Key voor symmetrische encryptie uitwisselen zonder eavesdroppers het kunnen horen

Methoden

1. Out of band: fysiek key afgeven irl
2. Reuse previous keys
3. Assymetric encryption
4. Diffie hellman
5. Trusted third party

# Diffie hellman

* Op basis primitieve wortels.
* Shared key delen zonder anderen het kunnen horen
* Wiskunde algo zie slides
* DDOS aanvallen hierbij nodig
* Man in the middle mogelijk

# KDC

# Assymetric

Public key uitwisselen:

**Public announcement**: broadcasten van public keys.   
-: mogelijkheid forgery  
**publiek beschikbare directory**: {name,pub key} entries van meerdere partijen. Identiteit moet bij die directory bewezen worden om data om te halen --> iets extra beveiliging  
**public key authority**: third party beheert de public keys van gebruikers

# PKI

* Keys uitwisselen via certificaten
* Signed door vertrouwde third party
* Identiteit van een persoon via public key is gegarandeerd

....

# X.509