TUTORIAL

CSCI361 – Computer Security

Sionggo Japit

sjapit@uow.edu.au

12 February 2024

FAST EXPONENTIATION

MODULAR EXPONENTIATION METHOD

Fast exponentiation

Modular Exponentiation Method

To calculate $\mathrm{X}^{a} \bmod m$:

1. Write a in base two:

$$a = a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots + a_{n-1} 2^{n-1}$$

2. Calculate X^{2^i}, where 1 £ i £ n-1.

3. Use $\mathrm{X}^{a} = (X^{2^0})^{a_0}$ ´ $(X^{2^1})^{a_1}$ ´ ...´ $(X^{2^{n-1}})^{a_{n-1}}$

   and multiply the X^{2i} for which a_i is not zero.

Fast exponentiation

For example:

- To find 7^{219} mod 1823
- Step 1: (determine how many bits are required to store the value 219)
  - n = $\log_2 219$ = 8 bits (round up)
- Step 2:
  - Calculate the first 8 terms as shown in the next slide.

$2^0 = 1$	7^1 (mod 1823)	7 (mod 1823)	7
$2^1 = 2$	7^2 (mod 1823)	7 x 7 = 49 (mod 1823)	49
$2^2 = 4$	7^4 (mod 1823)	$(7^2)^2 = (49)^2$ = 2401 (mod 1823) = 578 (mod 1823)	578
$2^3 = 8$	7^8 (mod 1823)	$(7^4)^2$ (mod 1823) = $(578)^2$ (mod 1823) = 334084 (mod 1823) = 475 (mod 1823)	475
$2^4 = 16$	7^{16} (mod 1823)	$(7^8)^2$ (mod 1823) = $(475)^2$ (mod 1823) = 225625 (mod 1823) = 1396 (mod 1823)	1396
$2^5 = 32$	7^{32} (mod 1823)	$(7^{16})^2$ (mod 1823) = $(1396)^2$ (mod 1823) = 1948816 (mod 1823) = 29 (mod 1823)	29
$2^6 = 64$	7^{64} (mod 1823)	$(7^{32})^2$ (mod 1823) = $(29)^2$ (mod 1823) = 841 (mod 1823)	841
$2^7 = 128$	7^{128} (mod 1823)	$(7^{64})^2$ (mod 1823) = $(841)^2$ (mod 1823) = 1780 (mod 1823)	1780

Fast exponentiation

- Step 3:
  - Break the exponential power. This can be achieved by expressing the power, in this case 219, in binary form; i.e., 219 = 11011011, and thus

    219 = 128 + 64 + 16 + 8 + 2 + 1

    And so,

$$7^{219} \bmod 1823$$

$$= 7^{128+64+16+8+2+1} \bmod 1823$$

$$= 7^{128} \text{´}\ 7^{64} \text{´}\ 7^{16} \text{´}\ 7^{8} \text{´}\ 7^{2} \text{´}\ 7^{1} \bmod 1823$$

Fast exponentiation

- Step 4:
  - Fill in equation with the pre-computed solution (from step 2)

    That is,

$$
\begin{aligned}
& 7^{219} \bmod 1823 \\
& = 1780 ´ \ 841 ´ \ 1396 ´ \ 475 ´ \ 49 ´ \ 7 \bmod 1823 \\
& = 297 ´ \ 1396 ´ \ 475 ´ \ 49 ´ \ 7 \bmod 1823 \\
& = 791 ´ \ 475 ´ \ 49 ´ \ 7 \bmod 1823 \\
& = 187 ´ \ 49 ´ \ 7 \bmod 1823 \\
& = 48 ´ \ 7 \bmod 1823 \\
& = 336 \bmod 1823
\end{aligned}
$$

SQUARE AND MULTIPLY (S SX) METHOD

Fast exponentiation

Square and Multiply (SX) method

To calculate N^p

1. Write p in binary equivalent
2. For each binary bit in p,
   - If ‘1’, replace with SX
   - If ‘0’, replace with S
3. Remove the first SX (of the most significant bit)
4. For each S, compute Square mod p
5. For each X, multiply with N mod p

Fast exponentiation

For example:

