Public Key Cryptography

Unit II

Number Theory

Introduction

- Number Theory is branch of mathematics devoted to the study of the properties of natural numbers and the integers.
  - Sometimes called “higher arithmetic,” it is among the oldest and most natural of mathematical pursuits.
- Mathematical interaction and number types are studied in number theory.
  - Types of numbers: odds, evens, primes, squares, integers
- Formal Mathematical proofs are used to describe or prove relationships among number types.

Introduction..

- Euclid was a number theorist who studied prime numbers.
  - He answered the question that “how many prime numbers are there?”
  - He proves that there are infinite prime numbers and used formal mathematics to prove it.
    - He used proof by contradiction for this purpose where he first assumed that there are finite prime numbers and then proved it wrong.
- Number theory is all about asking questions about numbers.

Introduction…

Number theory has its roots in the study of the properties of the natural numbers

$$\mathbb{N} = \{1,2,3, \dots\}$$

and various “extensions” thereof, beginning with the integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1 , 2, \dots\}$$

and rationals.

$$\mathbb{Q} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0 \right\}$$

This leads directly to distinct properties…

- Divisibility
- Congruences
- Cryptography
- Elliptic curve cryptography

Divisibility

- Euclidean algorithm and greatest common divisors.
- Primes and the Fundamental Theorem of Algebra
- Results and conjectures concerning primes:
  - Euclid’s theorem
  - The Riemann zeta function;
  - Arithmetic progressions

Congruences

- Modular (clock) arithmetic: $a^{(p-1)} \equiv 1(mod\ p)$ and its generalizations.
- Chinese remainder theorem
- A first view of primality testing and factorization.
- Groups, rings and fields (especially finite abelian groups and finite fields).
- Primitive roots modulo a prime
- Quadratic reciprocity

Cryptography

- Simple cryptosystems and symmetric ciphers
- Public key cryptography
  - Answer the question “How can two parties communicate securely over an insecure channel without first privately exchanging some kind of ‘key’ to each others’ messages?” They need a trapdoor function f that can be used to encode information easily but hard to invert without knowing “extra information”.
- Diffie-Hellman key exchange
- RSA cryptosystem

Elliptic Curve Cryptography

- The security of using elliptic curves for cryptography rests on the difficulty of solving an analogue of the discrete log problem.
- We can also use the group law on an elliptic curve to factor large numbers (Lenstra's algorithm).
- A deeper, more flexible sort of cryptosystem can be obtained from the "Weil pairing" on m-torsion points of an elliptic curve.

Euclidean Algorithm for GCD

- Used to determine GCD of two positive integers

Modular Arithmetic

Introduction

- Modulo operations
  - $7 \, mod \, 4 = 3$
  - $-11 \, mod \, 7 = 3$
- Negative Modulus can be calculated using the formula
  - $-x \, mod \, y = y \, - (x \, mod \, y)$
    - $if \, |x| \, mod \, y \, \neq 0$, it works
    - $if \, |x| \, mod \, y = 0$, it fails

Congruent modulo

- Two integers $a\ and\ b$ are said to be congruent Modulo n if
  - $(a\ mod\ n) = (b\ mod\ a)$
  - This is written as, $a\ \equiv (b\ mod\ n)\quad or\quad b\ \equiv (a\ mod\ n)$
  - E.g. $73\ \equiv 4\ (mod\ 23)\ means\ \ldots 73\ mod\ 23 = 4\ mod\ 23$
- Properties of congruence
  - $a\ \equiv b\ (mod\ n)\ \ if\ n\ |\ (a - b)$
  - $a\ \equiv b\ (mod\ n)\ \ implies\ \ b \equiv a\ (mod\ n)$
  - $if\ a\ \equiv b\ (mod\ n)\ \ and\ \ b\ \equiv c\ (mod\ n)$
    - $then, \boldsymbol{a}\ \equiv \boldsymbol{c}\ (\boldsymbol{mod}\ \boldsymbol{n})$

Modular Arithmetic properties

- $(a + b) mod\ n = [(a\ mod\ n) + (b\ mod\ n)]\ mod\ n$
- $(a - b) mod\ n = [(a\ mod\ n) - (b\ mod\ n)]\ mod\ n$
- $(a \times b) mod\ n = [(a\ mod\ n) \times (b\ mod\ n)]\ mod\ n$
  - E.g. $let\ a = 11, b = 15, n = 8$

    $\therefore (a \times b) mod\ n = (11 \times 15)\ mod\ n$

    $165\ mod\ 8 = 5$
  - $[(a\ mod\ n) \times (b\ mod\ n)]\ mod\ n = [(11\ mod\ 8) \times (15\ mod\ 8)]\ mod\ 8$

