Veena V Kangralkar
Asst Professor
Dept of CSE
KLSGIT, Belagavi

UNIT-5

Advanced Algorithms

* Number-Theoretic Algorithms *

Number-Theoretic Algorithms are widely used in inventions of Cryptographic Schemes based on large prime numbers Because, we don't know how to factor the product of large prime numbers efficiently.

→ A large input typically means an input containing large integer rather than an input containing many integers i.e (Sorting).

→ We shall measure the size of input in terms of the no of bits required to represent that input, not just the no. of integers in input.

* **Elementary Notations** - The Notation from Elementary number theory Concerning the set $Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of integers & Set $N = \{0, 1, 2, \ldots\}$ of Natural Numbers.

* **Divisibility & Division** - The notion of one integer being divisible by another is key to the theory of number.

* $d \mid a \Rightarrow$ "d divides a" means that $a = kd$ for some 'k'
  ⟶ a is divisible by d.

* $d \nmid a \Rightarrow$ d does not divide a.

→ There are two types of division

* Trivial division → Every +ve integer a is divisible by 1 & a.

* Non-Trivial divisions → of 'a' are factors of a.

Ex: The factors of 20 are 2, 4, 5, & 10.

* Prime & Composite numbers -

"An integer a>1 whose only division are trivial divisors 1 & a is a prime number

→ primes have many special properties & play a Critical role in number theory.

→ An integer a>1 that is not prime is a Composite number

* Common divisors & greatest Common divisors -

If d is a divisor of a & d is also a division of b, then d is a common divisor of a & b.

Ex ⇒ Divisors of 30 = 1, 2, 3, 5, 6, 10, 15, & 30.
Divisors of 24 = 1, 2, 3, 4, 6, 8, 12 & 24

* Common divisors of 30 & 24 = 1, 2, 3 & 6.

* Greatest Common divisor (GCD) of two integers a & b, not both zero, is the largest Common divisor of a & b. we denote it by gcd(a, b).

Ex: $GCD(30,24) = 6$.

→ The following are Elementary properties of gcd.

* $GCD(a,b) = GCD(b,a)$
* $GCD(a,b) = GCD(-a,b)$
* $GCD(a,b) = GCD(|a|,|b|)$
* $GCD(a,0) = |a|$
* $GCD(a,ka) = |a|$

* Relative prime integers : Two integers a & b are relatively prime if their only common divisor is 1.

Ex: Divisors of 8 = 1, 2, 4 & 8
Divisor of 15 = 1, 3, 5 & 15
∴ Common divisor = 1 (relatively prime)

* Greatest Common Divisor (GCD)-
We use Euclid's algorithm for efficiently computing the greatest common divisor (GCD) of two integers. The input integer 'a' & 'b' are arbitrary non-negative integer.

→ Euclid (a, b)
1. if b == 0
2. return a
3. Else return Euclid (b, a mod b)

→ Consider the computation of gcd (30, 21)

$$\begin{aligned} \text{Euclid}(30,21) &= \text{Euclid}(21, 30 \bmod 21) = \text{Euclid}(21,9) \\ &= \text{Euclid}(9, 21 \bmod 9) = \text{Euclid}(9,3) \\ &= \text{Euclid}(3, 9 \bmod 3) \\ &= \text{Euclid}(3,0) \end{aligned}$$

∴ GCD(30, 21) = 3

This computation calls Euclid recursively three times

Example: Extended Euclid Algorithm for (56, 15).

→ $a = 56,\ b = 15$

a	b	$\lfloor a/b \rfloor$	d	x	y
56	15	3	1	-4	15
15	11	1	1	3	-4
11	4	2	1	-1	3
4	3	1	1	1	-1
3	1	3	1	0	1
1	0	—	1	1	0

Substitute in Equation $d = ax + by$ at each step.

→ step 1 → $x' = 1,\ y' = 0$ ⟶ $d = 1(1) + 0(0) = 1$ ✓

→ step 2 → $x = 0,\ y = x' - \lfloor a/b \rfloor y' = 1 - 3(0) = 1$ ⟶ $d = 3(0) + 1(1) = 1$ ✓

→ Step 3 → $x = 1,\ y = 0 - 1(1) = -1$ ⟶ $4(1) + 3(-1) = 4 - 3 = 1$ ✓

→ step 4 → $x = -1,\ y = 1 - 2(-1) = 1 + 2 = 3$ ⟶ $11(-1) + 4(3) = -11 + 12 = 1$ ✓

→ Step 5 → $x = 3,\ y = -1 - 1(3) = -1 - 3 = -4$ ⟶ $15(3) + 11(-4) = 45 - 44 = 1$ ✓

→ Step 6 → $x = -4,\ y = 3 - 3(-4) = 3 + 12 = 15$ ⟶ $56(-4) + 15(15) = -224 + 225 = \boxed{1}$ ✓

Satisfies Equation $ax + by = d$ at every level of recursion.

