

7.2.1 Diffie - Hellman Example

$$Q: p = 23 \quad g = 5$$

Alice Bob

$$a = 6 \quad b = 15$$

$$(a) A = ? \quad (b) B = ?$$

$$(c) S = ?$$

$$\begin{aligned}\text{Solution (a)} \quad A &= g^a \bmod p \\ &= 5^6 \bmod 23 \\ &= 8\end{aligned}$$

$$\begin{aligned}\text{(b)} \quad B &= g^b \bmod p \\ &= 5^{15} \bmod 23 \\ &= (5^5)^3 \bmod 23 \\ &= (3125)^3 \bmod 23 \\ &= 20^3 \bmod 23 \\ &= 19\end{aligned}$$

③ Alice :

$$\begin{aligned}S &= B^a \bmod p \\ &= 19^6 \bmod 23 \\ &= 2\end{aligned}$$

Bob :

$$\begin{aligned}S &= A^b \bmod p \\ &= 8^{15} \bmod 23\end{aligned}$$

$$= (8^5)^3 \bmod 23$$

$$= 16^3 \bmod 23$$

$$= 2$$