2) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

**Ans:**

The Miller-Rabin test is a **probabilistic Algorithm**. It is typically used to test a large number for primality.

If it is given an odd number n that is not prime and a randomly chosen integer, a with 1 < a < n - 1, the probability that TEST will return MAY PRIME (i.e., fail to detect that n is not prime) is less than 1/4. Thus, if t different values of a are chosen, the probability that all of them will pass TEST (return MAY PRIME) for n is less than (1/4)t . For example, for t = 10, the probability that a non-prime number will pass all ten tests is less than $10^{-6}$ . Thus, for a sufficiently large value of t , we can be confident that n is prime if Miller's test always returns MAY PRIME. This gives us a basis for determining whether an odd integer n is prime with a reasonable degree of confidence. The procedure is as follows: Repeatedly invoke TEST (n) using randomly chosen values for a. If, at any point, TEST returns composite, then n is determined to be non-prime. If TEST continues to return inconclusive for t tests, then for a sufficiently large value of t, assume that n is prime.

**No Known method of efficiently proving the primality of very large numbers**. **All of the algorithms in use, including the most popular (Miller– Rabin), produced a probabilistic result**. However the algorithm, known as the AKS algorithm, does not appear to be as efficient as the Miller–Rabin algorithm. Thus far, it has not supplanted this older, probabilistic technique.

**Algorithm:**

**Miller_Rabin_Test** $(n, a)$ // $n$ is the number; $a$ is the base.
{
Find $m$ and $k$ such that $n - 1 = m \times 2^k$
$T = a^m \bmod n$
if $(T = \pm 1 \bmod n)$ return ***"a prime"*** **// May be**
for $(i = 1$ to $k)$
{
$T \leftarrow T^2 \bmod n$
if $(T = +1)$ return ***"a composite"***
if $(T = -1)$ return ***"a prime"*** **// May be**
}
return ***"a composite"*** **Time Complexity** $O(k(\log n)^3)$
}

10

**In short:**

The algorithm takes a candidate integer n as input and returns the result "composite" if n is definitely not a prime, and the result "inconclusive" if n may or may not be a prime. If the algorithm is repeatedly applied to a number and repeatedly returns inconclusive, then the probability that the number is actually prime increases with each inconclusive test. The probability required to accept a number as prime can be set as close to 1.0 as desired by increasing the number of tests made

3. Show that if n is an odd composite integer, then the Miller-Rabin test will return inconclusive for a = 1 and a = (n-1).

**Miller-Rabin test Algorithm**

**TEST (n)**
{
STEP-1: Find integers k, q, with k > 0, q odd, so that (n − 1 = 2k q);
STEP-2: Select a random integer a, 1 < a < n - 1;
STEP-3: if $a^q$ mod n = 1 then return("inconclusive");
STEP-4: for j = 0 to k - 1 do
STEP-5: if a2j qmod n = n - 1 then return("inconclusive");
STEP-6: return("composite");
}

**Now for the given question:**

First considering **a = 1**

In step 3 of TEST(n), the test is if $1^q$ mod n = 1 then return("inconclusive").

This clearly **returns "inconclusive."**

Now consider **a = n – 1.**

In step 5 of TEST(n),
for j = 0,
the test is if $(n – 1)^q$ mod n = n – 1

then **return("inconclusive")**.

This condition is met by inspection.

4. If n is composite and passes the Miller-Rabin test for the base a, then n is called a strong pseudoprime to the base a. Show that 2047 is a strong pseudoprime to the base 2

Given n = 2047

**TEST (2047)**
{
STEP-1: Find integers k, q, with k > 0, q odd, so that (n − 1 = 2k q);
STEP-2: Select a random integer a, 1 < a < n - 1;
STEP-3: if $a^q$ mod n = 1 then return("inconclusive");
STEP-4: for j = 0 to k - 1 do
STEP-5: if a2j qmod n = n - 1 then return("inconclusive");
STEP-6: return("composite");
}

In Step 1 of TEST(2047),
we set k = 1 and q = 1023,
because (2047 – 1) = (21 )(1023).

In Step 2

we select a = 2 as the base.

In Step 3

we have a q mod n = 21023 mod 2047
= (211) 93 mod 2047
= (2048)93 mod 2047
= 1

and so the **test is passed**.

5. Using Fermat's theorem,

a) Find $3^{201}$ mod 11.