* Extended form of Euclid's algorithm:

The Extended form of Euclid's algorithm is used to Compute the integer co-efficients 'x' & 'y' such that

$$\boxed{d = \gcd(a,b) = ax+by}$$

where 'x' & 'y' may be zero or negative.

→ The algorithm takes a pair of non-negative integer as input & returns a triple of the form: (d, x, y) that satisfies the Equation:

$$d = ax+by$$

* Extended-Euclid (a,b)

1. if $b == 0$
2. return $(a, 1, 0)$
3. Else (d', x', y') = Extended-Euclid $(b, a \bmod b)$
4. $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
5. return (d, x, y)

→ If in the above algorithm '$b==0$' then the algorithm returns not only '$d=a$' but also the co-efficients '$x=1$' & '$y=0$' (∵ initially conditions). retains the value "$d=a$" in Every step by changing the value of $x = y'$ & $y = x' - \lfloor a/b \rfloor y'$.

→ Lets see an Example. to Compute the Values (d, x, y) that the Call Extended-Euclid (99, 78)

→ $a=99$ $b=78$

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

— Given $(d', x', y') = (9, 1, 0) = (3, 1, 9)$ $\because a = 3$

Step 1: $x' = 1$, $y' = 0$ $\lfloor 9/b \rfloor = 2$

$y = x' - \lfloor 9/b \rfloor y'$

$= 1 - 2(0) = 1.$ $\therefore (d, x, y) = (3, 0, 1)$

Step 2: $x' = 0$, $y' = 1$, $\lfloor 9/b \rfloor = 2$

$y = x' - \lfloor 9/b \rfloor y'$

$= 0 - 2(1)$

$y = -2$ $\therefore (d, x, y) = (3, 1, -2)$

Step 3: $x' = 1$, $y = -2$, $\lfloor 9/b \rfloor = 1$

$y = x' - \lfloor 9/b \rfloor y'$

$= 1 - 1(2)$

$= 3$ $\therefore (d, x, y) = (3, -2, 3)$

Step 4: $x' = -2$, $y = 3$, $\lfloor 9/b \rfloor = 3$

$y = x' - \lfloor 9/b \rfloor y'$

$= -2 - 3(-3)$

$y = -11$ $\therefore (d, x, y) = (3, 3, -11)$

Step 5: $x' = 3$, $y' = 11$, $\lfloor 9/b \rfloor = 1$

$y = x' - \lfloor 9/b \rfloor y'$

$= 3 - 1(-11)$

$= 3 + 11$

$y = 14$ $\therefore (d, x, y) = (3, -11, 14)$

Substituting the Value of co-efficient in the foll eqn we get:

$x = -11$, $y = 14$ $d = ax + by$

$d = 99(-11) + 78(14)$

$\boxed{d = 3}$ // Hence proved that values of x & y are true as value of $d = 3$.

→ Compute the Values (d, x, y) for Extended-Euclid $(221, 81)$ 7

→ $a = 221$ $b = 81$

a	b	$\lfloor a/b \rfloor$	d	x	y
221	81	2	1	11	-30
81	59	1	1	-8	11
59	22	2	1	3	-8
22	15	1	1	-2	3
15	7	2	1	1	-2
7	1	7	1	0	1
1	0	–	1	1	0

→ Step 1: $x' = 1,\ y' = 0,\ \&\ \lfloor a/b \rfloor = 7$

$$y = x' - \lfloor a/b \rfloor y'$$
$$= 1 - 0(7)$$
$$y = 1 \qquad \therefore (d, x, y) = (1, 0, 1)$$

Step 2: $x' = 0,\ y' = 1,\ \lfloor a/b \rfloor = 2$

$$y = x' - \lfloor a/b \rfloor y'$$
$$= 0 - 2(1)$$
$$y = -2 \qquad \therefore (d, x, y) = (1, 1, -2)$$

Step 3: $x' = 1,\ y' = -2,\ \lfloor a/b \rfloor = 1$

$$y = x' - \lfloor a/b \rfloor y'$$
$$= 1 - 1(-2)$$
$$y = 3 \qquad \therefore (d, x, y) = (1, -2, 3)$$

Step 5: $x' = 3,\ y' = -8,\ \lfloor a/b \rfloor = 1$

$$= 3 - 1(-8)$$
$$y = 11 \qquad \therefore (d, x, y) = (1, -8, 11)$$

Step 4 on next Page.

