DH large num revision

Q $p = 353$ $g = 3$

Alice	Bob
$a = 97$	$b = 233$
$A = ?$	$B = ?$
$s = ?$	

Solution ① $A = g^a \bmod p$

$= 3^{97} \bmod 353$

$= (3^8)^{12} \cdot 3 \bmod 353$

$= (207^4)^3 \cdot 3 \bmod 353$

$= 140^3 \cdot 3 \bmod 353$

$= 40$

② $B = g^b \bmod p$

$= 3^{233} \bmod 353$

$= (3^8)^{29} \cdot 3 \bmod 353$

$= 207^{28} \cdot 207 \cdot 3 \bmod 353$

$= (207^4)^7 \times 207 \times 3 \bmod 353$

$= 140^7 \times 207 \times 3 \bmod 353$

$= (140^3)^2 \times 140 \times 207 \times 3 \bmod 353$

$= 131^2 \times 140 \times 207 \times 3 \bmod 353$

$= 248$

③ Alice

$S = B^a \bmod p$

$= 248^{97} \bmod 353$

$= (248^4)^{24} \cdot 248 \bmod 353$

$= (17^6)^4 \cdot 248 \bmod 353$

$= (135)^4 \cdot 248 \bmod 353$

$= 217 \times 248 \bmod 353$

$= 160$

$96 = 2 \times 48$

$= 4 \times 24$

$= 8 \times 12$

$24 = 4 \times 6$

④ Bob

$S = A^b \bmod p$

$= 40^{233} \bmod 353$

$= (40^4)^{58} \cdot 40 \bmod 353$

$= (44^2)^{29} \cdot 40 \bmod 353$

$= (171^4)^7 \times 171 \times 40 \bmod 353$

$= 187^7 \times 171 \times 40 \bmod 353$

$= (187^3)^2 \cdot 187 \times 171 \times 40 \bmod 353$

$= 231^2 \times 187 \times 171 \times 40 \bmod 353$

$= 4 \times 40 \bmod 353$

$= 160$

$233 = 2 \times 116 + 1$

$= 4 \times 58 + 1$

$58 = 2 \times 29$

$29 = 2 \times 14 + 1$

$= 4 \times 7 + 1$