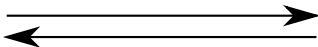


Client A

Server A



1. Get passphrase encrypted and verified public RSA key of user B from server



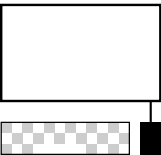
2. Encrypt&sign message and send back to server



3. Message is send to server of user B

Server B

Client B



4. User B can decrypt message with private key

