Ibrahim Burak Tanrikulu   21827852

Alice, Bob

KDC

$K_A \{ Bob, K_{AB} \}$

$ticket_B = K_B \{ Alice, K_{AB}, Expiration\ Date \}$

$[Alice, ticket_B, TS]_{Alice}$

$[g^B \bmod p]_{Bob}$

$[g^A \bmod p]_{Alice}$

Alice
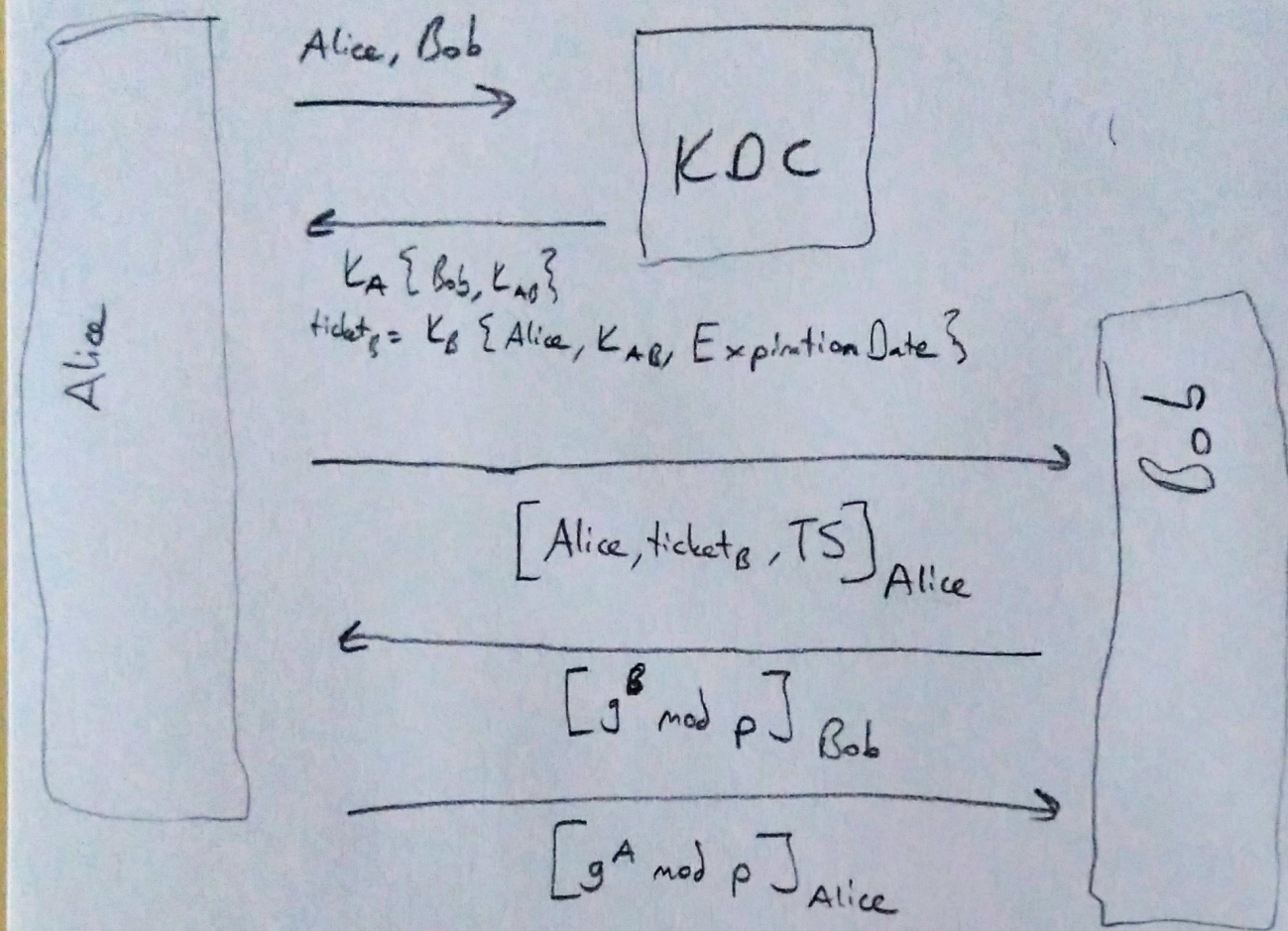
Bob

1- Added Expiration Date to ticket and TS (Time Stamp) to message.

2- Used signing with Alice's private key to authenticate Alice to Bob.

3- Used Diffie Hellman key exchange with RSA signature.