Diffie-Hellman key Exchange

What if no shared key to start with?

\[ \begin{align*}
& \text{Alice} \quad A = g^a \\
& \quad \text{Bob} \quad B = g^b \\
& \text{U} \quad \text{sees } A, B,
\end{align*} \]

Goal: Alice and Bob get a shared key, \( K \), \( U \) has no information about \( K \), even seeing all comms between them.

\[ B^a = (g^b)^a = g^{ab} = (g^a)^b = A \]

\( K = g^{ab} \)

- IF CDH is hard, \( U \) cannot sample \( K \) given \( A, B \).
- IF DDH is hard, \( U \) cannot distinguish \( K \) from a random group element.

Once Alice, Bob have a shared secret, can use it for MAC, sym. encryption, etc.