Diffie-Hellman Key Exchange

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

Step 1:

Client side:



Server side:



Step 2:

Client side:



Server side:



Proof of :

