150 Jahre culture of excellence

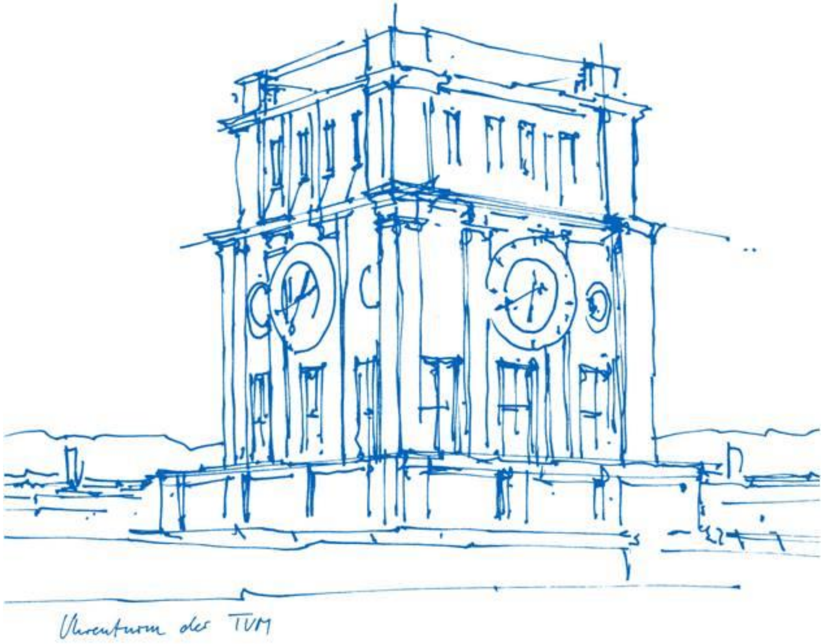
Assignment 2 Specification

Fabian Sauter, Kilian Traub, Atakan Yenel

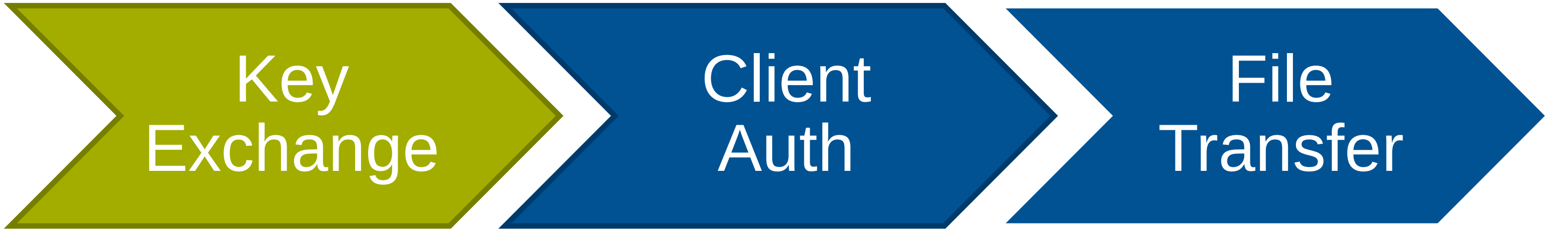
Group 5

Technische Universität München

Garching, 12.06.2018



Key Exchange



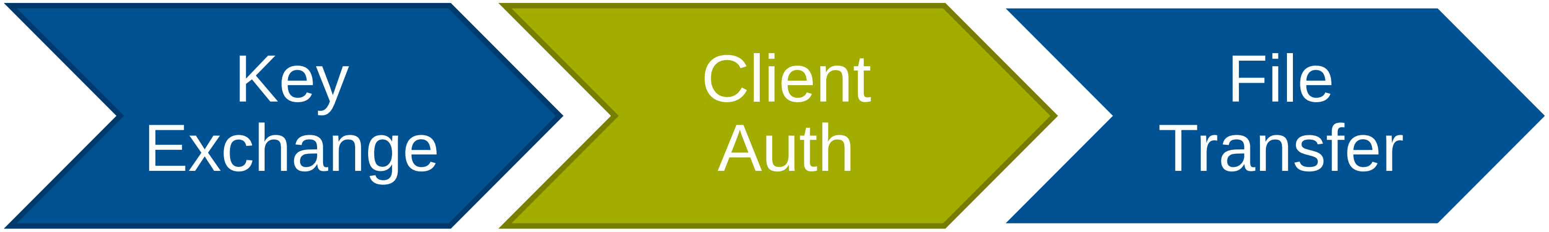
Client-Hello-Handshake

```
0      4       8      24          56             88              120      152
+------+-------+------+-----------+--------------+----------------+---------+
| Type | Flags | Port | Client ID | Prime Number | Primitive Root | Pub Key |
+------+-------+------+-----------+--------------+----------------+---------+
152        184               216        1000
+----------+-----------------+----------+--------+
| Checksum | Username Length | Username | UNUSED |
+----------+-----------------+----------+--------+
```

