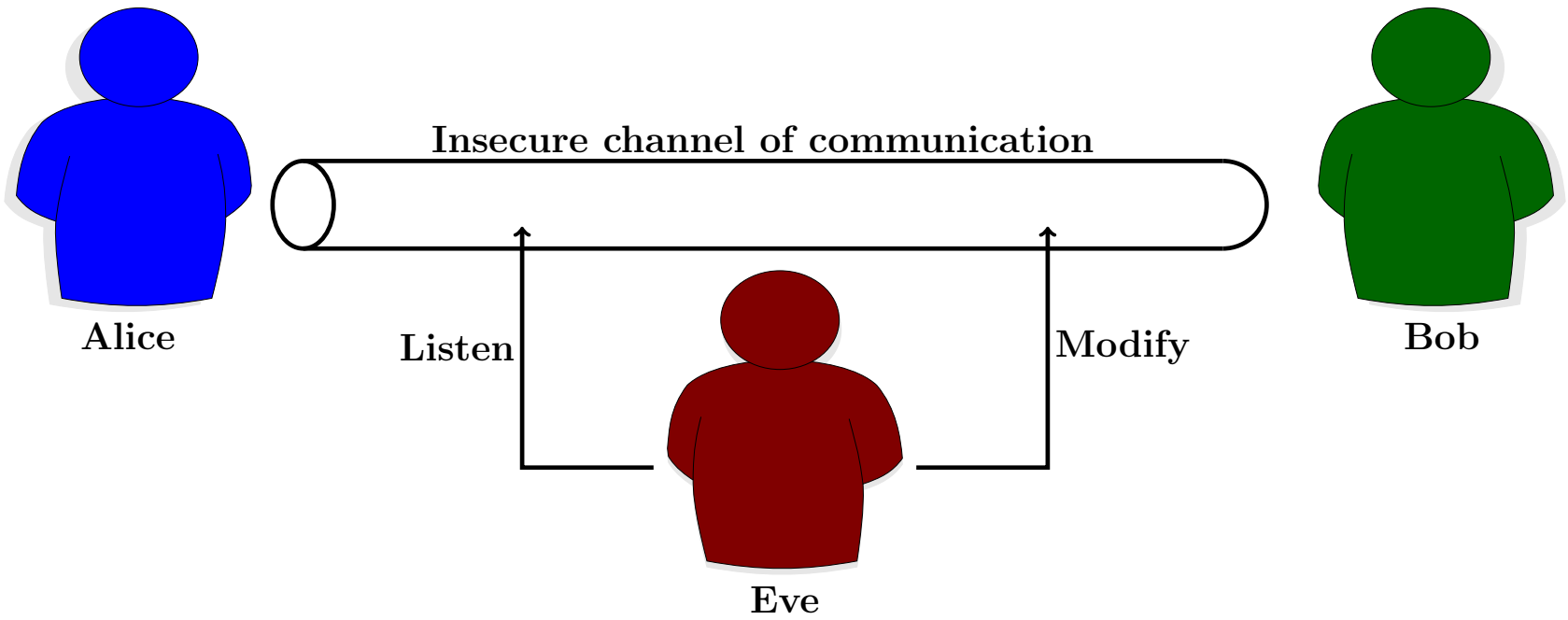
# Secure Key Exchange

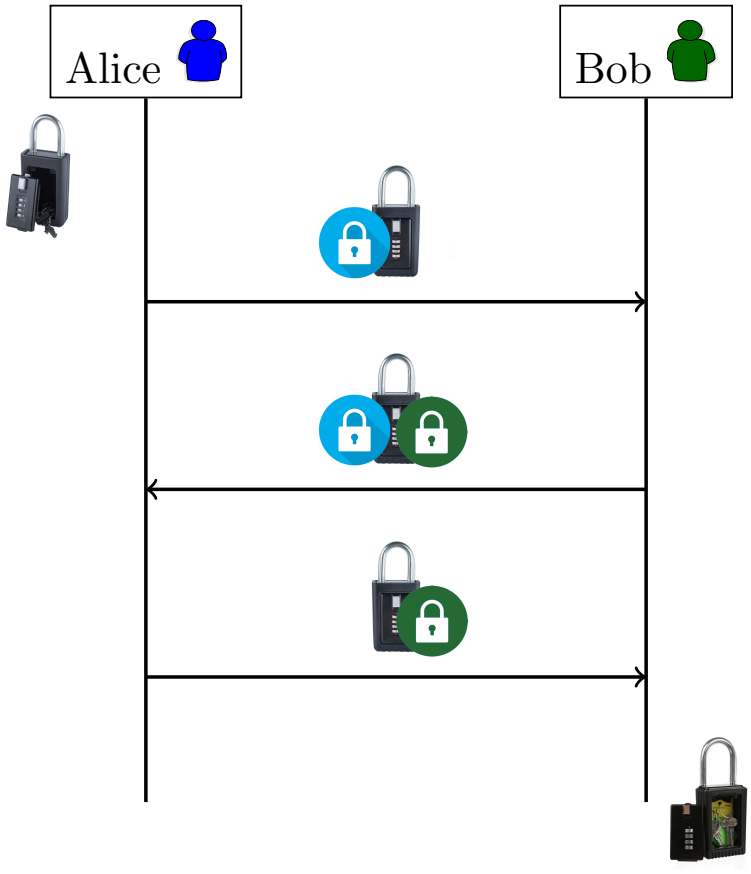
# The problem

Alice and Bob need to agree on a secret key.