According to Fermat's Theorem:

If p is prime and a is a positive Integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod p$$

Given,

p is "11" & a = 3

$$\Rightarrow 3^{10} \equiv 1 \pmod{11}$$

$$3^{201} = (3^{20})^{10} \times 3$$

$$= 3 \pmod{11}$$ //

b) Find a number n between 0 and 72 with n congruent to $9^{794}$ modulo 73.

$$9^{794} \equiv (9^{72})^{11} \cdot 9^2$$

$$\equiv 1^{11} \cdot 81$$

$$\equiv 81$$

$$\equiv 8 \pmod{73}$$ //

Therefore n is 8

c) Find a number x between 0 and 28 with x85 congruent to 6 modulo 29. (You should not need to use any brute force searching.)

By Fermat's Little Theorem,

Since '29' is a prime, that

if $x \not\equiv 0 \pmod{29}$, then

$x^{28} \equiv 1 \pmod{29}$

Clearly $x \equiv 0 \pmod{29}$ is not a solution

as $0^{86} \equiv 0 \pmod{29}$

we will rewrite the left side of the congruence given in the following way

$x^{86} = (x^{28})^3 . x^2 \equiv 1^3 . x^2 = x^2$

$\therefore x^2 \equiv 6 \pmod{29}$

So, from the above, it is clear that

$x \equiv 8 \pmod{29}$

(or)

$x \equiv 21 \pmod{29}$ //

Therefore x can be 8 or 21

6) Using Euler's Theorem

a) Find a number n between 0 and 9 such that n is congruent to $7^{1000}$ modulo 10.

We know that $\phi(10) = 4$

Therefore $7^4 \equiv 1 \pmod{10}$

By, Euclean's theorem

$\therefore 7^{1000} = (7^4)^{250} \equiv 1^{250} \pmod{10}$

$\therefore$ The last digit is 1.

$\therefore$ The "n" is "1".

b) Find a number x between 0 and 28 with x85 congruent to 6 modulo 35. (You should not need to use any brute force searching.)

Given

'x' need to be in b/w 0 & 28.

with $x^{85} \equiv 6$ modulo 35.

Using Euler's Theorem :

$x^{85} = x^{24} \times x^{24} \times x^{24} \times x^{13}$

$= (x^{24})^3 \times x^{13}$

Cancelling $x^{24}$ as we know that

by Euler's theorem $x^{\phi(n)} \equiv 1 \pmod{n}$

$\boxed{\text{let } x = a}$ $\phi(35) = 24$

$a^{24} = 1 \bmod 35$

So, $a^{12} = \pm 1 \bmod (35)$

So, $a^{13} = a^{12} . a = \pm a = 6 \bmod 35$

So $a = \{6, -6\} \bmod 35$.

As $6^2 = 1 \bmod (35)$

$(-6)^{13} = -6 \bmod 35$, so $a = 6 \bmod 35$

So, $a = 6$

Therefore for a) the " n " is 1

And

For b) " x " is 6

7) Determine the following:

a) Φ(41) b) Φ(27) c) Φ(231) d) Φ(440)

Given

a) $\phi(41)$ b) $\phi(27)$ c) $\phi(231)$ d) $\phi(440)$

Now

$\phi(41) = 40$, because 41 is prime

$\phi(27) = \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$

$\phi(231) = \phi(3) \times \phi(7) \times \phi(11) = 2 \times 6 \times 10 = 120$

$\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11) = (2^3 - 2^2) \times 4 \times 10 = 160$

Therefore answers are:

a) 40
b) 18
c) 120
d) 160

8) A box contains gold coins. If the coins are equally divided among six friends, four coins are left over. If the coins are equally divided among five friends, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven friends?

Forming the Equations:

1) coins equally divided among six, four coins are left over.

$$x \equiv 4 \pmod 6$$

2) Coins equally divided among five, three coins are left over.

$$x \equiv 3 \pmod 5$$

This is chinese Reminder Theorem problem.

STEP-1: $M = 6 \times 5 = 30$

STEP-2: $M_1 = \frac{30}{6} = 5$

$M_2 = \frac{30}{5} = 6$

STEP-3: $M_1^{-1} = 5$ & $M_2^{-1} = 1$

STEP-4: $x = (4 \times 5 \times 5 + 3 \times 6 \times 1)$

$= (100 + 18) = 118$

$= 118 \bmod 30$

$= 28$ //

∴ The Number of coins are 28

Now,

dividing '28' coins among '7' friends

$$28 \pmod 7 = 0$$

∴ zero coins are left.

Therefore there are **28 coins** and when they are divided among 7 people **zero coins will be left**.

9) Find the smallest positive integer that is one more than a multiple of 5, 2 more than a multiple of 11 and 3 more than a multiple of 7.

