① $q = 11$ | $q = 11$

② $\alpha < q$ and $\boxed{\text{mod } 11}$ | (P.R) primitive root

$2^5 \bmod 11$

$32 \bmod 11$

10

Power →	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
α $\boxed{2}$	2	4	8	5	$\boxed{10}$	9	7	3	6	1
3										
4										
5										
6										
7										
8										
9										
10										

$\alpha = 2$ | $\alpha = 2$

Private key | Private key

③ $X_A < q$ | $X_B < q$

$8 < 11 \Rightarrow X_A = \boxed{8}$ | $4 < q \Rightarrow X_B = \boxed{4}$

④ $Y_A = \alpha^{X_A} \bmod q$ | $Y_B = \alpha^{X_B} \bmod q$

$= 2^8 \bmod 11$ | $= 2^4 \bmod 11$

$= 256 \bmod 11$ | $= 16 \bmod 11$

$Y_A = 3$ | $Y_B = 5$

$\boxed{Y_B = 5}$ | $\boxed{Y_A = 3}$

$K = Y_B^{X_A} \bmod q$ | $K = Y_A^{X_B} \bmod q$

$= 5^8 \bmod 11$ | $= 3^4 \bmod 11$

$K = 4$ | $K = 4$