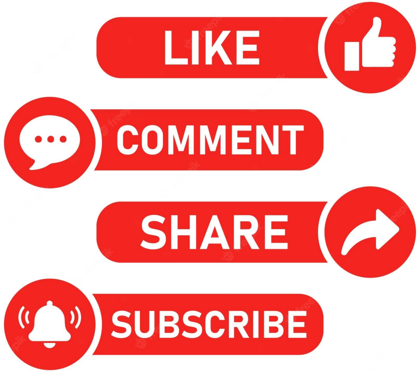


Unit 3

UNIT III ASYMMETRIC CRYPTOGRAPHY 9

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm

ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange –- Elliptic curve arithmetic – Elliptic curve cryptography.

What is Prime Number?

3, 5, 7, 11, 13, ...

1 3   1 5   1 13

1. **Prime numbers are numbers greater than 1 that only have two factors, 1 and the number itself.**
2. This means that a prime number is only divisible by 1 and itself.
3. If you divide a prime number by a number other than 1 and itself, you will get a non-zero remainder.
4. Any integer greater than 1 can be expressed as a product of prime factors:

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

$12 \Rightarrow 2^2 \times 3$

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

Primality Testing - Test if a given number is prime or not

any positive odd integer $n \geq 3$ can be expressed as

$$n - 1 = 2^k q \qquad \text{with } k > 0,\ q \text{ odd}$$

$\underline{\underline{7}} \Rightarrow 6 = 2^1 \times 3$

Miller Rabin

The **Miller–Rabin primality test** or **Rabin–Miller primality test** is a probabilistic primality test: an algorithm which determines whether a given number is likely to be prime

```
Input #1: n > 2, an odd integer to be tested for primality
Input #2: k, the number of rounds of testing to perform
Output: "composite" if n is found to be composite,
"probably prime" otherwise

let s > 0 and d odd > 0 such that n − 1 = 2^s d
repeat k times:
1)  a ← random(2, n − 2)
2)  x ← a^d mod n
    repeat s times:
      1) y ← x^2 mod n
         if y = 1 and x ≠ 1 and x ≠ n − 1 then
              return "composite"
         x ← y
    if y ≠ 1 then
         return "composite"
return "probably prime"
```

2^{nd}

$x = 1$

$y = 1 \bmod 13$

$= 1$ //

fail $\to x \neq 1$

$n = 13 \Rightarrow 12 = 2^2 \times 3$

$k = 1$

$s = 2$; $d = 3$

Loop: $k = 1$

1) Random$(2, 11) \Rightarrow 4$ (a)

2) $x = a^d \bmod n = 4^3 \bmod 13$

$= 12$ //

Loop:- $s = 2 \to 2$ times

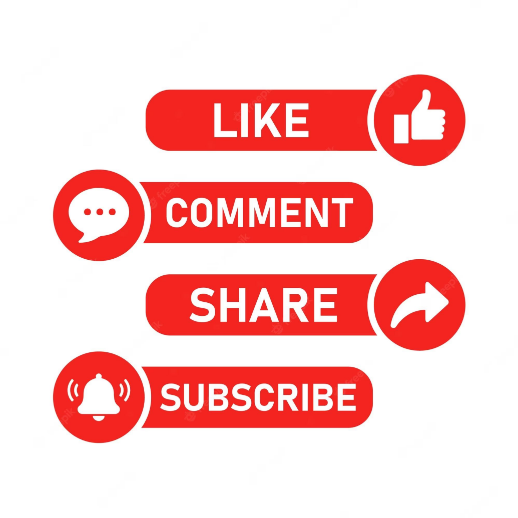
(i) $y = x^2 \bmod n = 12^2 \bmod 13$

$y = 1$

fail $\Rightarrow x \neq n-1$

$x \Rightarrow 1$

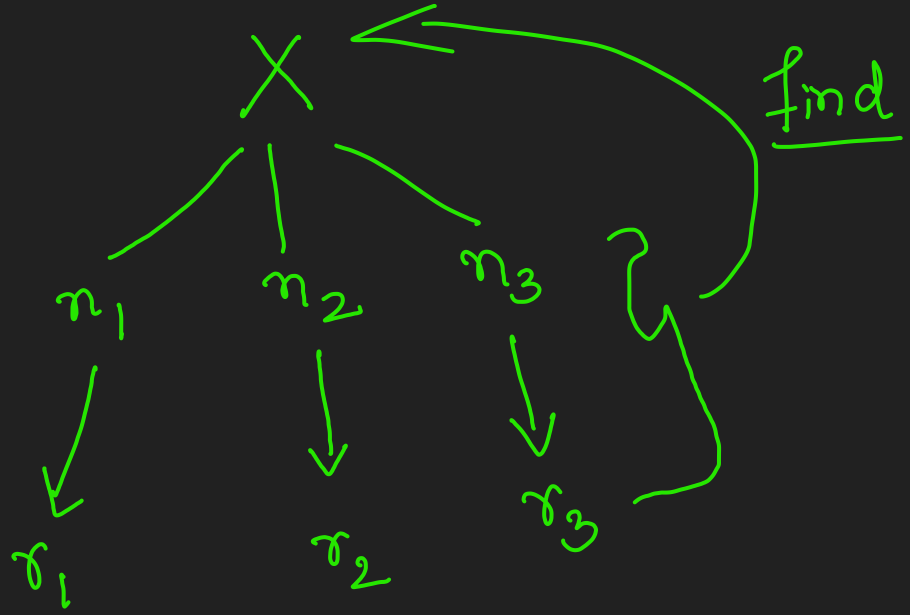
```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2k q);
2. Select a random integer a, 1 < a < n - 1;
3. if aq mod n = 1 then return("inconclusive");
4. for j = 0 to k - 1 do
5.    if a^(2^j q) mod n = n - 1 then return("inconclusive");
6. return("composite");
```