Step ~~4~~: ~~$x=3$~~, $x' = -2$, $y = 3$, $\lfloor a/b \rfloor = 2$

$$y = x' - \lfloor a/b \rfloor y'$$
$$= -2 - 3(2)$$
$$y = -8 \quad \therefore (d, x, y) = (1, 3, -8)$$

Step 6: $x' = -8$, $y' = 11$, $\lfloor a/b \rfloor = 2$

$$= -8 - 2(11)$$
$$y = -30 \quad \therefore (d, x, y) = (1, 11, 0)$$

Substitute the Values of Co-efficients i.e $x = 11$ & $y = -30$ in

$$d = ax + by$$
$$d = 221(11) + 81(-30)$$
$$\boxed{d = 1}$$

Home Work: Compute the Values (d, x, y) that the Call Extended-Euclid $(899, 493)$ returns.

* Solving Modular Linear Equation:
Consider the problem of finding solution to the Equation
$$ax \equiv b \pmod{n}$$
where $a > 0$ & $n > 0$. This problem has several application; for Eg. we shall use it as a part of procedure for finding Keys in RSA-public Key Cryptosystem & in network Security.
→ To Solve the Equation $ax \equiv b \pmod{n}$, the following algorithm prints all solutions to the Equation.
The inputs a & n are arbitrary positive integers & b is an arbitrary integer.

→ Algorithm for Solving Modular Linear Equation - $ax \equiv b \pmod{n}$

* Modular - Linear - Equation Solver (a,b,n)

1. $(d, x', y') = $ Extended Euclid (a, n)
2. if $d \mid b$
3. $x_0 = x'(b/d) \bmod n$
4. for $i=0$ to $d-1$
5. print $(x_0 + i(n/d)) \bmod n$
6. Else print "No Solutions"

→ find all Solutions to the Equation $14x \equiv 30 \pmod{100}$

$a=14,\ b=30,\ n=100$

Extended Euclid $(a,n) = $ Extended - Euclid $(14, 100)$

a	n	$\lfloor a/b \rfloor$	d	x	y
14	100	0	2	-7	1
100	14	7	2	1	-7
14	2	7	2	0	1
2	0	–	2	1	0

Step 1 → $x^a = 1,\ y^b = 0\ \ \lfloor a/b \rfloor = -$

Step 2 → $x^1 = 1,\ y^1 = 0,\ y = 1 - 0(-7) = 1. \quad \therefore (d,x,y) = (2,0,1).$

Step 3 → $y = 0 - 1(7)$

$y = -7 \quad \therefore (d,x,y) = (2,1,-7)$

step 4 → $y = 1 - (-7)(0)$

$y = 1 \quad \therefore (d,x,y) = (2,-7,1)$

If b/d " Solutions are present "

$b = 30,\ d = 2$

$\therefore b/d = \frac{30}{2} = 15$ // $\therefore$ Solutions are present for Equation

→ Compute $x_0 = x'(b/d) \bmod n$

$x' = 7 \quad (b/d) = 15 \quad n = 100$

$x_0 = -7(15) \bmod 100$

$= -105 \bmod 100$

$\boxed{x_0 95}$

(∵ $-b \bmod a$ = add a to b until Value mod n becomes 0].

$\therefore$ ~~100~~ $100 - 5 = 95$

$\rightarrow 105 = 100 + \boxed{5}$ ✓

$100 - 5 \quad 95$

$\therefore 105 + 95 = 200 \bmod 100 = \underline{0}$

→ for $i = 0$ to $d - 1$.

print $(x_0 + i(n/d) \bmod n \qquad (100/2) = 50$ [n/d]

$= 95 + 0(50) \bmod 100$

$= \underline{95}$

$x_0 = 95,\ i = 1 \quad n/d = 50,\ n = 100$

$x_0 + i(n/d) \bmod n$

$= 95 + 1(50) \bmod 100$

$= 145 \bmod 100$

45

$\therefore$ possible Solution of x is 95, 45 //

Ex: $12x \equiv 6 (\bmod 15)$, $a = 12,\ b = 6,\ n = 15$.

a	b	$\lfloor a/b \rfloor$	d	x	y	
12	15	0	3	-1	1	$y = 1 - 0(-1) = 1$
15	12	1	3	1	-1	→ $y = 0 - (1)(1) = -1$
12	3	4	3	0	1	→ $y = 1 - (4)(0) = 1$
GCD → 3	0	—	3	1	0	

→ $d = 3,\ b = 6,\ d/b \Rightarrow 3/6$ ✓ 6 is divisible by 3

$x' = -1.$

$x_0 = -1\,(6/3) \bmod 15$

$= -2 \bmod 15$ $\quad (15 - \cancel{0}2 = 13)$

$(13 + 2 = 15 \bmod 15 = 0)$

$\boxed{x_0 = 13}$

→ for $i = 0$ to $(d-1)$ $(3-1) = 2$. $i = (0, 1, 2)$ - 3 iterations.

