Each problem worth 10 points.

Problem 16.9 from textbook:
It contains Alice's name encrypted by the KDC-Bob secret key.

Problem 16.10 from textbook:
It has a nonce (e.g., time stamp) encrypted with the session key.

Problem 16.11 from textbook:
It contains the session key encrypted by the KDC-Bob secret key.

Problem 17.2 from textbook:
Answer:

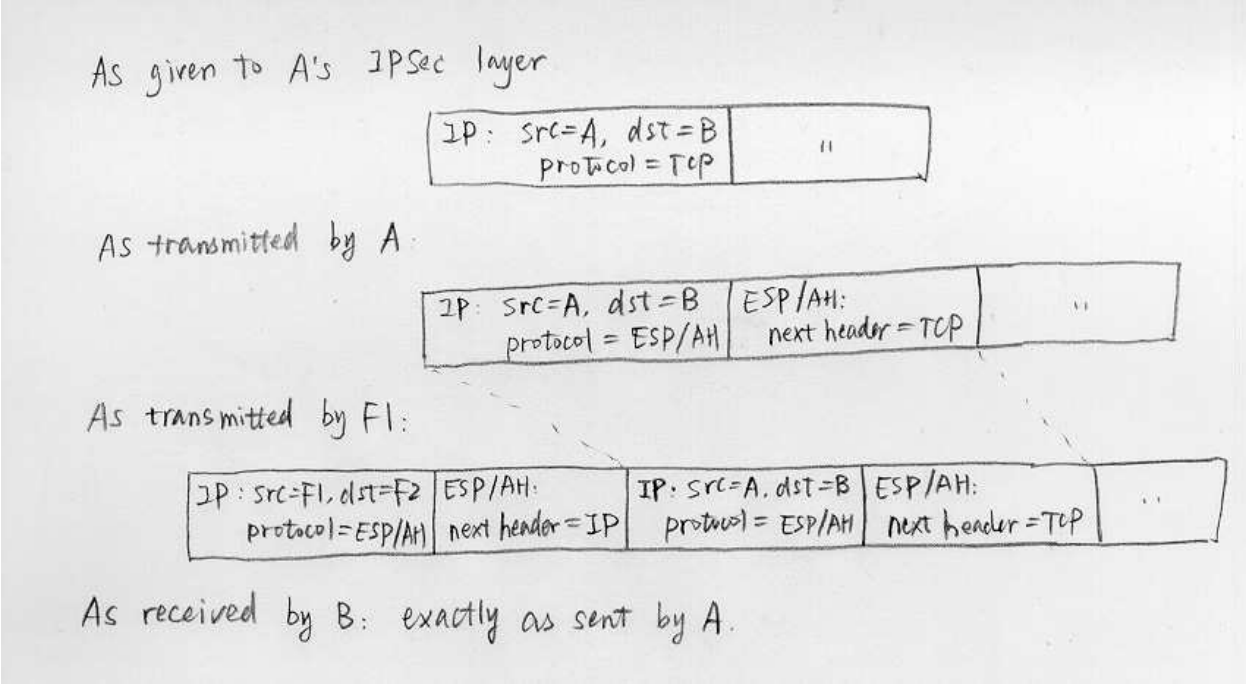
To integrity protect the first set of messages where the cookies and crypto suite information is exchanged. This will prevent a man-in-the-middle attack in step 1 for instance, where someone can suppress the original message and send a weaker set of crypto suites.

Problem 17.3 from textbook:

Answer:

a. Brute Force Cryptanalytic Attack: The conventional encryption algorithms use key lengths ranging from 40 to 168 bits.
b. Known Plaintext Dictionary Attack: TLS protects against this attack by not really using a 40-bit key, but an effective key of 128 bits. The rest of the key is constructed from data that is disclosed in the Hello messages. As a result the dictionary must be long enough to accommodate 2^{128} entries.
c. Replay Attack: This is prevented by the use of nonces.
d. Man-in-the-Middle Attack: This is prevented by the use of public-key certificates to authenticate the correspondents.
e. Password Sniffing: User data is encrypted.
f. IP Spoofing: The spoofer must be in possession of the secret key as well as the forged IP address.
g. IP Hijacking: Again, encryption protects against this attack.
h. SYN Flooding: TLS provides no protection against this attack.

Problem 6:
Answer:



Problem 7. (Firewall)

Answer:

1. Allow return TCP Connections to internal subnet.
2. Prevent Firewall system itself from directly connecting to anything.
3. Prevent External users from directly accessing the Firewall system.
4. Internal Users can access External servers,
5. Allow External Users to send email in.
6. Allow External Users to access WWW server.
7. Everything not previously allowed is explicitly denied.

Problem 8. (IDS: Password management)

Answer:
a. T = 26^4/2 seconds = 63.5 hours
b. Expect 13 tries for each digit. T = 13 × 4 = 52 seconds.

For 471 students only:

Problem 9 (Kaufman's book, Chapter 17, page 439, problem 5)
Answer:
Suppose one portion of your Intranet is connected to the Internet with firewall F1, and another portion of your Intranet is connected with firewalls F2 and F3. All addresses inside that portion are reachable equally well through F2 and F3. Since security associations (SAs) are pairwise, F1 will have two SAs: one to F2, and one to F3. When F1 forwards a packet for destination D, it has

to choose which SA to send it on, encrypting the packet with the key for the F1-F2 SA or with the key for the F1-F3 SA. Internet routing can route packets for D via either F2 or F3. If it chooses a different F than F1 assumed, then it will not work. So F1 has to specify which of the Fs the Internet should deliver the packet to.

For 571 students only:

Problem 10: (IDS: base-rate fallacy)
Answer:

Let WB equal the event "witness reports Blue cab",

Then:

$$Pr[Blue|\ WB] = \frac{Pr[WB|Blue]\ \Pr\ [Blue]}{Pr[WB|Blue]\ Pr[Blue] + [WB|Green]\ \Pr\ [Green]} = \frac{0.9 * 0.1}{0.9 * 0.1 + 0.1 * 0.9}$$
$$= 0.5$$

This example is referred to as the "juror's fallacy".