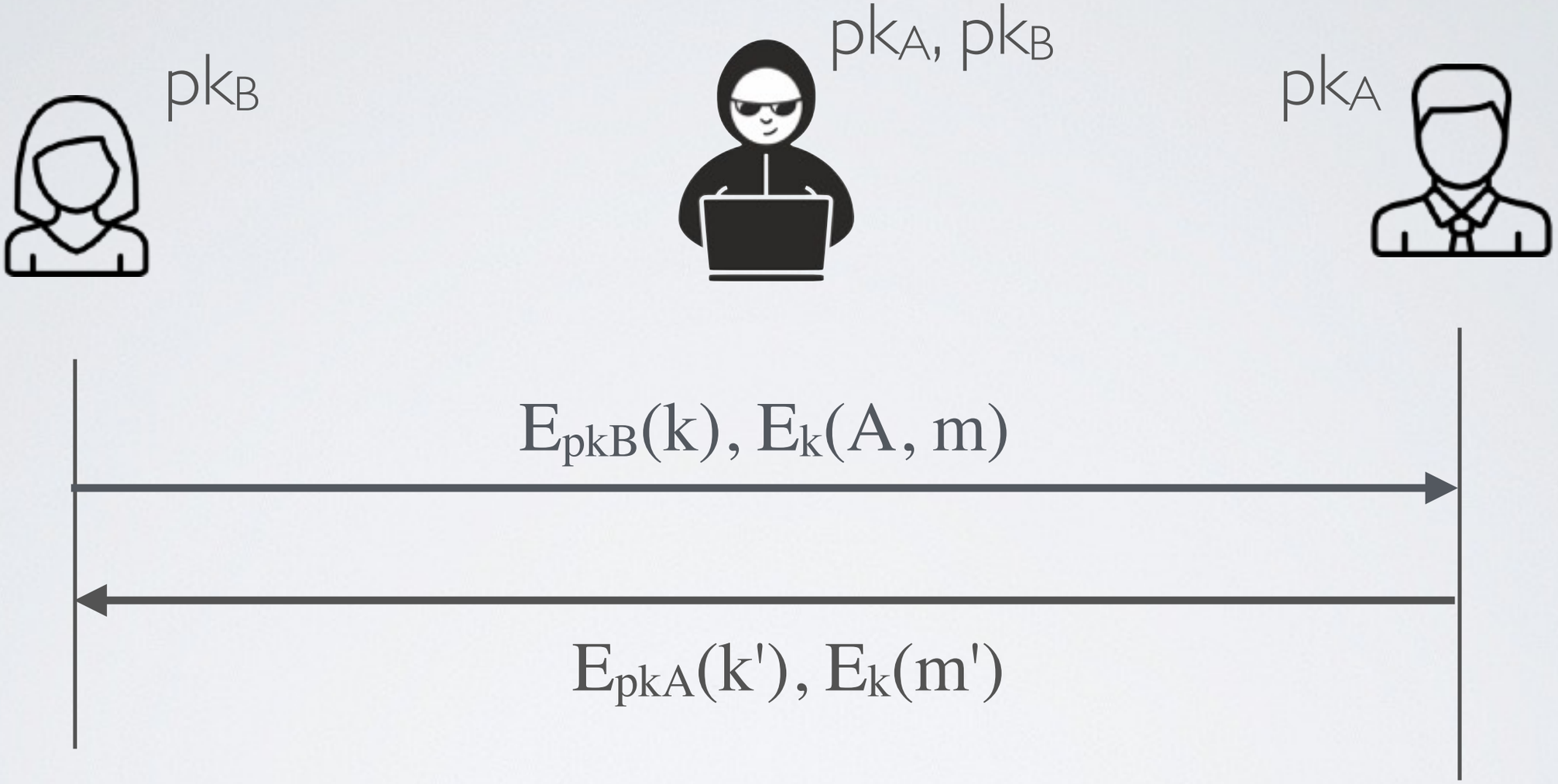
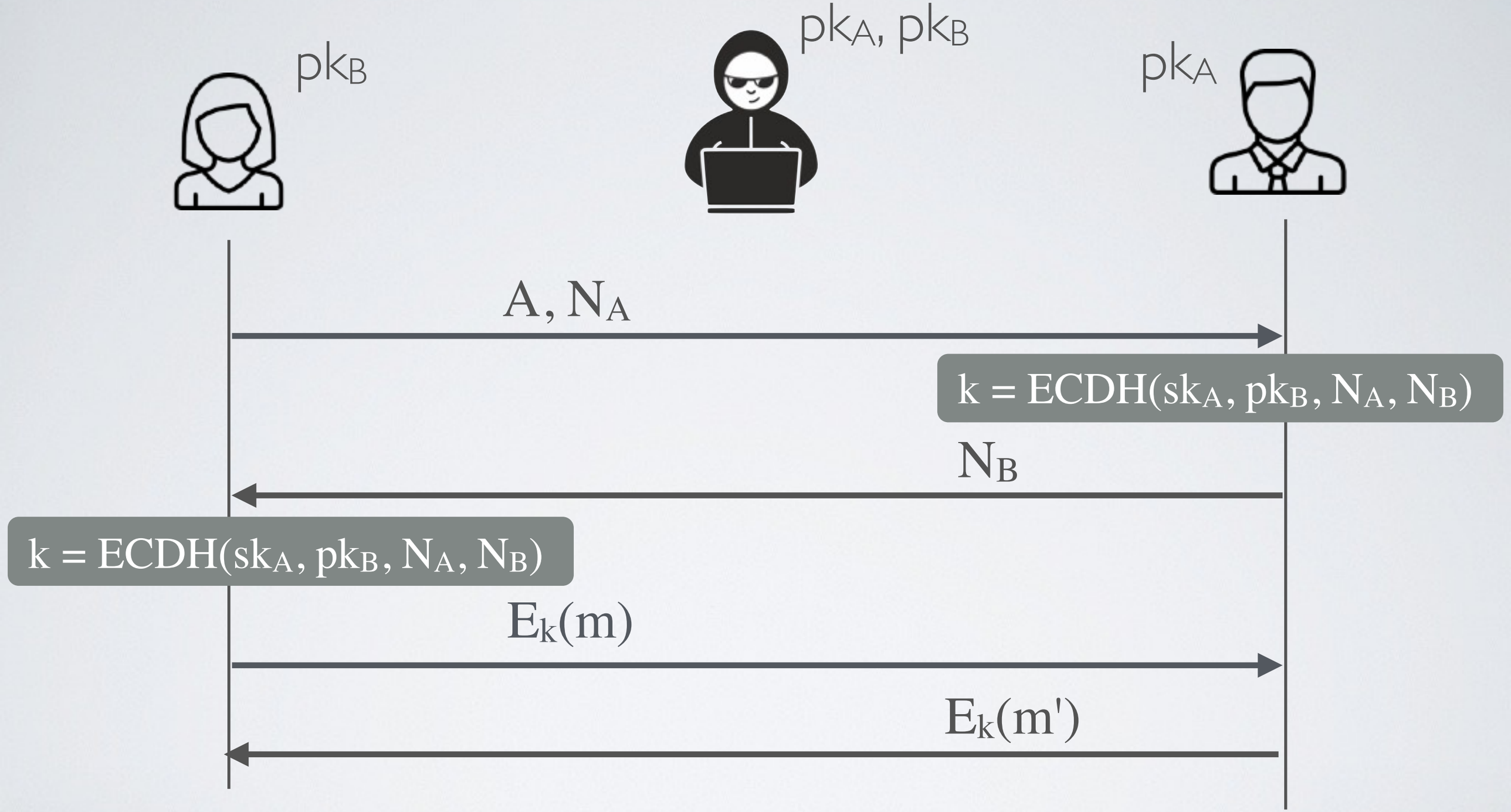
[broken] Key Wrapping



- Replay attack
- No Forward Secrecy
- Bad Authentication

[broken] Key Derivation using Long-Term Keys



- No Forward Secrecy