→ $(x_0 + i\,(n/d)) \bmod 15$

$i = 0,$

$x(13 + 0(15/3)) \bmod 15$

$13 + 0 \bmod 15$

$= 13$ //

$i = 1,$ $(13 + 1\,(15/3)) \bmod 15$

$= 13 + 1(5) \bmod 15$

$= 18 \bmod 15 = 3$ //

$i = 2,$ $x(13 + 2(5)) \bmod 15$

$23 \bmod 15 = 8$ //

∴, when $13 \times 12 \equiv 6 \pmod{15}$ Satisfies the Equation.

&

$3 \times 12 \equiv 6 \pmod{15}$ "

&

$8 \times 12 \equiv 6 \pmod{15}$ "

H.W → $35x \equiv 10 \pmod{50}$.

[illegible]

* Chinese Remainder Theorem:

Around A.D 100, the Chinese mathematician Sun-Tse solved the problem of finding those integers x that leave remainders 2, 3 & 2 when divided with 3, 5 & 7 respectively. One such solution is $x = 23$. (all solⁿ are of form $23 + 105k$ for arbitrary integer k)

→ The "Chinese remainder theorem" provides a correspondence between a system of equations modulo a set of pairwise relatively prime moduli & an equation modulo of their product.

→ Let $n_1, n_2, n_3 \ldots n_k$ are pairwise relatively prime integers.

→ Consider the correspondence

$$a = a_1 \bmod n_1$$

$$a = a_2 \bmod n_2$$

$$\vdots$$

$$a = a_k \bmod n_k$$

then there exists a solution "a" which is a unique integer.

→ Computation of "M" is done by

$$\boxed{M = n_1 \times n_2 \times n_3 \times \cdots \cdots n_k}$$

for $i = 1, 2, 3, \ldots k$

& $\boxed{m_i = \frac{M}{n_i}}$

Thus m_i is the product of all n's other than n_i.

→ Compute the inverse modulo

$\boxed{C_i = m_i^{-1} \bmod n_i}$ for $i = 1, 2, 3, \ldots k$

Finally we can compute $\underline{a}$ as a function of $a_1, a_2, \ldots a_k$ as shown

P.T.O

$$\boxed{a \equiv (a_1 c_1 m_1 + a_2 c_2 m_2 + \cdots \quad a_k c_k m_k) \bmod M}$$

Therefore for Each i, we have

$a \equiv a_i c_i m_i \bmod M$

$a \equiv a_i m_i (m_i^{-1} \bmod n_i) \bmod M \quad \because c_i = \text{inverse Modulo}$

$\boxed{a \equiv a_i \bmod n}$ //.

* find all Solution to Equation $x \equiv 4 \pmod 5$ & $x \equiv 5 \pmod{11}$

→. $x \equiv 4 \pmod 5$
$x \equiv 5 \pmod{11}$

$a_1 = 4$, $a_2 = 5$ $\quad n_1 = 5$, $n_2 = 11$

Compute $M = n_1 \times n_2 = 5 \times 11$, $\boxed{M = 55}$.

$m_1 = M/n_1 = \frac{55}{5} = 11$ //.

$m_2 = M/n_2 = 55/11 = 5$ //

Compute Modulo inverse c_i

$c_1 = m_1^{-1} \bmod n_1 = m_1 \times c_1 \equiv 1 \bmod n_1$

$11 \times c_1 \equiv 1 \bmod 5$

$\boxed{c_1 = 1}$.

$c_2 = m_2^{-1} \bmod n_2$

$m_2 \times c_2 \equiv 1 \bmod n_2$

$5 \times c_2 \equiv 1 \bmod 11$

$\boxed{c_2 = 9}$

→ Finally Compute a

$$a = a_1 c_1 m_1 + a_2 c_2 m_2 \bmod M$$

$$= 4 \times 1 \times 11 + 5 \times 9 \times 5 \bmod 55$$

$$= 44 + 225 \bmod 55$$

$$= 269 \bmod 55$$

$$\boxed{a = 49}$$ //

* find all integers x that leave remainders 1, 2, 3 when divided by 9, 8, 7 respectively

⇒ $x \equiv 1 \pmod 9$ $\quad a_1 = 1$ $\quad n_1 = 9$ $\quad M = n_1 \times n_2 \times n_3$

$x \equiv 2 \pmod 8$ $\quad a_2 = 2$ $\quad n_2 = 8$ $\quad = 9 \times 8 \times 7$