Thank You

Chinese Remainder Theorem

① pairwise coprime



Theorem

According to the theorem, the system of simultaneous congruences is defined as pairwise coprime positive integers $n_1, n_2, \cdots, n_k$ and arbitrary integers $a_1, a_2, \cdots, a_k$,

$$
\begin{aligned}
&x \equiv a_1 (mod\ n_1) \\
&x \equiv a_2 (mod\ n_2) \\
&\vdots \\
&x \equiv a_k (mod\ n_k)
\end{aligned}
$$

has a solution, which is a unique modulo, $N = n_1 n_2 \cdots n_k$.

Example 1

$X \equiv 8 \bmod 9$ ($8 \to r_1$, $9 \to a_1$)

$X \equiv 3 \bmod 20$ ($3 \to r_2$, $20 \to a_2$)

① $M = a_1 \times a_2 = 9 \times 20 = 180$

② $z_i = \frac{M}{a_i}$

$z_1 = \frac{M}{a_1} = \frac{180}{9} = 20$

$z_2 = M/a_2 = \frac{180}{20} = 9$

③ $y_i = (z_i)^{-1} \bmod a_i$

$y_1 = (20)^{-1} \bmod 9 = 5$

$y_2 = (9)^{-1} \bmod 20 = 9$

④ $w_i = (y_i z_i) \bmod M$

$w_1 = y_1 z_1 \bmod 180$

$= 5 \times 20 \bmod 180$

$= 100$

$w_2 = y_2 z_2 \bmod 180$

$= 9 \times 9 \bmod 180 = 81$

⑤ $X \equiv (\sum r_i w_i) \bmod M$

$X \equiv (r_1 w_1 + r_2 w_2) \bmod M$

$X \equiv (8 \times 100 + 3 \times 81) \bmod 180$

$X \equiv 1043 \bmod 180$

$\boxed{X \Rightarrow 143}$ //

Example: Solve the simultaneous congruences

$$x \equiv 6 \pmod{11}, \quad x \equiv 13 \pmod{16}, \quad x \equiv 9 \pmod{21}, \quad x \equiv 19 \pmod{25}.$$

r_1 a_1 r_2 a_2 r_3 a_3 r_4 a_4

① $M = a_1 a_2 a_3 a_4 = 11 \times 16 \times 21 \times 25$
$= 92400$

② $z_i = M/a_i$

$z_1 = M/a_1 = 92400/11 = 8400$
$z_2 = M/a_2 = 92400/16 = 5775$
$z_3 = M/a_3 = 92400/21 = 4400$
$z_4 = M/a_4 = 92400/25 = 3696$

③ $y_i = z_i^{-1} \bmod a_i$

$y_1 = (z_1)^{-1} \bmod a_1 = (8400)^{-1} \bmod 11 = 8$
$y_2 = (z_2)^{-1} \bmod a_2 = (5775)^{-1} \bmod 16 = 15$
$y_3 = (z_3)^{-1} \bmod a_3 = (4400)^{-1} \bmod 21 = 2$
$y_4 = (z_4)^{-1} \bmod a_4 = (3696)^{-1} \bmod 25 = 6$

Euclidean

modular inverse

④ $w_i = (y_i z_i) \bmod M =$

$w_1 = y_1 z_1 \bmod M = 8 \times 8400 \bmod 92400 = 67200$
$w_2 = y_2 z_2 \bmod M = 15 \times 5775 \bmod 92400 = 86625$
$w_3 = y_3 z_3 \bmod M = 2 \times 4400 \bmod 92400 = 8800$
$w_4 = y_4 z_4 \bmod M = 6 \times 3696 \bmod 92400$
$= 22176$

⑤ $X \equiv (r_1 w_1 + r_2 w_2 + r_3 w_3 + r_4 w_4) \bmod M$

$X \equiv (6 \times 67200) + (13 \times 86625) + (9 \times 8800) + (19 \times 22176)$
$\bmod 92400$

$X \equiv 2029869 \bmod 92400 \Rightarrow X = 89469$

Thank You