**3.1 In general terms, what are four means of authenticating a user’s identity?**

A user can authenticate their identity using something they know, something they have, something they are, or something they do, or some mix of these four.

**3.3 What are two common techniques used to protect a password file?**

One technique for storing passwords is to only store a hash of the password, and then when a user enters their password the entered value is hashed and compared against the stored value. Another technique is to then salt the passwords by adding a random value to the password before hashing, so that if someone attempts an offline dictionary attack and multiple users share a password, the attacker won’t figure out a whole bunch of people's passwords just by figuring out one.

**3.5 Explain the difference between a simple memory card and a smart card.**

A memory card can store data, a smart card has an embedded processor and necessary memory so that it can both store data and process information.

**3.7 In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.**

When a system first sets up biometric authentication for a user, the user provides information verifying their identity and the system extracts some biometric information. This is the enrollment step. Verification is when biometric authentication is used to verify the identity of a user after they present some other form of authentication, such as a password. Identification is when biometrics alone are used to identify and authenticate a user.

**3.9 Describe the general concept of a challenge-response protocol.**

In a challenge-response protocol, first the user requests to be authenticated. The system then issues a challenge in the form of a randomly generated number (nonce) and a function. The user then replies with some number that combines a hash of their password and the nonce using the function provided by the system. Then the system compares this response to the value of hashed password it has on file with the nonce combined with the function and if they match, approves the user.