Server-Hello-Handshake

```
0      4       8           40                72            88        120        152
+------+-------+-----------+-----------------+-------------+---------+----------+
| Type | Flags | Client ID | Sequence Number | Upload-port | Pub Key | Checksum |
+------+-------+-----------+-----------------+-------------+---------+----------+
```

Client Auth



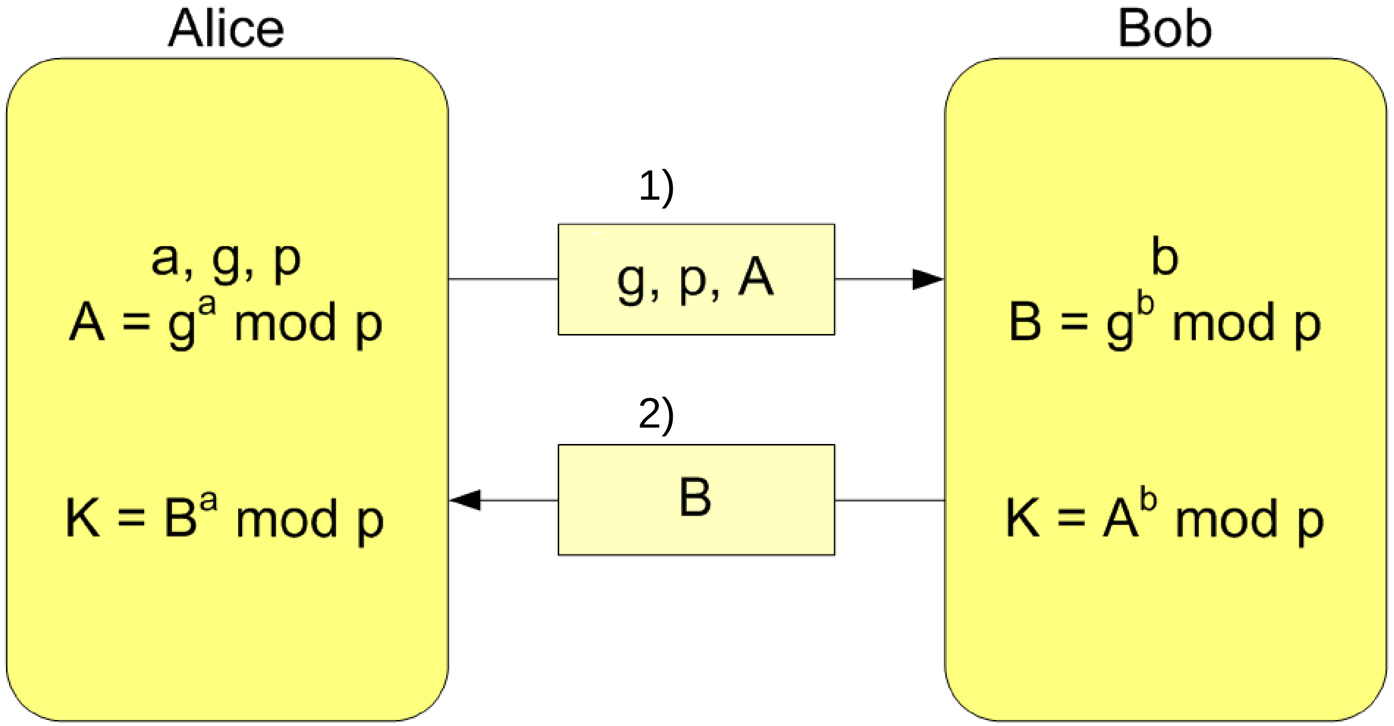
Auth-Request

```
0      4        8          40                                       72         104
+------+--------+-----------+----------------------------------------+----------+
| Type | UNUSED | Client ID | Server-Hello-Handshake Sequence Number | Checksum |
+------+--------+-----------+----------------------------------------+----------+
104               136
+-----------------+----------+
| Password Length | Password |
+-----------------+----------+
```

Auth-Result

```
0      4       8          40                            72         104
+------+-------+-----------+------------------------------+----------+
| Type | Flags | Client ID | Auth-Request Sequence Number | Checksum |
+------+-------+-----------+------------------------------+----------+
```

Diffie-Hellman Key Exchange



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

1) DiffieHellman::clientStartConnection();
2) DiffieHellman::onServerReceive(G,P,A);

Delta Sync - Client

Looks for changed hashes of files:

Changed hash:

- ❑ Calcs CRC32 of every 900 byte blocks
    - If CRC32 block changed compared to the previous run
        - ➢ Part gets marked for transmission
        - ➢ CRC32 get’s updated
    - If CRC32 is the same, compare all the other blocks
        - ➢ Update MD5

Delta Sync - Server

On file got changed by client:

- □ Server notes where changed and from who
- □ Server sends changes to all connected clients