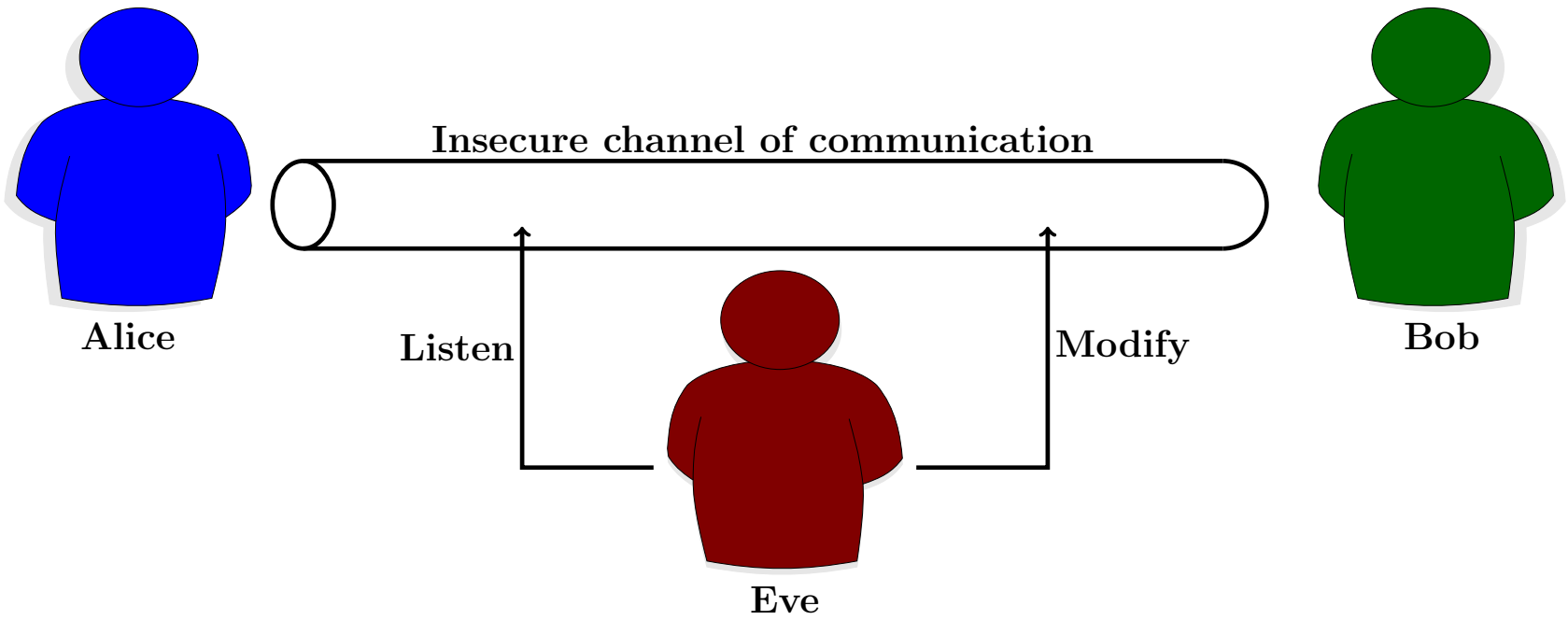
# Secure Key Exchange

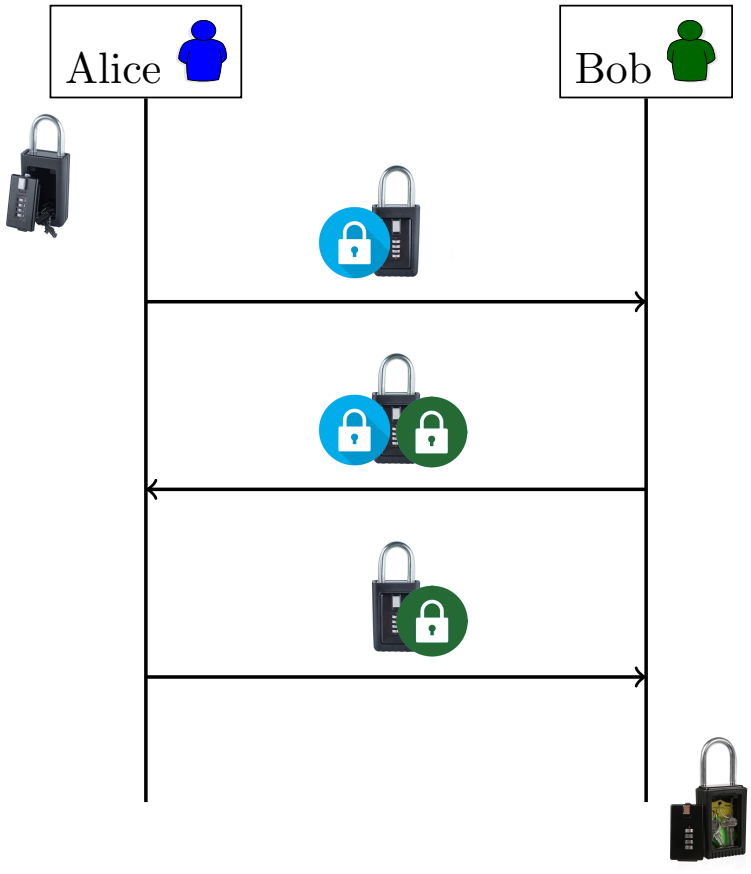
# The problem

Alice and Bob need to agree on a secret key.



