Key Exchange (KX)

faster than with asymmetric techniques

authentication, confidentiality, preserving the order of messages...

2 or more parties want to agree on a symmetric-key which they want to use for secure communication.
We formulate key exchange goals in terms of what we want from the symmetric session key, but we need to remember that these security property are then inherited for the subsequent secure communication.

Example applications:

Accessing a web-page

2 parties:
- Server (hosting the website), has some public key
- Client (visiting the website), anonymous

Goal:
The client should get the guarantees that the symmetric session key is only shared with the server hosting the webpage.

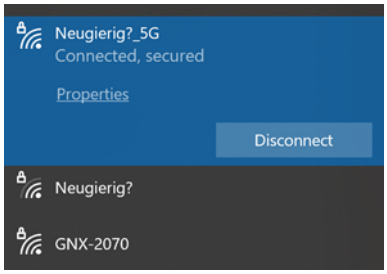
Protocol-type:
One-sided authenticated key exchange based on public-keys

Real-Life Protocol:
Transport Layer Security (TLS)

Note (tangent): TLS also has 2-sided authenticated modes as well as modes that authenticate via symmetric-keys

https://datatracker.ietf.org/doc/html/rfc8446

Connecting to a WLAN



2 parties:
- WLAN router
- User

= knows the password

Goals:
- The WLAN router should get confirmation that user is authorized to use WLAN.
- The user should be sure that the symmetric session-key is only shared with the WLAN router.

Is this possible? What does this tell us about WLAN connections?

Protocol-type:
2-sided password-authenticated key exchange (PAKE)

Real-life protocol:
IEEE 802.11-2012 for authentication between wireless devices
(sometimes also called WPA3)

End-to-end-encrypted messaging

2 parties (or more)

Goals:
- All users should be sure that the symmetric session-key is only shared with the intended partners.

Protocol-type
- Public-key based authenticated key exchange (2 parties)
- Public-key based authenticated group key exchange (> 2 parties)

Real-life protocols are implemented in various messaging app. An important question is whether the apps allow out-of-band verification of the link between a user name / phone number on the one hand and a public-key, e.g. via the scanning of a QR code.

Advanced Goals:
- Long-term sessions with key updates and dynamic groups (adds, removes)
- Forward-secrecy
- Post-compromise security

Real-life protocol:
Messaging Layer Security (MLS)
https://datatracker.ietf.org/doc/rfc9420/
1-minute introduction by myself: https://www.youtube.com/watch?v=YkDSmuq8_RU