Diffie-Hellman revision

Q: $p=7$ $g=5$

Alice	Bob
$a=7$	$b=4$
$A=?$	$B=?$
$s=?$	$s=?$

Solution ① $A = g^a \bmod p$

$= 5^7 \bmod 7$

$= 5$

② $B = g^b \bmod p$

$= 5^4 \bmod 7$

$= 2$

③ For Alice

$s = B^a \bmod p$

$= 2^7 \bmod 7$

$= 2$

④ For Bob

$$S = A^b \bmod p$$

$$= 5^4 \bmod 7$$

$$= 2$$