Information & System Security

Lecture 27

VIT-AP
UNIVERSITY

Mathematics Related to Public Key Cryptography

9-6 EXPONENTIATION AND LOGARITHM

Exponentiation: $y = a^x \;\rightarrow$ **Logarithm:** $x = \log_a y$

<u>Topics discussed in this section:</u>

9.6.1 Exponentiation

9.6.2 Logarithm

9.6.1 Exponentiation

$$y = a^x \bmod n$$

Fast Exponentiation

$$y = a^{\boxed{x_{n_b-1} \times 2^{n_b-1} + x_{n_b-2} \times 2^{n_b-2} + \cdots + x_1 \times 2^1 + x_0 \times 2^0}}$$

in which x_i is 0 or 1

$$\downarrow$$

$$y = \boxed{\boxed{a^{2^{n_b-1}}} \text{ or } \boxed{1}} \times \boxed{\boxed{a^{2^{n_b-2}}} \text{ or } \boxed{1}} \times \cdots \times \boxed{\boxed{a^2} \text{ or } \boxed{1}} \times \boxed{\boxed{a} \text{ or } \boxed{1}}$$

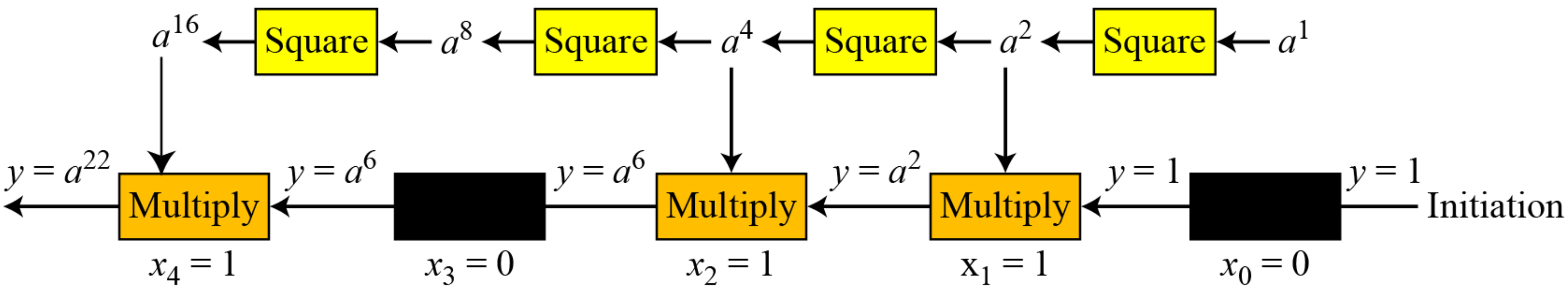
Example:

$$\boxed{y = a^9 = a^{1001_2} = a^8 \times 1 \times 1 \times a}$$

The idea behind the square-and-multiply method

Example

Figure shows the process for calculating $y = a^x$ using the Algorithm (for simplicity, the modulus is not shown). In this case, $x = 22 = (10110)_2$ in binary. The exponent has five bits.



Demonstration of calculation of a^{22} using square-and-multiply method

9.6.1 Continued

Calculation of 17^{22} mod 21

i	x_i	Multiplication (Initialization: $y = 1$)	Squaring (Initialization: $a = 17$)
0	0	$\rightarrow$	$a = 17^2 \bmod 21 = 16$
1	1	$y = 1 \times 16 \bmod 21 = 16 \rightarrow$	$a = 16^2 \bmod 21 = 4$
2	1	$y = 16 \times 4 \bmod 21 = 1 \rightarrow$	$a = 4^2 \bmod 21 = 16$
3	0	$\rightarrow$	$a = 16^2 \bmod 21 = 4$
4	1	$y = 1 \times 4 \bmod 21 = 4 \rightarrow$	

Note

The bit-operation complexity of the fast exponential algorithm is polynomial.

9.6.2 Logarithm

In cryptography, we also need to discuss modular logarithm.

Exhaustive Search

```
Modular_Logarithm (a, y, n)
{
    for (x = 1 to n − 1)   // k is the number of bits in x
    {
        if (y ≡ a^x mod n) return x
    }
    return failure
}
```

Order of the Group

Example

What is the order of group G = < Z_{21}^{*}, ×>?

|G| = ϕ(21) = ϕ(3) × ϕ(7) = 2 × 6 =12.

There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20.

All are relatively prime with 21.

Order of an Element

Example

Find the order of all elements in G = < Z_{10}^{*}, ×>.

Solution

This group has only ϕ(10) = 4 elements: 1, 3, 7, 9. We can find the order of each element by trial and error.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$.

b. $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$.

c. $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$.

d. $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$.

9.6.2 Continued

Euler's Theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$

Example

The following Table shows the result of $a^i \equiv x \pmod 8$ for the group G = < Z_8^*, ×>. $\phi(8)=4$.

The elements are 1, 3, 5, and 7.

Finding the orders of elements

	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$
$a=1$	**x: 1**	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a=3$	x: 3	**x: 1**	x: 3	x: 1	x: 3	x: 1	x: 3
$a=5$	x: 5	**x: 1**	x: 5	x: 1	x: 5	x: 1	x: 5
$a=7$	x: 7	**x: 1**	x: 7	x: 1	x: 7	x: 1	x: 7

Primitive Roots

In the group G = < Z_n^*, ×>, when the order of an element is the same as ϕ(n), that element is called the primitive root of the group.

