4.3.3.7 Example 5

Q : $q=47$, $a=5$ $\qquad y = a^{x} \text{ MOD } q$

$X_A=18$, $X_B=22$

Solution

$$\begin{tikzcd}
5^{18} \bmod 47 = 2 \arrow[dr] & 5^{22} \bmod 47 = 28 \arrow[dl] \\
28^{18} \bmod 47 = 24 & 2^{22} \bmod 47 = 24
\end{tikzcd}$$