryptography, SEC 1: Elliptic Curv.
3. George Barwood. Elliptic curve cryptographyfaq v1.12. 1997.Bruce Schneier.
4. Appliedcryptography (2nd ed.): protocols, algorithms, andsource code in C. John Wiley & Sons, Inc., NewYork, NY, USA, 1995.
5. N.Koblitz,A course in Number theory and cryptography,2nd ed.,brookes/ Cole, 1997.
6. N.A course in Number theory and cryptography. Newyork: Springer-Verlag, 1994. CER.TICOM:A Tutorial for Elliptic curve