# MultiRound Solution

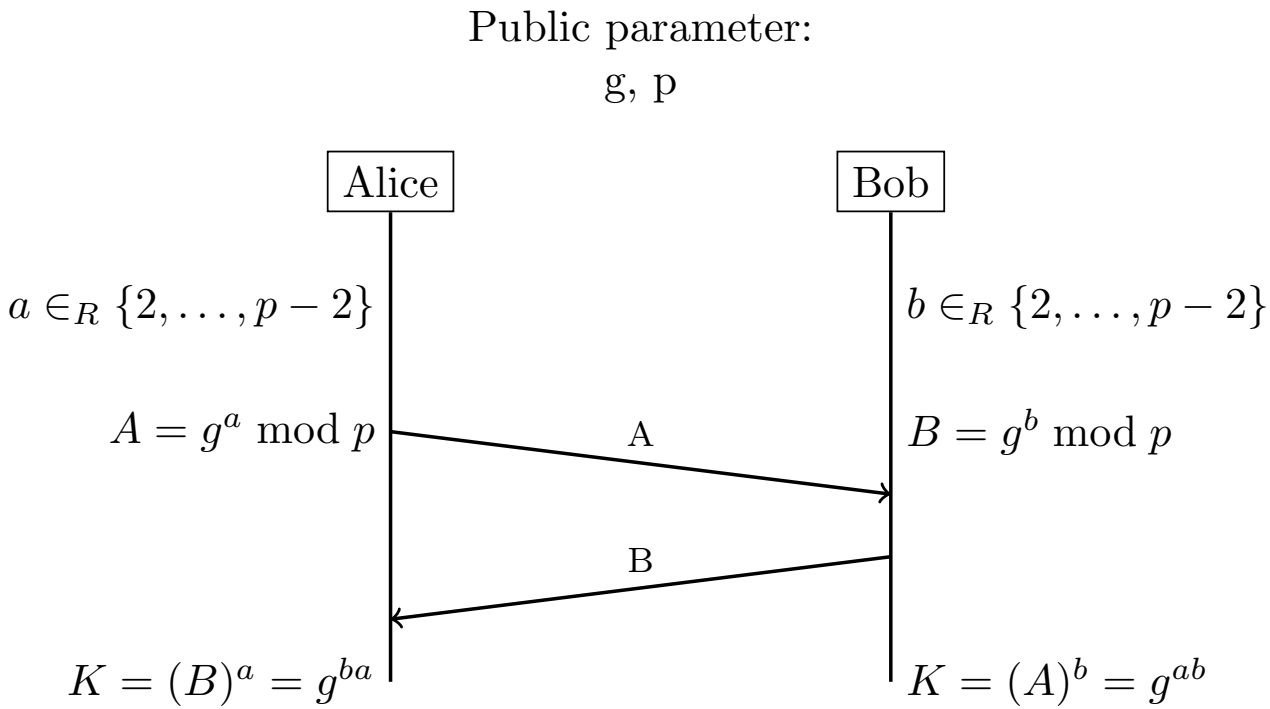
Public parameter:two sided lock box



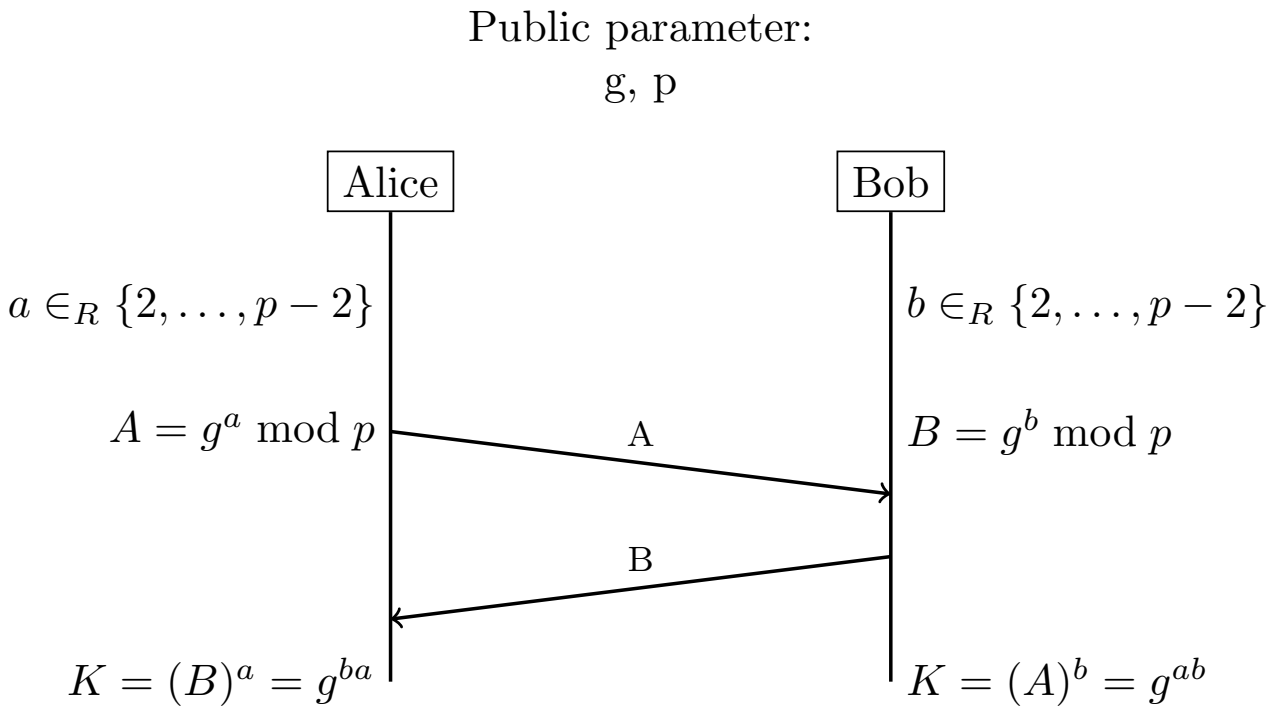
# Diffie Hellman Key Exchange

## Parameters

Prime number $p$, Primitive Root $g$
$(\{g^a \text{mod} p\}_{a \in \mathbb{N}} = \{1, \ldots, p-1\})$



