Exercise 11

1.

Four basic parts. Favourite celebrity , favourite animals, the birthday of someone you close to, and finally the abbreviation of self name. Use **$** to connect them. Finally, when typing the password on the keyboard, type the key right next to your password letter. For example, the password is **Jordan$cat$0928$QY**. And when typing, I actually type **Kptfsm$vsy$0928$WU**.

2.

Since the authentication is done by the authentication server AS, the ticket has no information about authentication, so the adversary which control the server V can intercept the communication after the authentication stage and re-direct the transmission to connect to the server V directly. Thus the message will be attacked or leaked.

3.

The reply attack can be implemented as following:

First, the adversary intercepts all the transmitted messages between A and B and stores them.

When B challenges A, the attacker intercepts the message C and send a fake C_f to A.

When A responses, the attacker intercepts $f_{KAC}(C_f)$ and send $f_{KCB}(C)$ to B.

By reply the transmission, both A and B cannot know that the transmitted messages are fake for that there is no direction indicator B.