

A widely used key exchange protocol

Diffie-Hellman-Merkle 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
- ✓ Solves the problem of having a key distribution server
- ✓ Ensures Perfect Forward Secrecy

- ⦿ But how to make sure Alice is talking to Bob and vice-versa?

Diffie-Hellman-Merkle alone **does not ensure authentication**

