Diffie-Hellman-Merkle in practice

- $\mathbf{g}$ is small (either 3, 5 or 7 and fixed in practice)
- $\mathbf{p}$ is at least 2048 bits (and fixed in practice)
- private keys $\mathbf{a}$ and $\mathbf{b}$ are 2048 bits as well

➡ So the public values $\mathbf{A}$ and $\mathbf{B}$
and the master key $\mathbf{k}$ are 2048 bits

➡ Use $\mathbf{k}$ to derive an AES key using a Key Derivation Function
(usually HKDF - the HMAC-based Extract-and-Expand key derivation function)

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**