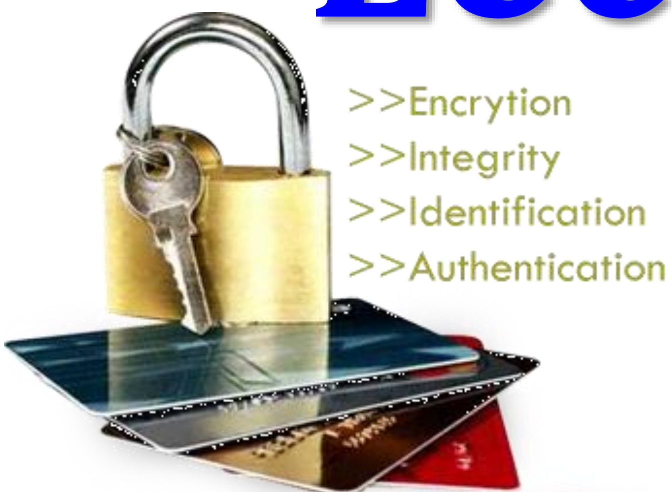
Information & System Security

Lecture 24



VIT-AP
UNIVERSITY

Mathematics Related to Public Key Cryptography

9-1 PRIMES

- ***Asymmetric-key cryptography uses primes extensively.***
- ***This section discusses only a few concepts and facts to pave the way for Chapter 10.***

Topics discussed in this section:

9.1.4 Euler's Phi-Function
9.1.5 Fermat's Little Theorem
9.1.6 Euler's Theorem
9.1.7 Generating Primes

9.1.4 Euler's Phi-Function

- *Euler's phi-function,* **$\phi(n)$**, *which is sometimes called the Euler's totient function.*

Properties:

1. $\phi(1) = 0.$
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

9.1.4 Continued

$\varnothing(n) = \varnothing(pq) = \varnothing(p) \times \varnothing(q) = (p-1) \times (q-1)$, where p and q are prime numbers.

Proof:

- To see that $\varnothing(n) = \varnothing(p) \times \varnothing(q)$, consider that the set of positive integers less than n is the set $\{1,\ldots,(pq-1)\}$.
- The integers in this set that are not relatively prime to n are the set $\{p,2p,\ldots,(q-1)p\}$ and the set $\{q,2q,\ldots,(p-1)q\}$.
- Accordingly,

$$
\begin{aligned}
\varnothing(n) &= (pq-1)-[(q-1) + (p-1)] \\
&= pq-(p + q) + 1 \\
&= (p-1) \times (q-1) \\
&= \varnothing(p) \times \varnothing(q)
\end{aligned}
$$

Proved.

9.1.4 Continued

- We can combine the four rules (discussed now) to find the value of $\phi(n)$.
- For example, if n can be factored as $n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$, then we combine the third and the fourth rule to find $\phi(n)$.

$$\boxed{\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})}$$

Note

The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of *n*.

Example

What is the value of $\phi(13)$?

Solution

Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

Example

What is the value of $\phi(10)$?

Solution

We can use the third rule: $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Example

What is the value of $\phi(240)$?

Solution

We can write $240 = 2^4 \times 3^1 \times 5^1$.

Then, $\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$

Example

Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution

No. The third rule applies when *m* and *n* are relatively prime. Here $49 = 7^2$.

We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

Example

What is the number of elements in Z_{14}*?

Solution

The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

9.1.5 Fermat's Little Theorem

First Version

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

Second Version

$$\boxed{a^{p} \equiv a \bmod p}$$

Example

Find the result of 6^{10} mod 11.

Solution

We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where *p* = 11.

Example

Find the result of 3^{12} mod 11.

Solution

Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using Fermat's little theorem.

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\,(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

9.1.5 Continued

Multiplicative Inverse

Fermat's theorem can be used to find multiplicative inverses modulo a prime.

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

Example

The multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

First Version

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

Second Version

$$\boxed{a^{k \times \phi(n) + 1} \equiv a \pmod{n}}$$

Note

The second version of Euler's theorem is used in the RSA cryptosystem.

Example

Find the result of 6^{24} mod 35.

Solution

We have 6^{24} mod 35 = $6^{\phi(35)}$ mod 35 = 1.

Example

Find the result of 20^{62} mod 77.

Solution

If we let k = 1 on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\,(20^{\phi(77)+1} \bmod 77) \bmod 77$$
$$= (20)(20) \bmod 77 = 15.$$

Multiplicative Inverse

Euler's theorem can be used to find multiplicative inverses modulo a composite.

$$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$$

Example

The multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

9.1.7 Generating Primes

Just think of following functions which generates some primes

- $f(n) = 2n+3 = \{3, 5, 7, 9, 11, 13, 15, 17, 19, 23, \ldots\}$

  [for $n = 0, 1, 2, \ldots$] [Linear]

- $g(n) = n^2+1 = \{2, 5, 10, 17, 26, 37, 50, 65, 82, 101, \ldots\}$

  [for $n = 1, 2, 3, \ldots$] [Quadratic]

- $h(n) = 2^n + 1 = \{2, 3, 5, 9, 17, 33, 65, 129, 257, 513, \ldots\}$

  [for $n = 0, 1, 2, 3, \ldots$] [Exponential]

Mersenne Primes

$$M_p = 2^p - 1$$

$$M_2 = 2^2 - 1 = 3$$
$$M_3 = 2^3 - 1 = 7$$
$$M_5 = 2^5 - 1 = 31$$
$$M_7 = 2^7 - 1 = 127$$
$$M_{11} = 2^{11} - 1 = 2047 \quad \textbf{Not a prime } (2047 = 23 \times 89)$$
$$M_{13} = 2^{13} - 1 = 8191$$
$$M_{17} = 2^{17} - 1 = 131071$$

Note

A number in the form $M_p = 2^p - 1$ is called a Mersenne number and may or may not be a prime.

9.1.7 Continued

Fermat Primes

$$\boxed{F_n = 2^{2^n} + 1}$$

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$
$F_5 = 4294967297$ [641×6700417 *Not a prime*]

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

Divisibility Algorithm

```
Divisibility_Test (n)
{ // n is the number to test for primality
  r ← 2
  while (r < √n )
  {
   if (r | n) return "a composite"
   r ← r + 1
  }
   return "a prime"
}
```

Note

The bit-operation complexity of the divisibility test is exponential.

Example

Assume n has 256 bits. What is the number of bit operations needed to run the divisibility-test algorithm?

Solution

The bit-operation complexity of this algorithm is $\mathbf{2^{n_b/2}}$. This means that the algorithm needs 2^{128} bits operations. On a computer capable of doing 2^{64} bits operations per second, the algorithm needs 2^{64} seconds to do the testing = 5,84,94,24,17,355 years (forever).

9.2.1 Continued
AKS Algorithm

- ***AKS** primality test is a deterministic primality-proving algorithm*

- *Developed by three **IIT Kanpur** computer scientists-Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.*

$Let\ a \in Z,\ n \in N,\ n \geq 2,\ and\ \ gcd(a, n) = 1.$

$Then\ n\ is\ prime\ if\ and\ only\ if$

$(X + a)^n = X^n + a\ (mod\ n).$ ***Polynomial***

AKS Algorithm

The bit-operation complexity of this algorithm is

$$O((\log_2 n_b)^{12})$$

Example

Assume *n* has 256 bits. What is the number of bit operations needed to run the AKS algorithm?

Solution

This algorithm needs only $(\log_2 256)^{12}$ = 68,71,94,76,736 bits operations. On a computer capable of doing 2^{32} bits operations per second, the algorithm needs only 16 seconds.

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.