$x \equiv 3 \pmod 7$ $\quad a_3 = 3$ $\quad n_3 = 7$ $\quad \boxed{M = 504}$

→ Compute m_i

$$m_1 = \frac{M}{n_1} = \frac{504}{9} = 56$$

$$m_2 = \frac{M}{n_2} = \frac{504}{8} = 63$$

$$m_3 = \frac{M}{n_3} = \frac{504}{7} = 72$$

$\boxed{m_1 = 56}$, $\boxed{m_2 = 63}$, $\boxed{m_3 = 72}$

→ Compute Modulo inverse (c_i)

$$c_i = m_i^{-1} \bmod n_i$$

* $C_1 = m_1^{-1} \bmod n_1$

$\Rightarrow m_1 \times C_1 \equiv 1 \bmod n_1$

$56 \times C_1 \equiv 1 \bmod 9$ $\quad (56 \bmod 9) = 2$

$2 \times \underbrace{C_1}_{?} \equiv 1 \bmod 9$

$2 \times 5 \equiv 1 \bmod 9 = 10 \equiv 1 \bmod 9 \equiv 2 \times 45 \equiv 5 \bmod 9$

$\therefore \boxed{C_1 = 5}$ //

* $C_2 = m_2^{-1} \bmod n_2$

$m_2 \times C_2 \equiv 1 \bmod n_2$

$63 \times C_2 \equiv 1 \bmod 8$

$7 \times C_2 \equiv 1 \bmod 8$ $\quad \because (63 \bmod 8 = 7)$

$\boxed{C_2 = 7}$ // $\quad 7 \times 7 C_2 \equiv 7 \bmod 8$

* $C_3 = m_3^{-1} \bmod n_3$

$m_3 \times C_3 \equiv 1 \bmod n_2$

$72 \times C_3 \equiv 1 \bmod 7$ $\quad (72 \bmod 7) = 2$

$2 \times C_3 \equiv 1 \bmod 7 = 2 \times 4 C_3 \equiv 4 \bmod 7$

$\boxed{C_3 = 4}$ //

Finally Compute 'a'

$a \equiv a_1 C_1 m_1 + a_2 m_2 C_2 + a_3 C_3 m_3 \bmod M$

$= 1 \times 5 \times 56 + 2 \times 63 \times 7 + 3 \times 72 \times 4 \bmod 504$

$= 2026 \bmod 504$

$\boxed{a = 10}$ is a unique sol: for all given Equation

* Powers of an Element (MODULAR_EXPONENTIATION).

A frequently occurring operation in number-theoretic computations is raising one number to a power modulo another number also known as "Modular-Exponentiation".

$$\boxed{a^b \bmod n}$$

where a & b are non-negative integers & n is a positive integer.

"Modular-Exponentiation" is an essential operation in many primality testing routine & in RSA Cryptosystems.

* Modular-Exponentiation(a, b, n)

```
c = 0
d = 1
let (bk, bk-1 ... b0) be the binary representation of b.
for (i = k down to 0)
      c = 2c
      d = (d.d) mod n   (repeated squaring)
   if bi = = 1
      c = c+1
     d = (d.a) mod n
return d.
```

* A Box contains Gold coins if the coins are Equally divided among three friends, two coins are left over. If the coins are Equall divided among five friends, three coins are left over. If the coins are Equall divided among seven friends, two coins are left over. Find the number of coins present in Box.?

H.M

58

→ Initially the value of $c=0$ & $d=1$ & let $\{b_{k-1}, b_k \ldots b_0\}$ be the binary representation of b.

→ Two important procedures to be followed are

* if in binary representation $b_i == 0$ then

$$c = 2 \times c$$

$$d = d \times d \bmod n$$

will give the value of c & d.

* if in binary representation $b_i == 1$ then

$$c = 2 \times c$$

$$d = d \times d \bmod n$$

Substitute the calculated 'c' & 'd' values in

$$c = c + 1.$$

$$d = d \cdot a \bmod n$$

to get the value of 'c' & 'd' respectively.

→ Solve the following Modular Exponentiation

$$7^{560} \bmod 561$$

Sol: The given Eqⁿ $7^{560} \bmod 561$ is of the form $a^b \bmod n$

$\therefore$ $a=7$, $b=560$ and $n=561$

Let us represent $b=560$ in binary form first.

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298 ~~166~~	166	67	$\boxed{1}$

2	560
2	280 - 0
2	140 - 0
2	70 - 0
2	35 - 0
2	17 - 1
2	8 - 1
2	4 - 0
2	2 - 0
	1 - 0

* At $i=9$, $b_i==1$, $C=0$, $d=1$

$C=2\times C=2\times 0=0$

$d=d^2 \bmod n = 1^2 \bmod 561 = 1$

& $C=C+1 = 0+1$

$\boxed{C=1}$

$d=d\cdot a \bmod n$

$=1\cdot 7 \bmod 561$

$=\boxed{d=7}$

* At $i=8$, $b_i==0$, $C=1$, $d=7$

20.

