

Asymmetric Protocols

Thierry Sans

Goals

1. Establish a session key to exchange data while ensuring Perfect Forward Secrecy
 - ✓ Use the Diffie-Hellman key exchange protocol
2. Ensure one-way or mutual authentication
 - ✓ Use asymmetric encryption