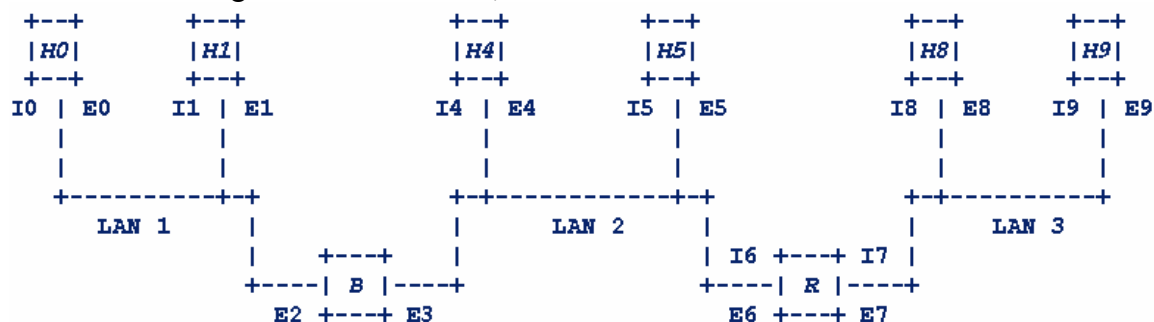CSE591 Computer and Network Security, fall 2005

[Assignment 1]
1. Suppose that instead of using 16 bits for the network part of a class B address, 20 bits had been used. How many class B networks would there have been?

2. A class B network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet?

3. You have just explained the ARP protocol to a friend. When you are all done, he says: "I've got it. ARP provides a service to the network layer, so it is part of the data link layer." What do you say to him?

4. Datagram fragmentation and reassembly are handled by IP and are invisible to TCP. Does this mean that TCP does not have to worry about data arriving in the wrong order?

5. Suppose two cards with the same IP address were placed on same Ethernet. What would happen? How about two cards with same IP address were placed on different Ethernets. What would happen?

6. Consider the figure below in which,

```
+--+          +--+              +--+          +--+              +--+          +--+
|H0|          |H1|              |H4|          |H5|              |H8|          |H9|
+--+          +--+              +--+          +--+              +--+          +--+
I0 | E0     I1 | E1            I4 | E4       I5 | E5            I8 | E8       I9 | E9
   |           |                 |             |                 |             |
   |           |                 |             |                 |             |
   +----------+-+               +-+-----------+-+               +-+----------+
     LAN 1     |                 |   LAN 2     |                 |   LAN 3
               |   +---+         |             | I6 +---+ I7 |
               +----| B |----+   |             +----| R |----+
               E2 +---+ E3       |             E6 +---+ E7
```

• B is a bridge. Its filtering table is initially empty.
• R is an IP router.
• H0, H1, H4, H5, H8 & H9 are hosts.
• I0, I1, I4, I5, I6, I7, I8 & I9 are 32-bit IP (interface) addresses, as shown.
• E0, E1, E2, ... , E9 are 48-bit Ethernet (interface) addresses, as shown.
Suppose host H4 sends an IP packet to host H9. This packet will, of course, be encapsulated in an Ethernet frame.
(a) What will the source Ethernet address in the header of that frame be, as the frame traverses LAN 2?
(b) What will the destination Ethernet address in the header of that frame be, as the frame traverses LAN 2?
(c) What will the destination IP address in the header of the encapsulated packet be, as the frame traverses LAN 2?
(d) What will the source Ethernet address in the header of the frame encapsulating the packet be, as that frame traverses LAN 3?
(e) What will the destination Ethernet address in the header of that frame be, as the frame traverses LAN 3?

(f) What will the source IP address in the header of the encapsulated packet be, as the frame traverses LAN 3?

(g) Bridge B will, of course, receive the frame off of LAN 2. Will it transmit acopy of it on LAN 1?

[Assignment 2]

Chapter 2

2.2 Random J. Protocol-Design has been told to design a scheme to prevent messages from being modified by an intruder. Random J. decides to append to each message a hash of that message. Why doesn't this solve the problem? (We know of a protocol that uses this technique in an attempt to gain security.)

