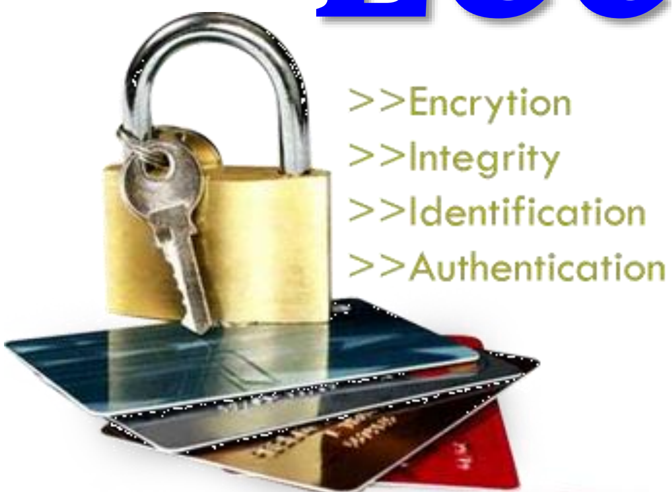
Information & System Security

Lecture 25



VIT-AP
UNIVERSITY

Mathematics Related to Public Key Cryptography

9-2 PRIMALITY TESTING

Finding an algorithm to correctly and efficiently test a very large integer and output a prime or a composite has always been a challenge in number theory, and consequently in cryptography. However, recent developments look very promising.

Topics discussed in this section:

9.2.1 Deterministic Algorithms

9.2.2 Probabilistic Algorithms

9.2.3 Recommended Primality Test

9.2.2 Probabilistic Algorithms

Fermat Test

If n is a prime, then $a^{n-1} \equiv 1 \bmod n$.

If n is a composite, it is possible that $a^{n-1} \equiv 1 \bmod n$.

Example

Does the number 561 pass the Fermat test?

Solution

Use base a=2.

$$2^{561-1} = 1 \bmod 561$$

The number passes the Fermat test, but it is not a prime, because 561 = 33 × 17.

9.2.2 *Continued*

Square Root Test

If n is a prime, $\sqrt{1} \bmod n = \pm 1$.
If n is a composite, $\sqrt{1} \bmod n = \pm 1$ and possibly other values.

Example

What are the square roots of 1 mod *n* if *n* is 7 (a prime)?

Solution

We can see that the only square roots are 1 and −1.

$$1^2 = 1 \bmod 7 \qquad (-1)^2 = 1 \bmod 7$$
$$2^2 = 4 \bmod 7 \qquad (-2)^2 = 4 \bmod 7$$
$$3^2 = 2 \bmod 7 \qquad (-3)^2 = 2 \bmod 7$$

Note: we don’t have to test 4, 5 and 6 because
4 = –3 mod 7, 5 = –2 mod 7 and 6 = –1 mod 7.

Example

What are the square roots of 1 mod *n* if *n* is 8 (a composite)?

Solution

There are four solutions: 1, 3, 5, and 7 (which is −1). We can see that

$$1^2 = 1 \bmod 8 \qquad (-1)^2 = 1 \bmod 8$$
$$3^2 = 1 \bmod 8 \qquad 5^2 = 1 \bmod 8$$

Example

What are the square roots of 1 mod *n* if *n* is 17 (a prime)?

Solution

There are only two solutions: 1 and −1

$$
\begin{array}{ll}
1^2 = 1 \bmod 17 & (-1)^2 = 1 \bmod 17 \\
2^2 = 4 \bmod 17 & (-2)^2 = 4 \bmod 17 \\
3^2 = 9 \bmod 17 & (-3)^2 = 9 \bmod 17 \\
4^2 = 16 \bmod 17 & (-4)^2 = 16 \bmod 17 \\
5^2 = 8 \bmod 17 & (-5)^2 = 8 \bmod 17 \\
6^2 = 2 \bmod 17 & (-6)^2 = 2 \bmod 17 \\
(7)^2 = 15 \bmod 17 & (-7)^2 = 15 \bmod 17 \\
(8)^2 = 13 \bmod 17 & (-8)^2 = 13 \bmod 17
\end{array}
$$

Example

What are the square roots of 1 mod *n* if *n* is 22 (a composite)?