Forming the Equations:

1) One more than a multiple of 5

$$x \equiv 1 \pmod 5$$

2) Two more than a multiple of 11

$$x \equiv 2 \pmod{11}$$

3) Three more than a multiple of 7

$$x \equiv 3 \pmod 7$$

This is Chinese Reminder Theorem problem

STEP-1: $M = 5 \times 11 \times 7 = 385$

STEP-2: $M_1 = \frac{385}{5} = 77$

$M_2 = \frac{385}{11} = 35$

$M_3 = \frac{385}{7} = 55$

STEP-3: $M_1^{-1} = 3$; $M_2^{-1} = 6$ & $M_3^{-1} = 6$

STEP-4: $x = (1 \times 77 \times 3 + 2 \times 35 \times 6 + 3 \times 55 \times$

$= 231 + 420 + 990 = 1,641$

$= 1,641 \bmod 385 = 101$ //

Therefore the **smallest positive integer** which satisfy the above condition is **101**

10) How many primitive roots does 25 have? Find them all.

Primitive roots:

If 'a' is a primitive root of number 'n' then

$$a^{\phi(n)} \equiv 1 \pmod n$$

From the Question 'n = 25'.

$\phi(5.5)$

$\phi(5).\phi(5)$

$(5-1)(5-1)$

$4 \times 4 = 16$

$$a^{16} \equiv 1 \pmod{25}$$

'a' can be 2, 3, 4, 5, 6, ..., 24

But 'a' can only satisfy to

2, 3, 8, 12, 13, 17, 22 & 23

Becouse to this numbers itself it gives the GCD of 1.

Therefore there are **8 primitive roots for 25**. And they are **2, 3, 8, 12, 13, 17, 22, and 23**

11)Perform encryption and decryption using the RSA algorithm, if p = 397; q = 401, e = 343; Plaintext M = "NO". [Coding: A=0, B=1, …, Z=25]

Given $p = 397$ and $q = 401$

$n = p.q = 397 \times 401 = 159197$

$\phi(n) = \phi(p.q) = \phi(p).\phi(q)$

$= 398 \times 400 = 158400$

Given $e = 343$

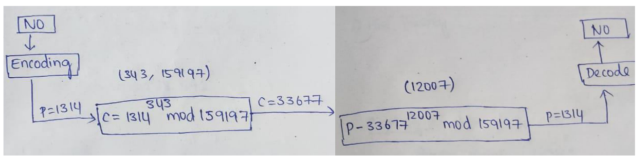
then

$d = e^{-1} \bmod \phi(n) = 343^{-1} \bmod 158400$

$= 12007$

plain text is "NO"

Encryption and Decryption:



12)Perform Rabin Cryptosystem (The example from the slide) and solve the problem showing the detailed steps.

1. Bob selects $p=23$ and $q=7$

Here $p \equiv 3 \bmod 4$

and

$q \equiv 3 \bmod 4$

2. STEP-2 :- Calculating 'n'

we know that

$n = p \times q \Rightarrow 161$

3. STEP-3:- Bob anounces 'n' as public key to Alice

4. STEP-4:- Alice plaintext is '24'.

5. STEP-5:- Here 161 (n) & 24 (plaintext) are Relatively prime

Now; cipher text $C = (24)^2 = 93 \bmod 161$

6. STEP-6:- Alice send '93' as cipher text to Bob.

7. STEP-7:- Calculating four values:

$a_1 = +(93^{(23+1)/4}) \bmod 23 = 1 \bmod 23$

$a_2 = -(93^{(23+1)/4}) \bmod 23 = 22 \bmod 23$

$b_1 = +(93^{(7+1)/4}) \bmod 7 = 4 \bmod 7$

$b_2 = -(93^{(7+1)/4}) \bmod 7 = 3 \bmod 7$

8. STEP-8:- Bob takes four possible Answer

1. $(a_1, b_1) = (1, 4)$
2. $(a_1, b_2) = (1, 3)$
3. $(a_2, b_1) = (22, 4)$
4. $(a_2, b_2) = (22, 3)$

9. STEP-9:- By using Chinese Remainder theorem

for ① $\Rightarrow$ $P = 1 \bmod 23$

$q = 4 \bmod 7$

$M = 23 \times 7 = 161$ $\quad M_1 = \frac{161}{23} = 7 \Rightarrow M_1^{-1} = 10$