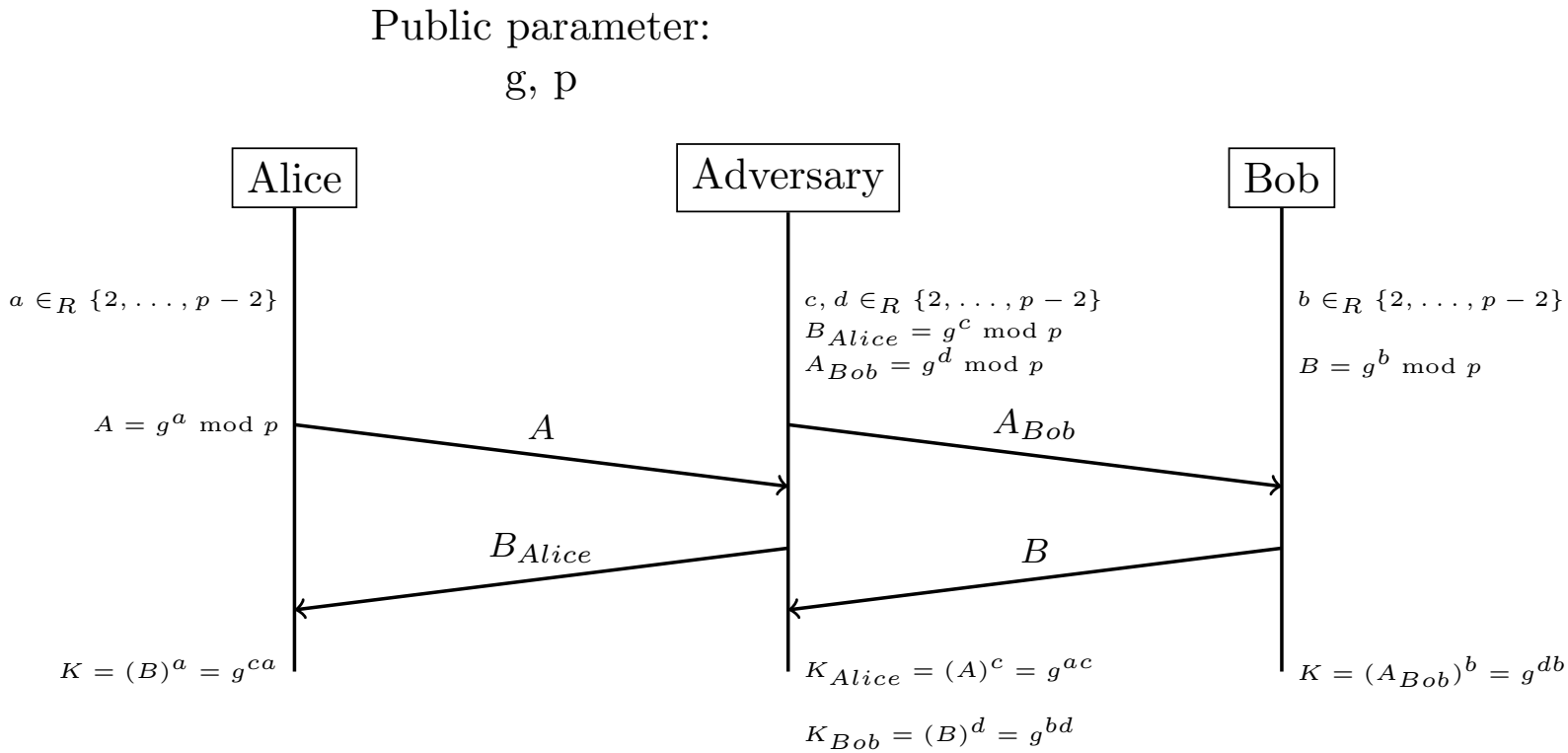
# Diffie Hellman Key Exchange




## Diffie-Hellman Assumption over $\mathbb{Z}_p$

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

# 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).