

Alice



private **a**



public **A**



a, B \rightarrow K

Eve



A



B



send at the same time

Bob



private **b**



public **B**



b, A \rightarrow K