Diffie-Hellman Key Exchange

Songyue Wang (sywang@cs.hku.hk)

Adopted from Dr. Allen M.H. Au lecture notes for HKU FITE3012

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

Step 1:

Client side:

$$\text{generate secret } a$$
$$A = g^a \bmod p$$
$$A \text{ will be shared to the server}$$

Server side:

$$\text{generate secret } b$$
$$B = g^b \bmod p$$
$$B \text{ will be shared to the client}$$

Step 2:

Client side:

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

Server side:

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

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

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

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

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

$= [(ap+b) \times \underbrace{(ap+b)}_{n \text{ times}} \times \ldots \times (ap+b)] \bmod p$

$= [(a^2p^2 + apb + apb + b^2) \times \underbrace{(ap+b) \times \ldots \times (ap+b)}_{n-1 \text{ times}}] \bmod p = b^n \bmod p$

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