7.2.1 Diffie-Hellman Example

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

Alice	Bob
$a = 6$	$b = 15$

(a) $A = ?$ (b) $B = ?$

(c) $S = ?$

Solution (a) $A = g^a \bmod p$

$= 5^6 \bmod 23$

$= 8$

(b) $B = g^b \bmod p$

$= 5^{15} \bmod 23$

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

$= (3125)^3 \bmod 23$

$= 20^3 \bmod 23$

$= 19$

③ Alice :

$S = B^a \bmod p$

$= 19^6 \bmod 23$

$= 2$

Bob :

$S = A^b \bmod p$

$= 8^{15} \bmod 23$

$= (8^5)^3 \bmod 23$

$= 16^3 \bmod 23$

$= 2$