    $= (3\ \times 7) mod\ 8$

    $= 21\ mod\ 8$

    $= 5$

Modular Arithmetic properties

- $if\ x\ \equiv y\ mod\ n\ ,\ a \equiv b\ mod\ n\ \ then, (\boldsymbol{x} + \boldsymbol{a}) \equiv (\boldsymbol{y} + \boldsymbol{b})\boldsymbol{mod\ n}$
  - E.g. $if\ 17 \equiv 4\ mod\ 13\quad ,\quad 42 \equiv 3\ mod\ 13$
  - $then,\ \ \mathbf{59} \equiv \mathbf{7}\ \boldsymbol{mod}\ \mathbf{13}\ \ \boldsymbol{is\ true}$
- $if\ x \equiv y\ mod\ n\ \ and\ \ a \equiv b\ mod\ n\ then, (\boldsymbol{x} - \boldsymbol{a}) \equiv (\boldsymbol{y} - \boldsymbol{b})\ \boldsymbol{mod\ n}$
  - $if\ 42\ \equiv 3\ (mod\ 13)\ \ ,\quad 14\ \equiv 1\ (mod\ 13)$
  - $then, \mathbf{28}\ \equiv \mathbf{2}\ (\boldsymbol{mod}\ \mathbf{13})\ \boldsymbol{is\ true}$

Euler’s Totient Function

Introduction

- It is represented using $phi\ as\ \phi(n)$ and may also be called Euler's phi function.
- Euler's totient function is defined as the no. of $+ve$ integers less than n that are coprime (having GDC 1) to n
  - $n \geq 1$
    - $\phi(5) = \{1,2,3,4\}$
    - $\phi(6) = \{1,5\}$ no. of elements in these sets is totient function.
  - Two integers a , b are said to be relatively prime, mutually prime or coprime if the only if $+ve$ integer / factor that divides both of them is 1
    - Now, when $n \ \rightarrow prime \quad \phi(n) = n - 1$
      - E.g. $\phi(5) = 4,\ \phi(23) = 23 - 1 = 22$
  - Also, $\phi(a * b) = \phi(a) * \phi(b) \quad [a\ \&\ b\ should\ be\ coprime]$
    - E.g. $\phi(35) = \phi(7)$* $\phi(5) = 6 * 4 = 24$

Totient Function Chart

n	$\phi(n)$	$nos. of\ coprime\ to\ n$
1	1	1
2	1	1
3	2	1, 2
4	2	1, 3
5	4	1, 2, 3, 4
6	2	1, 5
7	6	1, 2, 3, 4, 5, 6
8	4	1, 3, 5, 7
9	6	1, 2, 4, 5, 7, 8
10	4	1, 3, 7, 9

Euler’s Theorem

Fermat-Euler Theorem or Euler’s Totient Theorem

Introduction

- Euler’s theorem states that if x and n are coprime positive integers, then

$$\boldsymbol{x^{\phi(n)} \equiv 1\, mod\, n}$$

    - $where\ \phi(n) \rightarrow Euler's\ totient\ function$

- It is a generalized version of Fermat’s Theorem
  - E.g. $let\ x = 11, n = 10$ both are coprime
  - $\therefore\ we\ can\ represent\ them\ as$

$$11^{\phi(10)} \equiv 1\, mod\ 10$$
$$11^{4} \equiv\ 1\, mod\ 10$$
$$14641\ \equiv 1\, mod\ 10$$

- Note, $x^{\phi(n)a} \equiv 1\, mod\ n$
  - $11^{4*2} = 1\, mod\ 10$

Numerical Example

- Solve by Euler's Theorem
  - $4^{99} mod\ 35$

$$x = 4, n = 35$$
$$By\ Euler's\ theorem,$$
$$4^{\phi(35)} = 1\ mod\ 35$$
$$4^{24} \equiv 1\ mod\ 35\ \ \dots\dots(1)$$
$$4^{99} \rightarrow 4^{24(4)}.\ 4^{3}$$
$$\therefore 4^{99} mod\ 35 = 4^{24*4+3} mod\ 35$$
$$= (4^{24})^{4}\ \times 4^{3} mod\ 35$$
$$= \ (4^{24})^{4}\ mod\ 35\ \times 4^{3} mod\ 35$$
$$\text{Type equation here.}$$
$$\because (a \times b) mod\ n \equiv (a\ mod\ n)(b\ mod\ n)$$
$$= 1 \times 4^{3} mod\ 35$$
$$= 64\ mod\ 35 = 29$$
$$\therefore 4^{99} mod\ 35 = 29$$

