4.3.3.5 Example 3

Q : $q = 97$, $a = 5$

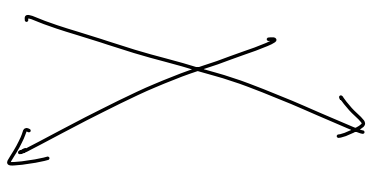
$X_A = 36$, $X_B = 58$

$y = a^x \bmod q$

Solution

$5^{36} \bmod 97 = 50$

$5^{58} \bmod 97 = 44$



$44^{36} \bmod 97 = 44$

$50^{58} \bmod 97 = 75$