

4.3.3.7 Example 5

$$Q : q = 47, a = 5$$

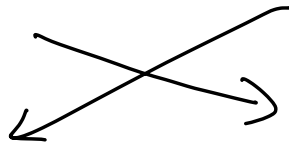
$$X_A = 18, X_B = 22$$

$$y = a^x \text{ MOD } q$$

Solution

$$5^{18} \text{ mod } 47 = 2$$

$$5^{22} \text{ mod } 47 = 28$$



$$28^{18} \text{ mod } 47 = 24$$

$$2^{22} \text{ mod } 47 = 24$$