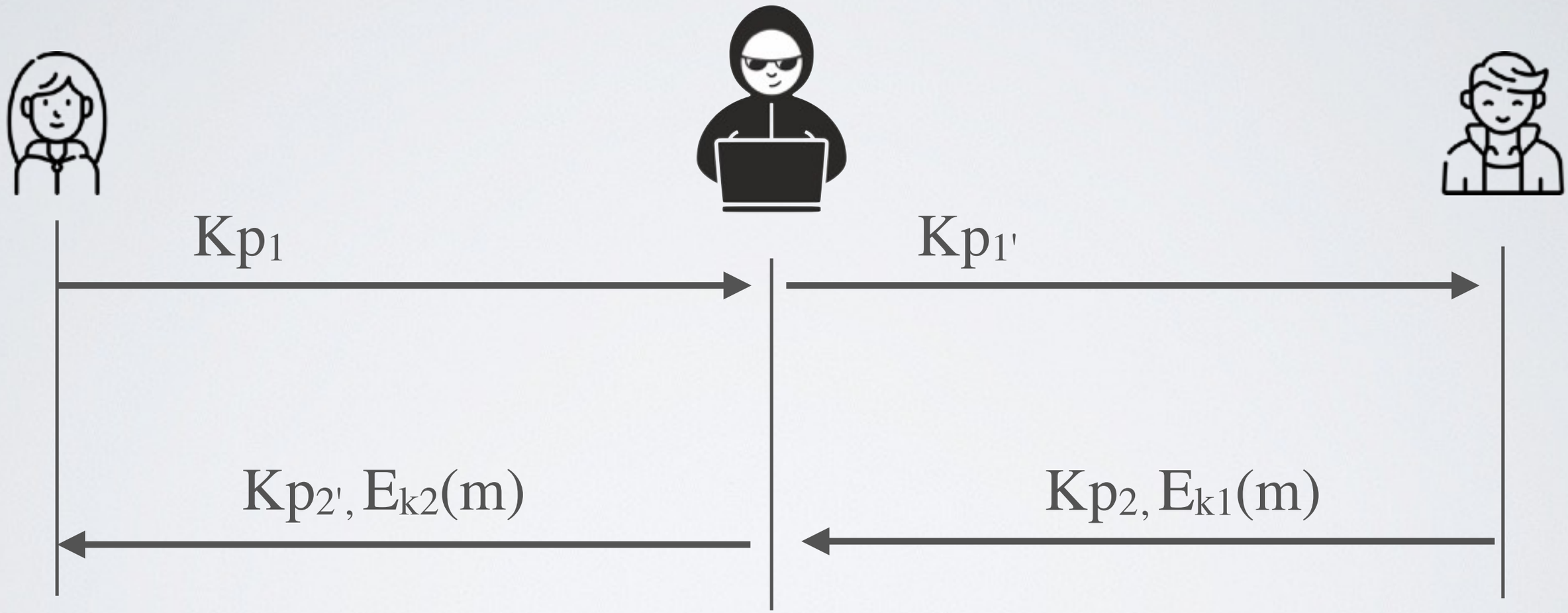
The key exchange is not authenticated



Key Derivation with Authenticated Short-Term Keys