Solution

Surprisingly, there are only two solutions, +1 and −1, although 22 is a composite.

$$1^2 = 1 \bmod 22$$
$$(-1)^2 = 1 \bmod 22$$

9.2.2 Continued

Miller-Rabin Test

$$n - 1 = m \times 2^k$$

Idea behind Fermat primality test

$$a^{n-1} = a^{m \times 2^k} = [a^m]^{2^k} = [a^m]^{\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{k \text{ times}}}$$

Note

The Miller-Rabin test needs from step 0 to step $k - 1$.

9.2.2 Continued

Miller-Rabin Test

```
Miller_Rabin_Test (n, a) // n is the number; a is the base.
{
  Find m and k such that n − 1 = m × 2^k
  T = a^m mod n
  if (T = ± 1 mod n) return "a prime"     // May be
  for (i = 1 to k)
  {
    T ← T^2 mod n
    if (T = +1) return "a composite"
    if (T = −1) return "a prime"     // May be
  }
  return "a composite"
}
```

Time Complexity $O(k(\log n)^3)$

Example

Does the number 561 pass the Miller-Rabin test?

Solution

Using base 2, let $561 - 1 = 35 \times 2^4$, which means $m = 35$, $k = 4$, and $a = 2$.

Initialization:	$T = 2^{35} \bmod 561 = 263 \bmod 561$
$k = 1$:	$T = 263^2 \bmod 561 = 166 \bmod 561$
$k = 2$:	$T = 166^2 \bmod 561 = 67 \bmod 561$
$k = 3$:	$T = 67^2 \bmod 561 = +1 \bmod 561$ → **a composite**

Example

We already know that 14 is not a prime. Let us apply the Miller-Rabin test.

Solution

With base 2, let $14 - 1 = 13 \times 2^0$, which means that $m = 13$, $k = 0$, and $a = 2$.

- **In this case, because $k = 0$, we should do only the initialization step: $T = 2^{13} \bmod 14 = 2 \bmod 14$.**
- **However, because the algorithm never enters the loop, it returns a composite.**

Example

We know that 61 is a prime, let us see if it passes the Miller-Rabin test.

Solution

We use base 2.

$$61 - 1 = 15 \times 2^2 \;\rightarrow\; m = 15 \quad k = 2 \quad a = 2$$

$$\textit{Initialization:} \quad \mathrm{T} = 2^{15} \bmod 61 = 11 \bmod 61$$

$$k = 1 \qquad \mathrm{T} = 11^2 \bmod 61 = -1 \bmod 61 \rightarrow \textbf{a prime}$$

9.2.3 Recommended Primality Test

Today, one of the most popular primality test is a combination of both

- *the Miller-Rabin test*
- *the divisibility test*

Example

The number 4033 is a composite (37 × 109). Does it pass the recommended primality test?

Solution

1. Perform the Miller-Rabin test with a base of 2,

   $4033 - 1 = 63 \times 2^6$, which means m is 63 and k is 6.

Initialization: $T \equiv 2^{63} \pmod{4033} \equiv 3521 \pmod{4033}$

$k = 1$ $\quad T \equiv T^2 \equiv 3521^2 \pmod{4033} \equiv -1 \pmod{4033} \rightarrow$ **Passes**

2. But we are not satisfied. We continue the Miller-Rabin test with another base, 3.

9.2.3 *Continued*

Example

Initialization: $T \equiv 3^{63} \pmod{4033} \equiv 3551 \pmod{4033}$

$k = 1 \quad T \equiv T^2 \equiv 3551^2$ (mod 4033 $\equiv 2443 \pmod{4033}$

$k = 2 \quad T \equiv T^2 \equiv 2443^2$ (mod 4033 $\equiv 3442 \pmod{4033}$

$k = 3 \quad T \equiv T^2 \equiv 3442^2$ (mod 4033 $\equiv 2443 \pmod{4033}$

$k = 4 \quad T \equiv T^2 \equiv 2443^2$ (mod 4033 $\equiv 3442 \pmod{4033}$

$k = 5 \quad T \equiv T^2 \equiv 3442^2$ (mod 4033 $\equiv 2443 \pmod{4033}$ $\rightarrow$**Failed (composite)**

3. Perform the divisibility tests first with the numbers 2, 3, 5, 7, …, 61. We found that 37 is divisible by 4033.

Conclusion:

4033 is a composite number.

References

- **Chapter 9** - Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.

- **Chapter 8** - William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.