Problem 1

Recall the MIG-in-the-middle attack. Suggest some ways to prevent and/or detect it. Explain why they work.

Problem 2

Suppose that the attacker can eavesdrop on a message exchange where a Kerberos v4 client requests the ticket-granting ticket (TGT).

A) Explain how this helps the attacker mount an off-line dictionary attack.
B) How would you modify the protocol for requesting the TGT to prevent offline dictionary attacks?

Problem 3:

Suppose that, from today onward, UCI is blocking all packets to/from your favorite streaming service using a firewall that works by checking source and destination IP addresses and discarding packets if either the source (of incoming) or destination (of outgoing) packets is in that streaming service. To survive for the remainder of the quarter, you must find a way to bypass this restriction. Explain how IPSec can help you to bypass the firewall and regain access to your favorite streaming services. Which IPSec mode (Tunnel or Transport) is more appropriate considering this goal and why?

Problem 4

Many bank websites have adopted the following anti-fraud defense. The first time a user registers at the bank's website, she enters her username and password as usual, and is given a choice between several pictures. The association between the username and the chosen picture is stored in the bank's database. In all subsequent sessions, the user types in her username and expects to be shown a picture. Unless she sees the picture she chose during her first session, she does not type in her password. This way, users avoid giving their passwords to fake websites.

A) Describe a man-in-the-middle attack that allows a fake website to show the user her chosen picture. (Assume that this is not the user's first session, i.e., she has already chosen the picture.)
B) Design a cookie-based defense for this anti-phishing scheme that prevents the man-in-the-middle attack you discovered in part A.

Problem 5

Recall all biometric authentication techniques discussed in class. Which one do you think is the best? Explain your reasons carefully. Consider issues such as: ease of enrollment, difficulty of fraud/forgery, static vs dynamic authentication and cost. Be concise!