Diffie-Hellman Key Agreement

Diffie-Hellman protocol allows two communicating parties, say Alice and Bob, to create a symmetric session key with out the need of a KDC (Key Distribution Center)

Diffie-Hellman Protocol

Alice and Bob chose two numbers p and g which are public.
‘p’ is a large prime of the order of 1024 bits. ‘g’ is a generator of order p-1 in the group Z_p^*

Alice chooses a large random number ‘x’ in the range 0 to p-1 and calculates R1 = g^x mod p

Bob chooses a large random number ‘y’ in the range 0 to p-1 and calculates R2 = g^y mod p

Alice sends R1 to Bob and Bob sends R2 to Alice

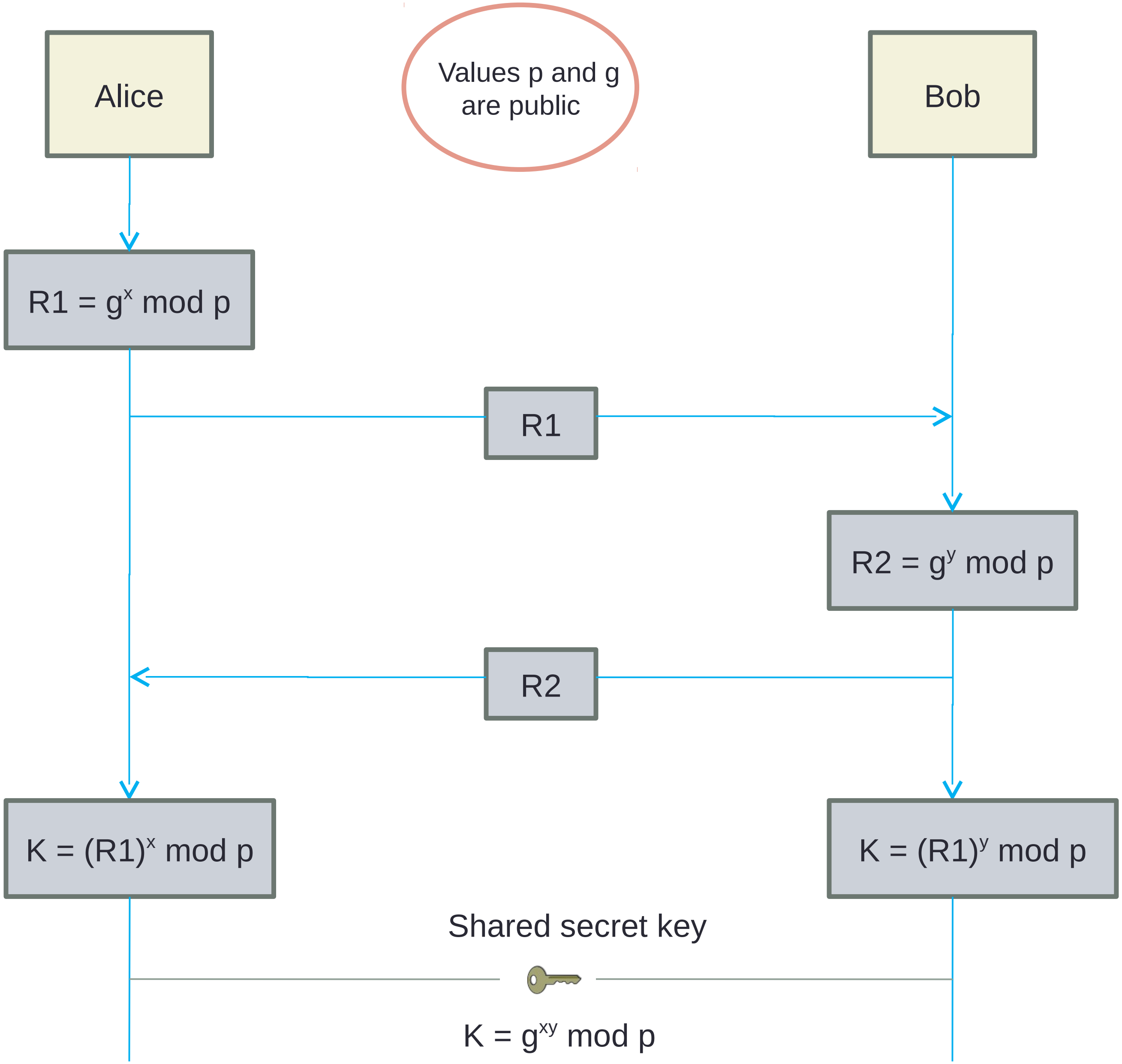
Alice Calculates K = $(R2)^x$ mod p

Bob Calculates K = $(R1)^y$ mod p

$$K = (g^x \text{ mod } p)^y \text{ mod } p = (g^y \text{mod } p)^x \text{ mod } p = g^{xy} \text{ mod } p$$

K is the symmetric key for the session

Diffie-Hellman Key Agreement



Alice

Values p and g are public

Bob

R1 = g^x mod p

R1

R2 = g^y mod p

R2

K = $(R1)^x$ mod p

K = $(R1)^y$ mod p

Shared secret key

K = g^{xy} mod p

P is a large prime of the order of 1024 bits

g is a generator of order p-1 in the group Zp*