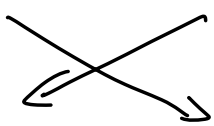
4.3.3.9 Exaple 7

Q : $p = 23$ $g = 5$

$a = 6$ $b = 15$ $y = g^x \bmod p$

Solution

① $5^6 \bmod 23 = 8$ $5^{15} \bmod 23 = 19$



$19^6 \bmod 23 = 2$ $8^{15} \bmod 23 = 2$

② $5^{15} \bmod 23$

$= (5^3)^5 \bmod 23$

$= (125)^5 \bmod 23$

$= 10^5 \bmod 23$

$= 19$