# MultiRound Solution

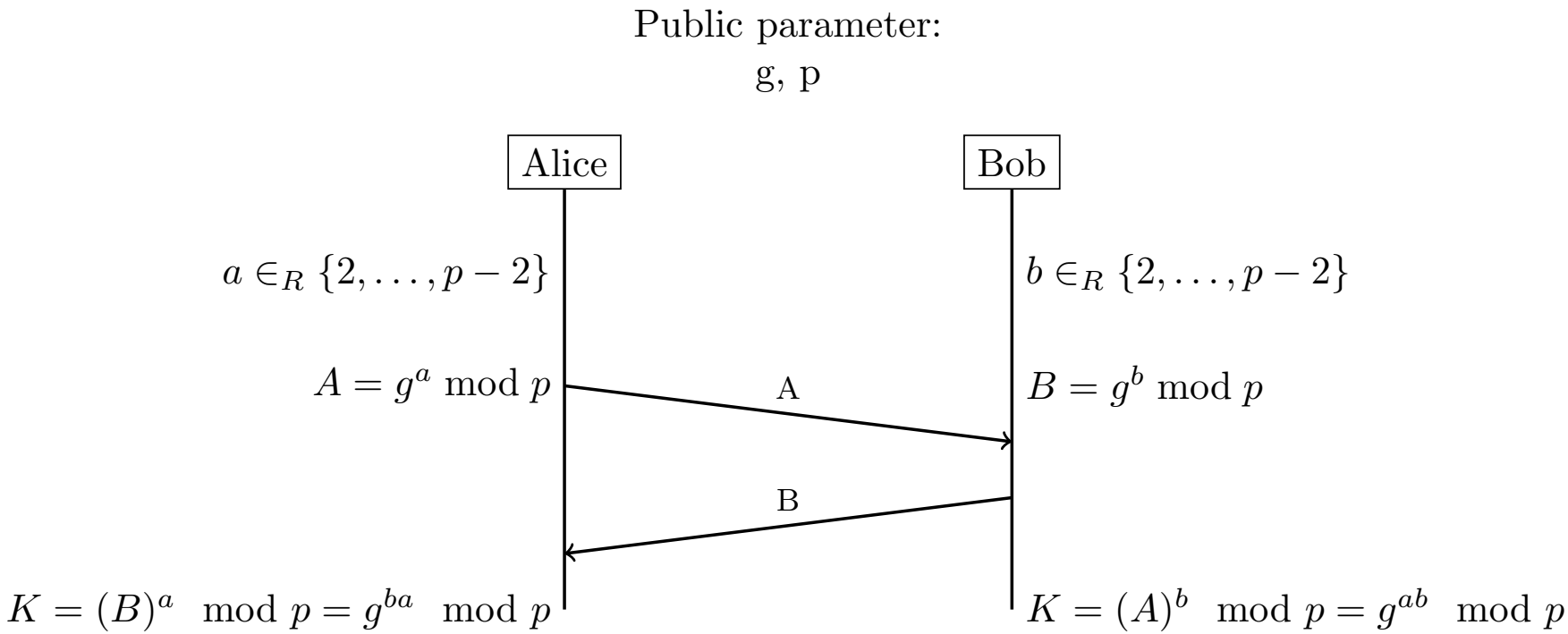
Public parameter:two sided lock box



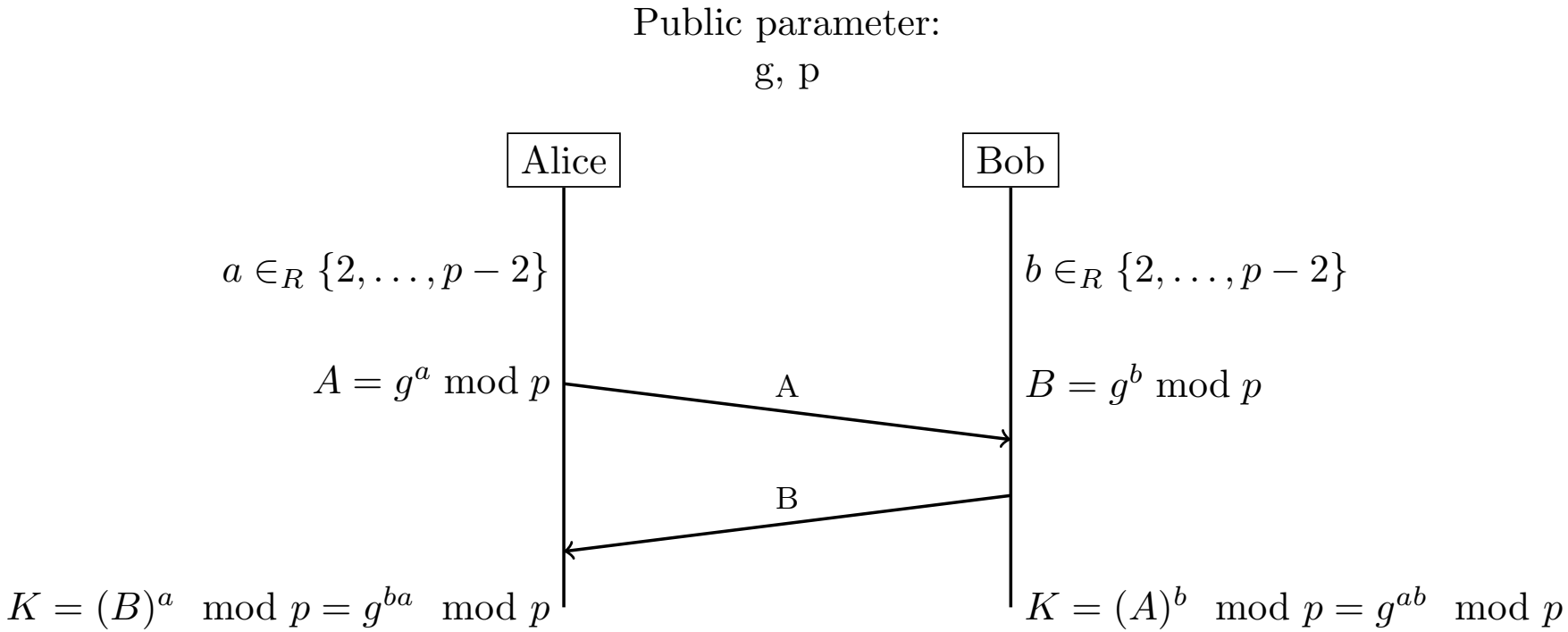
# Diffie Hellman Key Exchange

## Parameters

Choose a prime $p$ and a number $g < p$ such that $gcd(g, p-1) = 1$.



