Quiz 4

1. The following figure depicts the message exchange in Kerberos v4 for Alice to receive a ticket granting ticket (TGT) from KDC. What is the purpose of TGT? In this exchange, does KDC authenticate Alice? Is there any security consequence if someone else impersonates Alice to perform this exchange? Explain why.

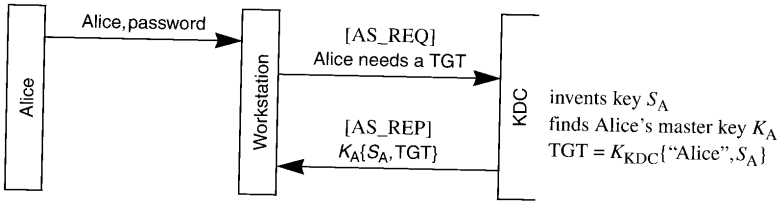

Figure 13-1. Obtaining a TGT

When Alice needs to access a remote resource, her workstation sends the TGT to the KDC along with a request for a ticket to the resource's node. The TGT contains the information the KDC needs about Alice's login session, which allows the KDC to operate without having any volatile data. Hence, it can have a largely static database.

No, KDC does not authenticate Alice.

There is no security consequence, since the reply message is encrypted with Alice's master Key K_A and only Alice can decrypt the message and obtain S_A and TGT.