$C=2\times C=2\times 1=2$

$\boxed{C=2}$

$d=d^2 \bmod n$

$=7^2 \bmod 561$

$\boxed{d=49}$

* At $i=7$,

$b_i==0$, $C=2$, $d=49$

$C=2\times C=2\times 2=4$

$\boxed{C=4}$

$d=d^2 \bmod n$

$=49^2 \bmod 561$

$\boxed{d=157}$

* At $i=6$,

$b_i==0$, $C=4$, $d=157$

$C=2\times C=2\times 4$

$\boxed{C=8}$

$d=d^2 \bmod n$

$=157^2 \bmod n$

$\boxed{d=526}$

* At $i=5$,

$b_i==1$, $C=8$, $d=526$

$C=2\times C=2\times 8=16$, $C+1=17$

$\boxed{C=17}$

$d=d^2 \bmod n = 526^2 \bmod 561$

$=103$

$d=d\cdot a \bmod 561$

$=103\times 7 \bmod 561$

$\boxed{d=160}$

* At $i=4$,

$b_i==1$, $C=17$, $d=160$

$C=2\times C=2\times 17=34$

$C=C+1=35$

$\boxed{C=35}$

$d=d^2 \bmod n$

$=160^2 \bmod n$

$d=355$

$d=d\cdot a \bmod n$

$=355\cdot 7 \bmod 561$

$\boxed{d=241}$

Apply Modular Exponentiation (a, u, n).

$\therefore$ MOD_Exp $(2, 221, 443)$

$2^{221} \bmod 443$

$\boxed{x_0 = 442}$

i	7	6	5	4	3	2	1	0
b	1	1	0	1	1	1	0	1
c	1	3	6	13	27	55	110	221
a	2	8	64	218	246	93	232	442

for $i = 1$ to $t(1)$

$X_1 = X_0^2 \bmod n$

$= 442^2 \bmod 443$

$\boxed{X_1 = 1}$.

Sequence of $x = \{442, 1\}$.

$\therefore x_1 = 1$, & $x_0 = 442 = n-1 = 443-1$

$\therefore$ The given $n = 443$ is a prime no.

Ex. $n = 341$.

* Number-theoretic Algorithms: UNIT-3

Veena V. Kaugrekar
Asst Professor
Dept of CSE
KLSGIT, Belagavi

→ Modular Arithmetic → (for Complex Cryptographic algorithms)

* finite group → A group $(S, \oplus)$ is a set & S together with a binary Operation $\oplus$ defined on S for which the foll properties holds.

* Closure → for all $a, b \in S$, we have $a \oplus b \in S$
* Identity → there Exists an Element $e \in S$ called the identity of group Such that $e \oplus a = a \oplus e = a$

If a Group $(S, \oplus)$ Satisfies the Commutative law $a \oplus b = b \oplus a$ for all $a, b \in S$ then it is an* abelian group

We Can form finite abelian group by using addition & Multiplication modulo n where n is a +ve integer

→ Addition group Modulo $(Z_n, +_n)$ & Multiplicative group Modulo $(Z_n^*, \cdot_n)$.

→ RSA Cryptosystem :- The working procedure of RSA Algorithm is as shown below.

1. Select any two large prime numbers p & q such that $p \neq q$.

2. Compute $n = p \times q$

3. Select a small odd integer e such that it is relatively prime to $\phi(n)$.

$$\phi(n) = (p-1)(q-1)$$

$$GCD(e, \phi(n)) = 1 \quad de \equiv 1 \pmod{\phi(n)}$$

4. Compute d as multiplicative inverse of e modulo $\phi(n)$

$$\boxed{e \times d \equiv 1 \pmod{\phi(n)}}$$

5. publish the pair of $P = (e, n)$ as public keys.

6. Keep secret key pair as $S = (d, n)$ as secret or private keys

* To Transform a Message M to Cipher text

$$\boxed{P(m) = m^e \bmod n}$$

* To Transform a Ciphertext to Original Message i.e Decyphering process.

$$\boxed{S(c) = c^d \bmod n}$$

→ Consider an RSA Key set with $P=11, q=29, n=319$ & $e=3$ what value of d should be secret key? What is Encrypted value of Message $M=100$?

⇒ $P=11,\ q=29,\ M=100.$

Compute $n = P \times q = 11 \times 29$

$$\boxed{n = 319}$$

→ Compute $\phi(n) = (P-1)(q-1) = (10)(28)$

$$\boxed{\phi(n) = 280}$$

Select 'e' such that, it is relative prime with $\phi(n)$.

