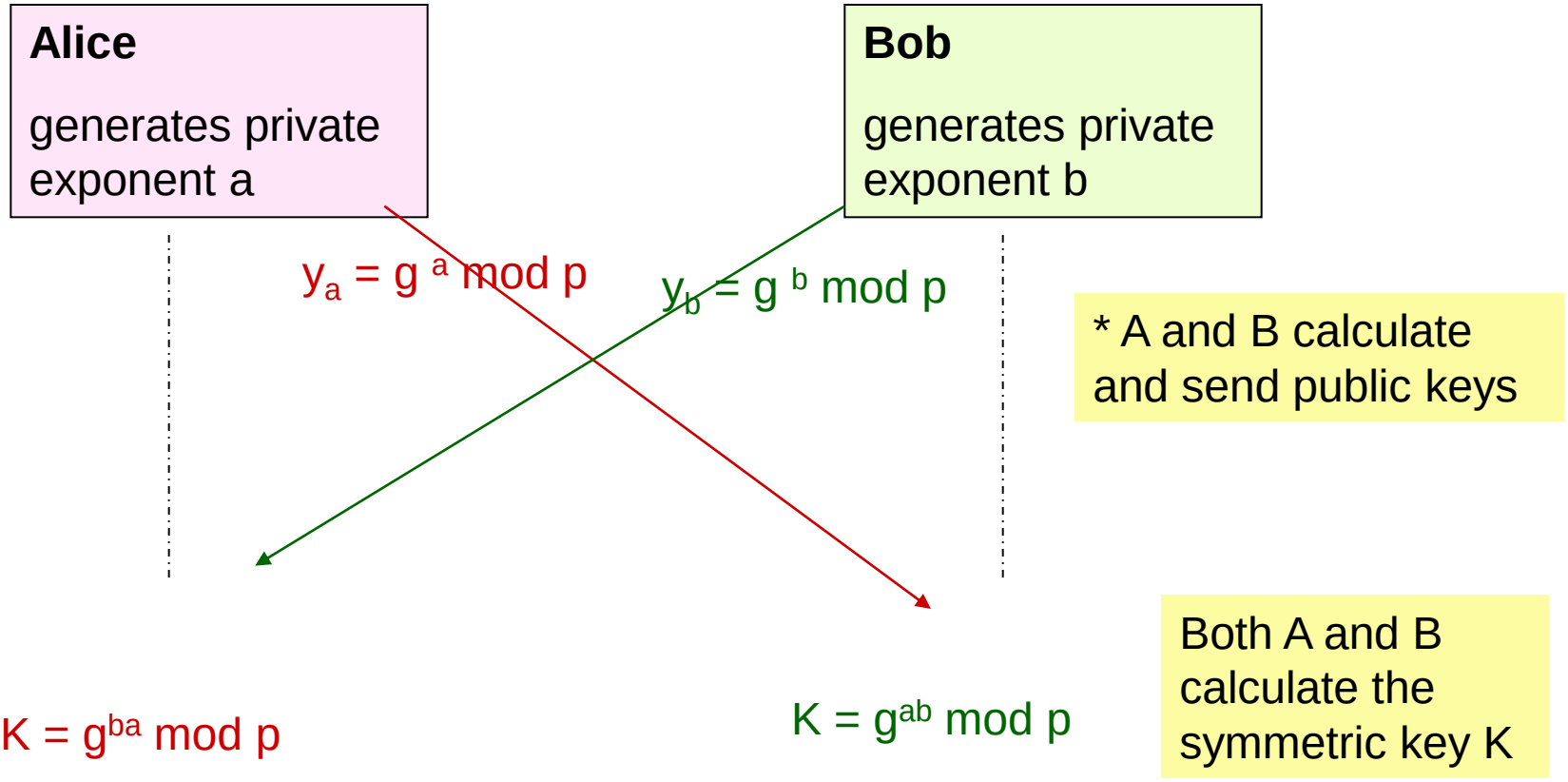
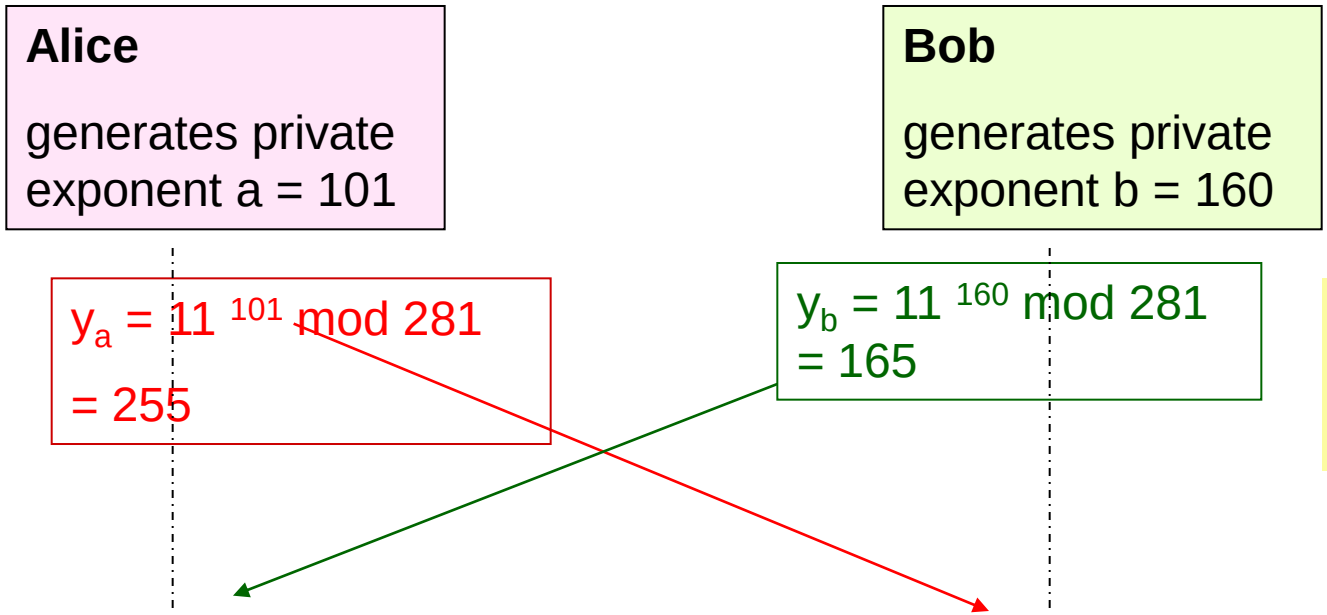
Diffie – Hellman key exchange

Prime p and a generator g are given



Diffie – Hellman example

Prime p = 281 and generator g = 11



* A and B send public keys

$K = 165^{101} \bmod 281 = 59$

$K = 255^{160} \bmod 281 = 59$

Both A and B calculate the symmetric key K

DH security

If modulus p is sufficiently large (> 1024 bits), then the enemy listening to the channel cannot calculate the private keys a and b even if they see the powers g^a and g^b mod p.

This is because solving exponent from g^x mod p = y is one of the hard problems in mathematics. It is called Discrete Logarithm Problem, DLP.