

Diffie-Hellman Key Exchange

Public parameters: p (a prime number), q (a base).

Step 1:

Client side:

generate secret a

$$A = g^a \bmod p$$

A will be shared to the server

Server side:

generate secret b

$$B = g^b \bmod p$$

B will be shared to the client

Step 2:

Client side:

$$\begin{aligned} SK &= B^a \bmod p \\ &= ((g^b) \bmod p)^a \bmod p \\ &= g^{ab} \bmod p \end{aligned}$$

Server side:

$$\begin{aligned} SK &= A^b \bmod p \\ &= ((g^a) \bmod p)^b \bmod p \\ &= g^{ab} \bmod p \end{aligned}$$

Proof of $(m \bmod p)^n \bmod p = m^n \bmod p$:

$$\text{let } m = ap + b, b < p$$

$$(m \bmod p)^n \bmod p = [(ap + b) \bmod p]^n \bmod p = b^n \bmod p$$

$$m^n \bmod p = (ap + b)^n \bmod p$$

$$= [(ap + b) \times (ap + b) \times \dots \times (ap + b)] \bmod p$$

n times

$$= [(a^2 p^2 + apb + apb + b^2) \times (ap + b) \times \dots \times (ap + b)] \bmod p$$

$n-1$ times

$$= b^n \bmod p$$

$$\therefore (m \bmod p)^n \bmod p = m^n \bmod p$$