Fermat’s Theorem

Fermat’s Little Theorem

Introduction

- It is special case of Euler's theorem
  - $If\ n\ is\ prime\ and\ 'x'\ is\ a + ve\ integer\ not\ divisible\ by\ n\ then$

$$x^{n-1} \equiv 1\ mod\ n, \qquad \phi(n) = n - 1$$
$$n \rightarrow prime\ no.$$
$$x\ is\ not\ divisible\ by\ n$$

  - $e.g.\ x = 3,\ n = 5$

$$3^{5-1} = 3^4 = 81$$

$\therefore 81 \equiv 1\ mod\ 5$

Euler’s Theorem

- $x^{\phi(n)} \equiv 1\, mod\, n$
- $x^{n-1} \equiv 1\, mod\, n\ \ \dots\dots Fermat's\ Theorem$
- Another form of Fermat's Theorem
  - $x^{n} \equiv x\, mod\, n$

Numerical solved by Fermat’s Theorem

- $2^{16} mod\ 17$

$$By\ Fermat's\ Theorem$$
$$x^{n-1} \equiv 1\ mod\ n$$
$$2^{17-1} \equiv 1\ mod\ 17$$
$$2^{16} \equiv 1\ mod\ 17$$
$$\therefore 2^{16} mod\ 17 = 1$$

RSA Algorithm

Introduction

- Rivest-Shamir-Adleman developed in 1978
- It is an asymmetric cryptographic algorithm (2 keys) i.e. public and private key concepts is used here.
- The acronym RSA is made from the initial letters of the surnames of Ron Rivest, Adi Shamir & Leonard Adleman.
- Public key: known to all users in network
- Private Key: Kept secret, not sharable to all

Introduction…

- If public key of user A is used for encryption, we have to use the private key of same user for decryption.
- RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some value n.

Key Generation

- Select 2 large prime numbers $'p'$ and $'q'$
- Calculate $n = p * q$
- Calculate $\phi(n) = (p-1) * (q-1) \ldots\ldots\ldots\ldots\ldots Euler's\ Totient\ F^n$
- Choose value of e

$$1 < e < \phi(n) \quad and \quad \gcd(\phi(n), \mathrm{e}) = 1$$

- Calculate

$$d \equiv e^{-1} mod\ \phi(n)$$
$$i.e. ed \equiv 1\ mod\ \phi(n)$$

- Public key : $\{e, n\}$
- Private Key: $\{d, n\}$

Encryption & Decryption

- Plaintext = $M < n,\ C = Ciphertext$
- Encryption

$$C = M^e mod\ n$$

- Decryption

$$M = C^d\ mod\ n$$

- Note
  - (e, n) is public key used in encryption
  - (d, n) is private key used for decryption

Chinese Remainder Theorem

Introduction

- Chinese remainder theorem states that there always exists an “x” that satisfies the given congruence.

$$x \equiv rem[0] (mod\ num[0])$$
$$x \equiv rem[1] (mod\ num[1])$$
$$\dots \dots \dots \dots$$
$$and\ (num[0], num[1], \dots \dots, num[m - 1])\ all\ must\ be\ coprime\ to\ one\ another$$

Examples

- $e.g\ 1{:}\ x \equiv 1\ mod\ 5, x \equiv 3\ mod\ 7;$
  - $here\ 5\ and\ 7\ are\ coprime\ we\ have\ to\ find\ this\ x = 31$

- $e.g. x \equiv 2\ mod\ 3, x \equiv 3\ mod\ 4, x \equiv 1\ mod\ 5$
  - $\gcd(3,4) = \gcd(4,5) = \gcd(3,5) = 1$

    $hence\ they\ coprime\ and\ then\ only\ x\ exists$

    $here, x = 11$

Question

- If we have N books and if we divide it in 5 students remainder=3 and if we divide it in 4 students books left = 2, so find the no. of books?
  - As per Chinese remainder theorem
    if,
    $x \equiv a_1 \; mod \; m_1$
    $x \equiv a_2 \; mod \; m_2$
    $x \equiv a_3 \; mod \; m_3$
    $(i) \gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_3, m_1) = 1 \; i.e \; all \; are \; coprime$

$$(ii) x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 + \cdots + M_n X_n a_n) mod \; M$$

$$M = m_1 * m_2 * m_3 \ldots \ldots m_n$$

$$M_i = \frac{M}{m_i}$$

$$\therefore M_1 = m_2 m_3; \;\; \mathrm{M}_2 = \mathrm{m}_1 \mathrm{m}_3; \;\;\; \mathrm{M}_3 = \mathrm{m}_1 \mathrm{m}_2$$