$M_2 = \frac{161}{7} = 23 \Rightarrow M_2^{-1} = 4$

$P_1 = (1 \times 10 \times 7 + 4 \times 4 \times 23) \bmod 161$

$P_1 = (70 + 368) = 116 \bmod 161$

$= 116$

for ② $\Rightarrow$ $P = 1 \bmod 23$

$q = 3 \bmod 7$ $\quad M = 23 \times 7 = 161$

$M_1 = \frac{161}{23} = 7$ $\quad M_2 = \frac{161}{27} = 23$

$M_1^{-1} = 10$ $\quad M_2^{-1} = 4$

$P_2 = (1 \times 10 \times 7 + 3 \times 4 \times 23) \bmod 161$

$= 346 \bmod 161$

$= 24 \bmod 161$

$= 24$

for ③ $\Rightarrow$ $P = 22 \bmod 23$ & $q = 4 \bmod 7$

$M = 23 \times 7 = 161$

$M_1^{-1} = 7$ & $M_2^{-1} = 4$

$\therefore P_3 = (22 \times 10 \times 7 + 4 \times 4 \times 23) \bmod 161$

$1908 \bmod 161 = 137$

$= \cancel{1816} \bmod 161 = \cancel{45}$ //

For ④ $\Rightarrow$ $P = 22 \bmod 23$ & $q = 3 \bmod 7$

$M = 161$

$M_1 = \frac{161}{23} = 7$ & $M_2 = 23$

$M_1^{-1} = 10$ $\quad M_2 = 4$

$P_4 = 1816 \bmod 161 = 45$ //

10. STEP-10:-

$\therefore$ The possible plaintexts are

161, 24, 137 & 45

11. STEP-11:- Bob have to make decision which is correct plaintext.

The one correct is '24' i.e., second one.

13) Perform RSA-based digital signature scheme (key generation, signing, and verifying) where p = 167, q=113, e=201, and the message M="hi". [Coding: A=0, B=1, …, Z=25]

Given

$p=167$ & $q=113$

By Using RSA-based digital Signature schema

Key Generation :-

$n=p.q= 167 \times 113 = 18{,}871$

$\varnothing(n) = \varnothing(p.q) = \varnothing(p).\varnothing(q)$

$= 166 \times 112 = 18{,}592$

$e = 201$

$d = 201^{-1} \bmod 18{,}592$

$= 185$

Signing:

Given plaintext is "hi"

$\therefore M = 78$

Now

$S = (78^{185}) \bmod 18871$

$= 12126 \bmod 18871$

Verification:-

$M' = 12126^{201} \bmod 18871$

$= 78 \bmod 18871$

The message is accepted as

$M \equiv M' \bmod n$

Therefore the message is verified

14)Perform ElGamal-based digital signature scheme (key generation, signing, and verifying) where p = 3119, e1=2, d=127, r=307, and the message M=320.

ElGamal-based digital signature schema :-

Given $p=3119$, $\overset{e_1}{\cancel{q}}=2$, $d=127$ & $r=307$

Message is $M=320$

Key Generation:-

$e_2 = e_1^d$

$= 2^{127} \bmod 3119$

$e_2 = 1702$

Therefore senders public key $=(e_1, e_2, P)$

$=(2, 1702, 3119)$

and

private key $= d$

$= 127$

Signing:-

$M=320$

$s_1 = e_1^r = 2^{307} = 2083 \bmod 3119$

$s_2 = (M - d \times s_1) \times r^{-1} = (320 - 127 \times 2083) \times 307^{-1}$

$= 2105 \bmod 3118$

Sender sends $M$, $s_1$ and $s_2$ to receiver.

The receiver uses public key to calculate $V_1$ & $V_2$

Verification:-

$V_1 = e_1^M = 2^{3000} = 704 \bmod 3119$

$V_2 = d^{s_1} \times s_1^{s} = 1702^{2732} \times 2083^{2526}$

$= 704 \bmod 3119$

$\boxed{\therefore V_1 = V_2}$

(verified)

15)Alice and Bob use Diffie-Hellman Key Agreement protocol to agree upon a secret key. They select p=331, g=97, x=53 and y=67. Find the secret key.

Given

$g=97$, $P=331$, $x=53$ & $y=67$

we need to use Diffie-Hellman key Argument Method.

1) Alice uses $x=53$

so, $R_1 = 97^{53} \bmod 331$

$= 312$

2) Bob uses $y=67$

so, $R_2 = 97^{67} \bmod 331$

$= 217$

3) Alice send 312 to Bob

4) Bob send 217 to Alice

5) Alice calculates the symmetric key

$K = 217^{53} \bmod 331$

$= 129$

6. Bob calculate the symmetric key

$K = 312^{67} \bmod 331$

$= 129$

The value of K is same for both Alice & Bob

$\therefore g^{xy} \bmod P = 97^{53\times67} \bmod 331$

$97^{3551} \bmod 331$

$= 129$ //