$GCD(e, \phi(n)) = 1$

$GCD(e, 280) = 1$

$\boxed{e=3}$ $\quad \therefore GCD(3, 280) = 1.$

→ Compute 'd' as Multiplicative inverse of e modulo $\phi(n)$

$e \times d \equiv 1 \pmod{\phi(n)}$

$3 \times d \equiv 1 \pmod{280}$

$3 \times 187 \equiv 1 \pmod{280}$

$\boxed{d = 187}$ – big no..

How to solve for such big numbers.

Use. Extended Euclid & Modular linear Equation Algorithms.

$3d \equiv 1 \pmod{280}$

$ax \equiv b \pmod{n}$

$a = 3,\ b = 1,\ n = 280$

Extended-Euclid (a, n)

$\rightarrow (3, 280)$

a	$n(b)$	$\lfloor a/b \rfloor$	d	x	y
3	280	0	1	-93	1.
280	3	93	1	1	-93
3	1	3	1	0	1
1	0	-	1	1	0

$x' - 3(0) = 1 - 3(0) = 1$

$0 - 93(1) = -93$

$1 - (0)(-93) = 1$

– Modular-Linear Equation.

$d = 1,\ b = 1.\ d/b$ yes, $x' = -93$

$x_0 = -93(1/1) \bmod 280$

$= -93 \bmod 280$

$\underline{x_0 = 187 \bmod 280 = 187}$.

$i = 0$ to $1 - 1 = 0$

print $(187 + 0(280/1)) \bmod 280$

$187 \bmod 280 = \underline{187}$.

$\therefore$ $\boxed{d \rightarrow \text{Secret Key} = 187}$

→ Public Key $(e,n) = (3,319)$ } Publishing Public & Secret (Private) Keys.
Secret Keys $(d,n) = (187,319)$

* Encryption → Creating Cipher.

$$p(m) = m^e \bmod n$$
$$= 100^3 \bmod 319$$

$$\boxed{C = 254}.$$

* Decryption → Deciphering → Refer Class notes.

$$s(c) = c^d \bmod n$$
$$= 254^{187} \bmod 319 \rightarrow a^b \bmod n.$$

$\boxed{M = 100}$ //.

Bigger Number. So use Modular Exponentiation.

$b=187,\ a=254,\ n=319.$

i	8	7	6	5	4	3	2	1	0
b	1	0	0	1	1	1	0	1	1
c	1	2	4	9	19	39	78	157	315
d	254	78	210 ~~23~~	67	$\boxed{100}$	0	0	0	

initially $c=0$, $d=1$

2	187
2	93 − 1
2	46 − 1
2	23 − 0
2	11 − 1
2	5 − 1
2	4 − 1
2	2 − 0.
	1 − 0

~~* when you get d = value as 0 then Consider previous d value as the answer. In this Example it is $\boxed{100}$~~ $= \boxed{M}$ ✓

→ Primality testing: Primality testing is a part of number theoretic algorithms that deals with the problem of finding large prime numbers.

* Pseudoprimality testing (* Fermate theorem)

if 'p' is a prime number then

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{for} \ \forall \ a \in Z_p^+ \ \cdots \ (1)$$

Fermate theorem applies to every element in Z_p except 0. Since $0 \notin Z_p^+$.

→ Fermate theorem implies that if 'p' is prime then 'p' satisfies Equation (1) for every a. if 'p' does not satisfy Equation (1) then 'p' is certainly composite.

Pseudo Prime (n)

1. if Modular. Exponentiation $(2, n-1, n) \not\equiv 1 \pmod{n}$
2. return "Composite" // Definitely not prime.
3. Else return 'prime' // we hope.

Ex $n = 561$ — Carmichael number. — deceiving us as prime nos. which are not in actual.

pseudoprime (n)

= Modular-Exponentiation $(2, n-1, n)$

= Modular. Exponentiation $(2, 560, 561)$.

= Modular. Exponentiation

Ex: of RSA.

→. $p=3,\ q=11,\ m=2\ ,\ n=p\times q=3\times 11=33$

$\phi(n)=(p-1)(q-1)=(2)(10)=\phi(n)=20$

Select Small odd integer 'e' Such that $GCD(e,\phi)=1$

$GCD(e,20)=1$

$CD(3,20)=1$

$\boxed{e=3}$.

'd' → ?

$e\times d\equiv 1(\mathrm{mod}\ \phi(n))$

$3\times d\equiv 1(\mathrm{mod}\ 20)$

$3\times 7\equiv 1(\mathrm{mod}\ 20)$

$\boxed{d=7}$.

Public Key $(e,n)=(3,33)$

(Secret) Private Key $(d,n)=\cancel{7}(7,33)$

* Encryption → $P(m)=m^e \bmod n$

$=2^3 \bmod 33$

$\boxed{C=8}$.

* Decryption → $S(m)=c^d \bmod n$

$=8^7 \bmod 33$

$\boxed{M=2}$ //.