Continued…

- To calculate X_i

$$M_i X_i \equiv 1 \, mod \, m_i$$
$$e.g. M_1 X_1 \equiv 1 \, mod \, m_1$$

Diffie-Hellman Key exchange Algorithm

Introduction

- It is not an encryption algorithm
- It is used to exchange the secret keys between 2 users
- We will use asymmetric encryption to exchange the secret key b/w users
- Why to use algorithm
  - Because when we are sending a key to receiver, it can be attacked in between

Algorithm

- Consider a prime number 'q'
- Select 'α' such that it must be the primitive root of 'q' and $\alpha < q$

  $'a' is\ a\ primitive\ root\ of\ q\ if$

  $a\ mod\ q$

  $a^2 mod\ q$

  $a^3 mod\ q\ \ldots\ldots\ldots\ldots\ldots\ldots a^{q-1} mod\ q$

  $gives\ results\ \{1,2,3,\ldots\ldots,q-1\}$

  $i.e\ values\ should\ not\ be\ repeated\ \&$

  $we\ should\ have\ all\ values\ in\ the\ set\ from\ 1\ to\ q-1$

Algorithm continued…

Note: $X \rightarrow private\ key\ of\ user$; $Y \rightarrow public\ \ key\ of\ user$

- Assume X_A(private key) and $X_A < q$ of A

$$Calculate\ Y_A = \alpha^{X_A} mod\ q \quad \rightarrow public\ key\ of\ A$$

- Assume X_B (private key of B) and $X_B < q$

$$Calculate\ Y_B = \alpha^{X_B} mod\ q \quad \rightarrow public\ key\ of\ B$$

- Now to calculate the secret key both the sender & receiver will use public keys

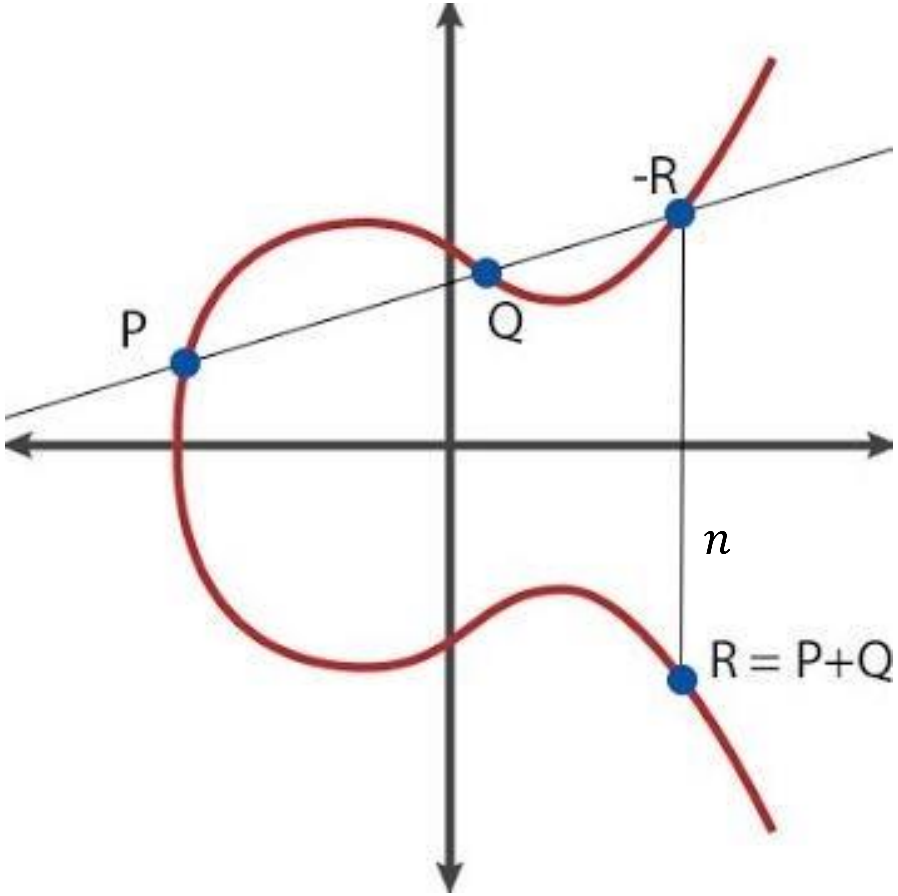
$$K_1 = (Y_B)^{X_B} mod\ q \qquad K_2 = (Y_A)^{X_B} mod\ q$$

- $K_1 = K_2; then\ we\ say\ exchange\ is\ successful$.

