**Kerberos v Authentication**

- **C** = Client Principal
- **α** = Client Address
- **K_c** = Hashed Client Password
- **auth** = Authentication Server (one)
- **Tgs** = Ticket-Granting Server (multiple)
- **K_{tgs}** = Hashed tgs Password
- **s** = Server (many)
- **K_s** = Hashed Server Password

**t** = Current Time

- **K_c, tgs** = Session key between C and Tgs
- **K_c, s** = Session key between C and s

**Protocol Overview**

1. **Data**
   - **C**
   - **auth**

2. **Tgs**
   - **1**

3. **Tgs**
   - **3**

4. **S**
   - **4**

5. **C**
   - **5**

1, 2 called "kinit" (e.g., once a day)

2, 3 contain "ticket-granting ticket"

3, 4 (e.g., once per service needed)

4, 5 contain "server ticket"