$\therefore a^b \bmod n$

$2^{560} \bmod 561 = 1$. ← Solved

$\therefore n = 561$ is a prime no. as per pseudoprime but in real 561 is a composite number. To Overcome this drawback "Miller-Rabin Primality test" was introduced.

* Miller Rabin Radomized primality test :- The Miller-Rabin primality test is an modification over pseudoprime but such as:
* It tries randomly choosen base value 'a' instead of just one base value (i.e $a=2$).
* While Computing Each Modular-Exponentiation, it looks for non-trivial Square root of '1' modulo n. if it finds one: it stops & return Composite.

Miller-Rabin (n, s)

1. for $j = 1$ to s
2. a = Random $(1, n-1)$
3. if witness (a, n)
4. return Composite // definitely.
5. return prime // we hope.

Witness (a, n)

1. let t & u be such that $t \geq 1$, u is odd, & $\boxed{n-1 = 2^t \cdot u}$
2. $x_0 =$ Modular Exponentiation (a, u, n)
3. for $i = 1$ to t
4. $x_i = x_{i-1}^2 \bmod n$
5. if $x_i == 1$ & $x_{i-1} \neq 1$ & $x_{i-1} \neq n-1$
6. return True.
7. if $x_t \neq 1$
8. return True.
9. Else return False.

Solved in class.

for. Ex. $n = 561 \to$ we get solved sequence as.

$x = \{241, 298, 166, 67, 1\}$.

$\therefore x_4 = 1$ & $x_3 = 67 \neq n-1$ (560) — Composite.

is a witness to the compositeness of n.

$\therefore a = 7$. is a witness to the compositeness of n.

Ex: $n = 443$, $n-1 = 442$

choose $a \to (1, 442)$

$\boxed{a = 2}$

$\to$. $n-1 \to 2^t \cdot u$

$\frac{442}{2^1} = 221$, $\frac{442}{2^2} = 110.5$ $\therefore (442) = 2^t \cdot u = 2^1 \cdot 221$

$\therefore \boxed{t = 1}$ $\boxed{u = 221}$.

H.W $\to n = 341$

Ex. $n = 443$

$n = 443$, $n-1 = 442$

Choose 'a' random integer $(1, 442)$

$\boxed{a = 2}$.

→ represent $n-1$ in terms of $2^t \cdot u$

$\therefore$ t & u $= \frac{442}{2^1} = 221$ // $\frac{442}{2^2} = 110.5$ ✗

$\therefore$ $442 = 2^t \cdot u = 2^1 \cdot 221$ $\boxed{t = 1}$ $\boxed{u = 221}$

→ Apply Modular-Exponentiation (a, u, n)

$\therefore$ Mod_Exp $(2, 221, 443)$

$2^{221} \bmod 443$

$\boxed{x_0 = 442}$

i	7	6	5	4	3	2	1	0
bi	1	1	0	1	1	1	0	1
c	1	3	6	13	27	55	110	221
d	2	8	64	218	246	93	232	442

for $i = 1$ to $t(1)$

$x_1 = x_0^2 \bmod n$

$= 442^2 \bmod 443$

$\boxed{x_1 = 1}$ //

The Sequence of x Values $= \{442, 1\}$.

Check →. $\therefore$, $x_1 = 1$ & $x_0 = 442 = n-1$. → Condition Satisfies for no to be prime

$\therefore$ The Given $n = 443$ is a prime //.

* At $i=3$,

$b_i == 0$, $c=35$, $d=241$

$c = 2\times c = 2\times 35$

$\boxed{c=70}$

$d = d^2 \bmod n$

$= 241^2 \bmod n$

$\boxed{d=298}$

* At $i=2$,

$b_i == 0$, $c=70$, $d=298$

$c = 2\times c = 2\times 70 = 140$

$\boxed{c=140}$

$d = d^2 \bmod n$

$298^2 \bmod 561$

$\boxed{d=166}$

* At $i=1$

$b_i == 0$, $c=140$, $d=166$

$c = 2\times c = 2\times 140$

$\boxed{c=280}$

$d = d^2 \bmod n$

$= 166^2 \bmod 561$

$\boxed{d=67}$

* At $i=0$

$b_i == 0$ $c=280$ $d=67$

$c = 2\times c = 2\times 280$

$\boxed{c=560}$

$d = d^2 \bmod n$

$= 67^2 \bmod 561$

$\boxed{d=1}$

$\therefore 7^{560} \bmod 561 = 1$.

→ Solve $28^{10} \bmod 47$ using Modular Exponentiation

i	3	2	1	0
b_i	1	0	1	0
c	1	2	5	10
d	28	32	2	4

~~for i=1 to t(>)~~

H.W → $2^{85} \bmod 341$. → Check for number 341 whether it is prime or not