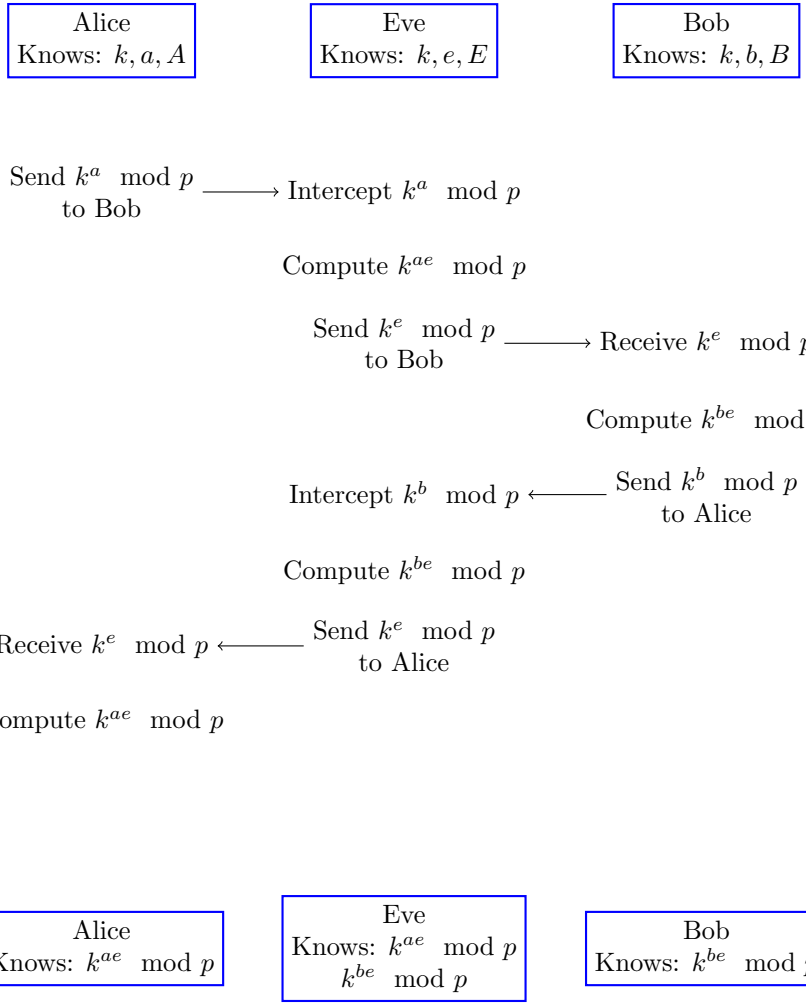
Alice
Knows: k, a, A
Eve
Knows: k, e, E
Bob
Knows: k, b, B
Send $k^a \mod p$ to Bob
Intercept $k^a \mod p$
Compute $k^{ae} \mod p$
Send $k^e \mod p$ to Bob
Receive $k^e \mod p$
Compute $k^{be} \mod p$
Intercept $k^b \mod p$
Send $k^b \mod p$ to Alice
Compute $k^{be} \mod p$
Receive $k^e \mod p$
Send $k^e \mod p$ to Alice
Compute $k^{ae} \mod p$
Alice
Knows: $k^{ae} \mod p$
Eve
Knows: $k^{ae} \mod p$
$k^{be} \mod p$
Bob
Knows: $k^{be} \mod p$