(Details about the solution could be found in the ipython file)

Question 1

PIN is 5377

R is 157

Question 2

The message is 'My favorite machine at the gym is the vending machine.'

Question 3

If the identity of the server is not included when sending the ticket to the client, it would lead to malicious activities. An eavesdropper could intercept the ticket sent from the ticket-granting server. Hence a meet-in-the-middle attack can occur since the server can't identify the client responsible for the request.

Question 4

To achieve forward secrecy, the compromise of their long term RSA keys should not compromise the past session keys. This can be achieved by using a station-to-station protocol, where Bob sends the encrypted signature (E_k(sign_b(R_B, R_A))) to Alice, this doesn't allow the attacker to compromise a previous session key if they obtain Bob's private key b.

Question 5

Secret key a = 253269165174290268846821928601654697793514680881