Compute 7^{219} mod 1823

- Step 1:
  - Write 219 in binary form; i.e., 11011011
- Step 2:
  - Express 11011011 in SX form; i.e., SX SX S SX SX S SX SX
- Step 3:
  - Drop the first SX, we have SX S SX SX S SX SX

Fast exponentiation

- Step 4:
  - Construct the expression SX S SX SX S SX SX
    - $7^2 \text{ x } 7$ SX S SX SX S SX SX
    - $(7^2 \text{ x } 7)^2$ SX S SX SX S SX SX
    - $((7^2 \text{ x } 7)^2)^2 \text{ x } 7$ SX S SX SX S SX SX
    - $(((7^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7$ SX S SX SX S SX SX
    - $((((7^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7)^2$ SX S SX SX S SX SX
    - $((((((7^2 \text{ x } 7)^2)^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7$ SX S SX SX S SX SX
    - $(((((((7^2 \text{ x } 7)^2)^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7$ SX S SX SX S SX SX
    - $(((((((7^2 \text{ x } 7)^2)^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7$ mod 1823

Fast exponentiation

- Step 4:
  - …then compute as follow:
    - $(((((((\ 7^2 \text{ x } 7\ )^2)^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $(((((((\ 343\ )^2)^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((((((\ 117649\ )^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((((((\ 977\ )^2) \text{ x } 7)^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((((\ 6681703\ )^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((((\ 408\ )^2 \text{ x } 7)^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $(((\ 1165248\ )^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $(((\ 351\ )^2)^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((\ 123201\ )^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $((\ 1060\ )^2 \text{ x } 7)^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $(\ 7865200\ )^2 \text{ x } 7 \ \ \text{mod } 1823$
    - $(\ 778\ )^2 \text{ x } 7 \ \ \text{mod } 1823$
    - 4236988 mod 1823
    - 336

Fast exponentiation

SX S SX SX S SX SX

Alternatively,

$$SX:\ 7^2\ ´\ 7 \bmod 1823 = 343$$

$$S\ :343^2 \bmod 1823 = 977$$

$$SX:977^2\ ´\ 7 \bmod 1823 = 408$$

$$SX:408^2\ ´\ 7 \bmod 1823 = 351$$

$$S\ :351^2 \bmod 1823 = 1060$$

$$SX:1060^2\ ´\ 7 \bmod 1823 = 778$$

$$SX:778^2\ ´\ 7 \bmod 1823 = 336$$

$$Hence\ 7^{219} \bmod 1823 = 336$$

Fast exponentiation

Another example:

Compute 22^{199} mod 71

1. Express 199 as binary: 11000111
2. Express 11000111 as SX S notation:

   SX SX S S S SX SX SX

3. Drop the first SX term (of the most significant bit)
4. Translate the SX S notation to modulo expression and solve:

Fast exponentiation

- SX S S S SX SX SX

$= ((((((22^2 \text{ x } 22)^2)^2)^2)^2 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (((((58 \text{ x } 22)^2)^2)^2)^2 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (((((69^2)^2)^2)^2 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= ((((4^2)^2)^2 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (((16^2)^2 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= ((43^2) \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (3 \text{ x } 22)^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (66^2 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= (25 \text{ x } 22)^2 \text{ x } 22 \pmod{71}$

$= 53^2 \text{ x } 22 \pmod{71}$

$= 40 \text{ x } 22 \pmod{71}$

$= 28$

Fast exponentiation

SX S S S SX SX SX

Alternatively,

$$
\begin{aligned}
SX &: 22^2 \quad \text{´}\ 22 \bmod 71 = 69 \\
S &: 69^2 \quad \bmod 71 = 4 \\
S &: 4^2 \quad \bmod 71 = 16 \\
S &: 16^2 \quad \bmod 71 = 43 \\
S &: 43^2 \quad \bmod 71 = 66 \\
SX &: 66^2 \quad \text{´}\ 22 \bmod 71 = 53 \\
SX &: 53^2 \quad \text{´}\ 22 \bmod 71 = 28
\end{aligned}
$$

$$Hence\ 22^{199} \bmod 71 = 28$$