Example

The Table (previous) shows that there are no primitive roots in G = < Z_8^*, ×> because no element has the order equal to ϕ(8) = 4. The order of elements are all smaller than 4.

Example

The following Table shows the result of $a^i \equiv x \pmod 7$ for the group G = < Z_7^*, ×>. In this group, ϕ(7) = 6.

		$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
	$a = 1$	$\boxed{x: 1}$	x: 1	x: 1	x: 1	x: 1	x: 1
	$a = 2$	x: 2	x: 4	$\boxed{x: 1}$	x: 2	x: 4	x: 1
Primitive root →	$a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	$\boxed{x: 1}$
	$a = 4$	x: 4	x: 2	$\boxed{x: 1}$	x: 4	x: 2	x: 1
Primitive root →	$a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	$\boxed{x: 1}$
	$a = 6$	x: 6	$\boxed{x: 1}$	x: 6	x: 1	x: 6	x: 1

Note

The group G = < Z_n^*, ×> has primitive roots only if *n* is 2, 4, p^t, or $2p^t$.

Example

For which value of *n*, does the group G = < Z_n^*, ×> have primitive roots: 17, 20, 38, and 50?

Solution

a. G = < Z_{17}^*, ×> has primitive roots, 17 is a prime.
b. G = < Z_{20}^*, ×> has no primitive roots.
c. G = < Z_{38}^*, ×> has primitive roots, 38 = 2 × 19 prime.
d. G = < Z_{50}^*,×> has primitive roots, 50 = 2 × 5^2 and 5 is a prime.

Note

If the group G = < Z_n^*, ×> has any primitive root, the number of primitive roots is $\phi(\phi(n))$.

Example

Find number of primitive roots of 7 and 19.

Solution

(a) $\phi(\phi(7)) = \phi(7-1) = \phi(6) = \phi(2 \times 3) = \phi(2) \times \phi(3) = 2$.

7 has 2 primitive roots— 3 and 5.

(b) Try to find $\phi(\phi(19))$.

9.6.2 Continued

Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Primitive roots of 19 are {2,3,10, 13,14,15}

9.6.2 Continued

Cyclic Group: ***If g is a primitive root in the group, we can generate the set Z_n^* as $Z_n^* = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$***

Example

The group G = < Z_{10}^*, ×> has two primitive roots because ϕ(10) = 4 and ϕ(ϕ(10)) = 2. It can be found that the primitive roots are 3 and 7. The following shows how we can create the whole set Z_{10}^* using each primitive root.

$$g = 3 \rightarrow g^1 \bmod 10 = 3 \quad g^2 \bmod 10 = 9 \quad g^3 \bmod 10 = 7 \quad g^4 \bmod 10 = 1$$
$$g = 7 \rightarrow g^1 \bmod 10 = 7 \quad g^2 \bmod 10 = 9 \quad g^3 \bmod 10 = 3 \quad g^4 \bmod 10 = 1$$

The group G = <Z_n*, ×> is a cyclic group if it has primitive roots.
The group G = <Z_p*, ×> is always cyclic.

The idea of Discrete Logarithm

Properties of G = < Z_p^*, ×>:

1. ***Its elements include all integers from 1 to p − 1.***
2. ***It always has primitive roots.***
3. ***It is cyclic. The elements can be created using g^x where x is an integer from 1 to $\phi(n) = p - 1$.***
4. ***The primitive roots can be thought as the base of logarithm.***

   If the group has ***k*** primitive roots, calculations can be done in ***k*** different bases. Given $x=\log_g y$ for any element in ***y*** in the set, there is an ***x*** that is the log of ***y*** in base ***g***. This type of logarithm is called **discrete logarithm**.

Solution to Modular Logarithm using Discrete Logs

Solve $y = a^x \pmod{n}$ when y is given, and we need to find x.

Tabulation of Discrete Logarithms

- One way to solve the above-mentioned problem is to use a table for each Z_p^* and different bases.
- This type of table can be precalculated and saved.

Discrete logarithm for $\mathbf{G} = \langle \mathbf{Z}_7{}^*, \times \rangle$

y	1	2	3	4	5	6
$x = L_3\, y$	6	2	1	4	5	3
$x = L_5\, y$	6	4	5	2	1	3

Example

Find x in each of the following cases:

1. $4 \equiv 3^x \pmod 7$.

2. $6 \equiv 5^x \pmod 7$.

Solution

We can easily use the tabulation of the discrete logarithm in the previous Table.

1. $4 \equiv 3^x \bmod 7 \rightarrow x = L_3 4 \bmod 7 = 4 \bmod 7$

2. $6 \equiv 5^x \bmod 7 \rightarrow x = L_5 6 \bmod 7 = 3 \bmod 7$

Using Properties of Discrete Logarithms

Comparison of traditional and discrete logarithms

Traditional Logarithm	Discrete Logarithms
$\log_a 1 = 0$	$L_g 1 \equiv 0 \pmod{\phi(n)}$
$\log_a (x \times y) = \log_a x + \log_a y$	$L_g(x \times y) \equiv (L_g x + L_g y) \pmod{\phi(n)}$
$\log_a x^k = k \times \log_a x$	$L_g x^k \equiv k \times L_g x \pmod{\phi(n)}$

Using Algorithms Based on Discrete Logarithms

- Cannot be used if ***n*** is very large.

Note

The discrete logarithm problem has the same complexity as the factorization problem.

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.