A widely used key exchange protocol

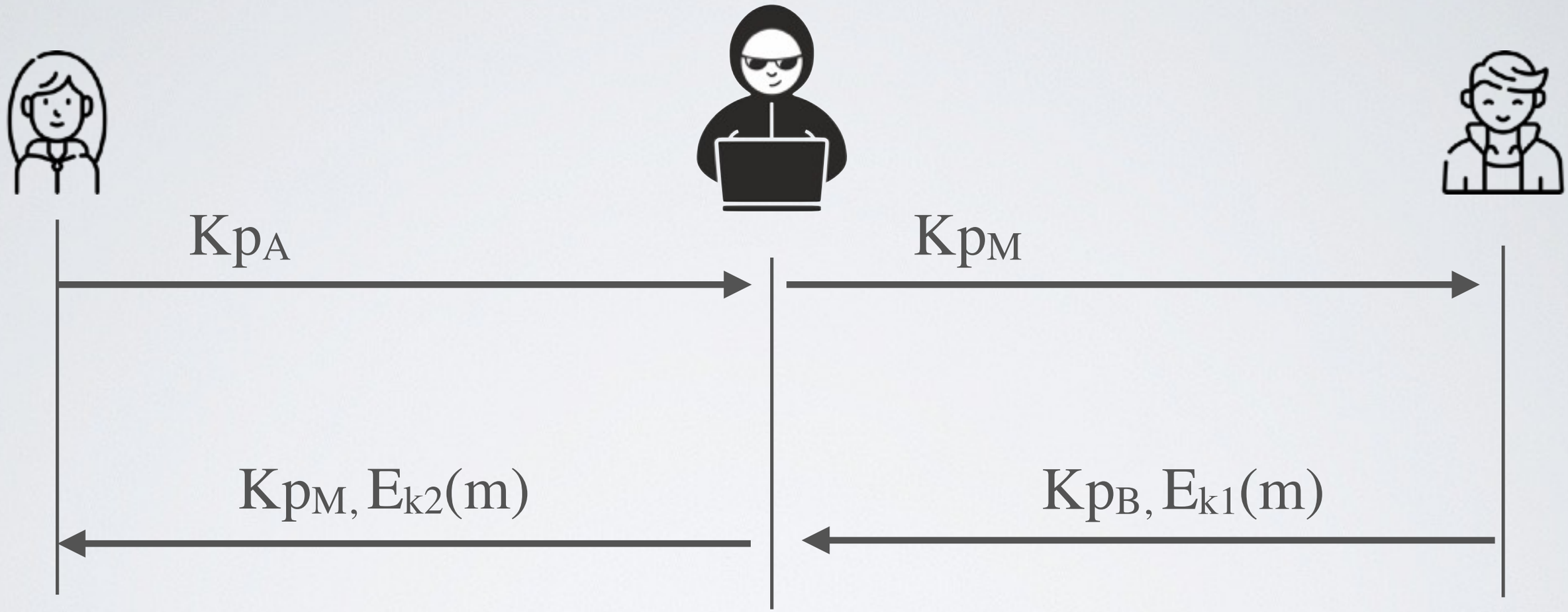
ECDH is in many protocols

- SSH
- TLS (used by HTTPS)
- Signal (used by most messaging apps like Whatsapp)
- and so on …

✓ It is fast and requires two exchanges only

◉ But how to make sure Alice is talking to Bob and vice-versa? Diffie-Hellman-Merkle alone **does not ensure authentication**

Are we done yet?



- ✓ Encryption and key exchange protects against confidentiality ...
- ◉ ... but not **does not protect integrity**