Elliptic Curve Cryptography

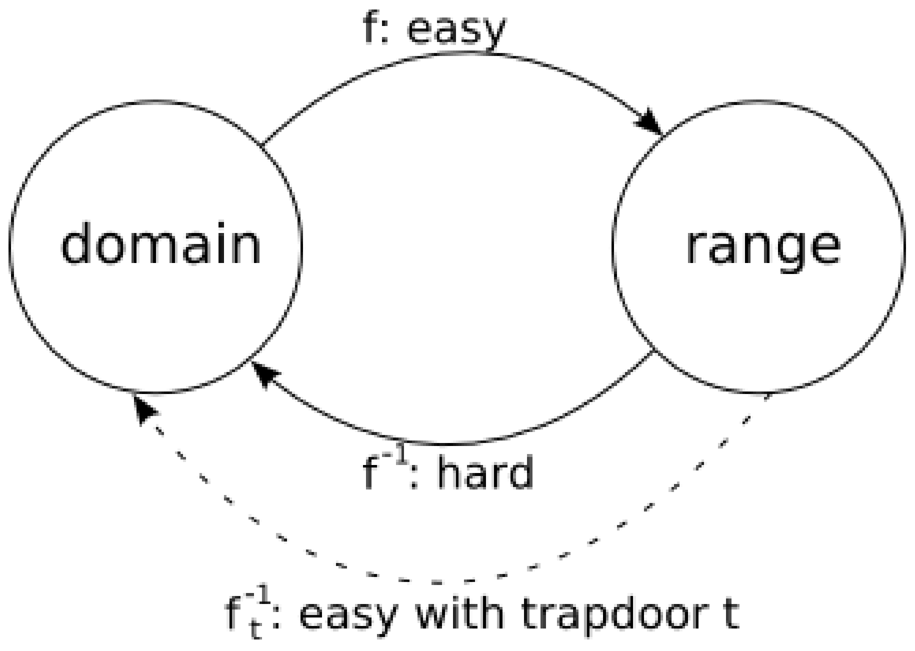
Introduction

- It is asymmetric public key cryptosystem.
- It provides equal security with smaller key size (as compared to RSA) as compared to non ECC algos. i.e. small key size and high security
- It makes us of Elliptic curves.
- Elliptic curves are defined by some mathematical functions cubic form e.g. $y^2 = x^3 + ax + b \quad \rightarrow$ $equation\ of\ degree\ 3$



Trapdoor Function

- It is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the trapdoor.



Algorithm

- Let $E_p(a, b)$ be the elliptic curve
  Consider the equation,
  $$Q = KP; \quad where\ Q, P\ are\ points\ on\ curve\ \&\ K < n$$
- If $K\ and\ P\ \rightarrow given$, it should be easy to find Q but if we know $Q\ and\ P$, it should be extremely difficult to find K.
  This is called the discrete logarithm problem for elliptic curves. And it is a one way function i.e. trapdoor function.

ECC - Algorithm

ECC – Key Exchange

- Global Public Elements
  - $E_q(a, b)$: elliptic curve with parameters a, b and q (prime no. or an integer of the form 2^m)
  - G : Point on the elliptic curve whose order is large value of n
- User A key generation
  - Select private key n_A, $n_A < n$
  - calculate public key P_A, $P_A = n_A \times G$
- User B key generation
  - Select private key n_B, $n_B < n$
  - calculate public key P_B, $P_B = n_B \times G$

ECC – Algorithm continues…

- Calculation of secret key by user A
  - $K = n_A \times P_B$
- Calculation of secret key by user B
  - $K = n_B \times P_A$

ECC Encryption

- Let the message be M
- First encode this message M into a point on elliptic curve.
- Let this point be $P_m \rightarrow This\ point\ is\ encrypted$
  for encryption chose a random positive integer k
- The Cipher point will be
  $C_m = \{kG, P_m + kP_B\}$, for encryption public key of B is used
  this point will be sent to the receiver

ECC - Decryption

- For decryption, multiply 1st point in the pair with receiver's secret key i.e. $kG \times n_B$, for decryption private key of B used
- Then subtract it from 2nd point in the pair i.e

$$P_m + kP_B - (KG * n_B)$$
$$but\ we\ know\ P_B = n_B \times G$$

So, $= P_m + kP_B - kP_B = P_m$ (original point)

- So, Receiver gets the same point.