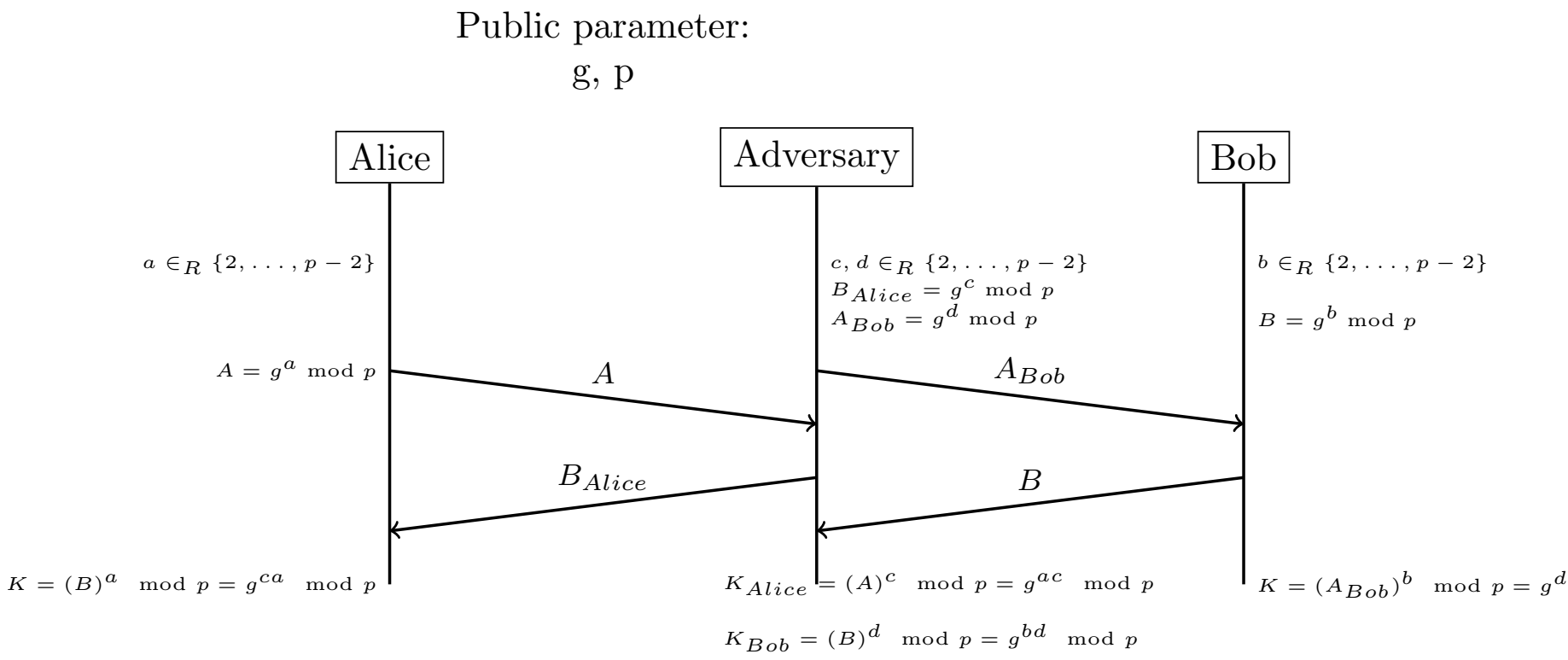
# Diffie Hellman Key Exchange




## Diffie-Hellman Assumption

There is no polynomial time algorithm to compute $g^{ab} \bmod p$ from $g^a \bmod p$ and $g^b \bmod p$.

# Man-in-the-Middle Attack



# Man-in-the-Middle Attack: How to Solve?

Basic Idea: Authenticating Public Key.

Requirement: Trusted Third Party: Certification Authority (CA).