Question 1

Suppose a computer is authenticated based on its IP address (no passwords are used). Identify one strength and one weakness of such an authentication mechanism.

Question 2

(a) Problem 2, Chapter 9, page 236.

(b) Let a dictionary have 4,096 words. Let a user pick 5 words at random for choosing a password (i.e., the password comprises of these 5 words). What is the strength of this password in bits?

Question 3

(a) Could $f(K_{AB}, R)$ be a secure hash function of K_{AB} and R in the protocol below? Explain briefly.

(b) Give two reasons why should we use different keys for different purposes?

(c) What is the problem when session key establishment to protect the rest of the session does not follow an authentication protocol? Explain briefly.

(d) What would be a good session key between Alice and Bob following the authentication exchange (shown below) such that (i) even if an adversary obtains the key, it cannot find K_{AB}, and (ii) the session key is unique for every session?

(e) Consider the one-way authentication protocol shown in the figure below. Here, Bob is a stateless server, and therefore it is inconvenient to require him to remember the challenge he sent to Alice. Let K_{AB} be the secret key shared between Alice and Bob. Now, this protocol is vulnerable to a replay attack where an eavesdropper can record R, $K_{AB}\{R\}$ pair and replay that later. If we enhance the protocol such that R represents the current time, is the protocol secure? Identify one strength, and one weakness of this enhanced protocol.

(f) Problem 7, page 289, chapter 11.

(g) Problem 8, page 289, chapter 11.

(h) Here K_{AB} is the shared secret between Alice and Bob, R1 and R2 are random nonces (random numbers used only once), and the function f is a secret key function or a hash function. The protocol of this question is vulnerable to an offline dictionary attack by Trudy impersonating as Alice. Modify this protocol appropriately to remove this vulnerability.

Question 4

(a) Chapter 12, Problem 5, page 302.

(b) Chapter 12, Problem 15, page 302-303.

Question 5

(a) Let us plot the observed clock offset, in microseconds, on the y-axis and the time since the start of the finger printing measurements, in seconds, at the fingerprinter, on the x-axis. Let (6, 60) and (8, 85) be two points at times 6s and 7.5s, where the clock offset is observed by the fingerprinter to be 60 and 85, respectively. Estimate the clock skew of the fingerprintee from these two points. You can assume that the network delays are negligible.

(b) Why is it not easy to fabricate clock skews of access points?

(c) Could ambient conditions change the clock skew-based fingerprints? Explain briefly. Describe one approach to deal with changes in ambient temperature.

(d) Suppose that a manufacturing plant of *linksys* access points can produce 10^6 unique clock skew fingerprints. How many access points manufactured at this plant do you need to examine to find two that have the same fingerprint with a very high probability? After knowing this number, would you feel confident using the fingerprint method to detect unauthorized access points? Explain briefly.