2.3 Suppose Alice, Bob, and Carol want to use secret key technology to authenticate each other. If they all used the same secret key K, then Bob could impersonate Carol to Alice (actually any of the three can impersonate the other to the third). Suppose instead that each had their own secret key, so Alice uses K_A, Bob uses K_B, and Carol uses K_C. This means that each one, to prove his or her identity, responds to a challenge with a function of his or her secret key and the challenge. Is this more secure than having them all use the same secret key K? (Hint: what does Alice need to know in order to verify Carol's answer to Alice's challenge?)

2.4 As described in §2.6.4 *Downline Load Security*, it is common, for performance reasons, to sign a message digest of a message rather than the message itself. Why is it so important that it be difficult to find two messages with the same message digest?

2.5 What's wrong with the protocol in §2.4.4 *Authentication*? (Hint: assume Alice can open two connections to Bob.)

Chapter 3

3.1 Come up with as efficient an encoding as you can to specify a completely general one-to-one mapping between 64-bit input values and 64-bit output values.

3.3 How many DES keys, on the average, encrypt a particular plaintext block to a particular ciphertext block?

3.4 Make an argument as to why the initial permutation of the bits of the DES key cannot have any security value.

3.7 What would change in the DES description if keys were input as 56-bit quantities rather than 64-bit quantities?

3.8 Why is a DES weak key (see §3.3.6 *Weak and Semi-Weak keys*) its own inverse? Hint: DES encryption and decryption are the same once the per-round keys are generated.

3.12 Verify the *MixColumn* result in Figure 3-25 by using the same method (in conjunction with Figure 3-28's table) to compute *InvMixColumn* of the *MixColumn* result and checking that you produce the *MixColumn* input.

Chapter 4
4.3 Let's assume you do DES double encryption by encrypting with K_1 and doing DES in decrypt mode with K_2. Does the same attack work as with double encryption with K_1 and K_2? If not, how could it be made to work?

4.6 Consider the following alternative method of encrypting a message. To encrypt a message, use the algorithm for doing a CBC decrypt. To decrypt a message, use the algorithm for doing a CBC encrypt. Would this work? What are the security implications of this, if any, as contrasted with the "normal" CBC?

[Assignment 3]
Chapter 6
6.2 In section §6.4.2 *Defenses Against Man-in-the-Middle Attack*, it states that encrypting the Diffie-Hellman value with the other side's public key prevents the attack. Why is this the case, given that an attacker can encrypt whatever it wants with the other side's public key?

6.3 In RSA, is it possible for more than one d to work with a given e, p, and q?

6.5 In DSS, other than saving users the trouble of calculating their own p, q, and g, why is there an efficiency gain if the value of p, q, and g are constant, determined in the specification?

6.8 Suppose Fred sees your RSA signature on m_1 and on m_2 (i.e. he sees m_1^d mod n and m_2^d mod n). How does he compute the signature on each of m_1^j mod n (for positive integer j), m_1^{-1} mod n, $m_1 \cdot m_2$ mod n, and in general $m_1^j \cdot m_2^k$ mod n (for arbitrary integers j and k)?

6.10 In ElGamal, how does knowing the secret number used for a signature reveal the signer's private key? How do two signatures using the same secret number reveal the signer's private key? [Hint: p-1 is twice a prime. Even though not all numbers have inverses mod p-1, division can still be performed if one is willing to accept two possible answers. (We're neglecting the case where the divisor is $(p$-1$)/2$, since it is extremely unlikely.)]

Chapter 7
7.1 If m and n are any two positive integers, show that m/gcd(m,n) and n/gcd(m,n) are relatively prime. [Hint: use the result of Euclid's algorithm.]

7.2 If a and b are relatively prime, and bc is a multiple of a, show that c is a multiple of a. [Hint: use the result of Euclid's algorithm.]

7.3 In mod n arithmetic, the quotient of two numbers r and m is a number q such that mq = r mod n. Given r, m, and n, how can you find q? How many qs are there? Under what conditions is q unique? [Hint: mq = r mod n iff there is an integer k such that qm + kn = r. Divide by gcd(m,n).]

7.7 For what type of number n is $\phi(n)$ largest (relative to n)?

7.8 For what type of number n is $\phi(n)$ smallest (relative to n)?

7.9 Is it possible for $\phi(n)$ to be bigger than n?

7.13 Prove that if $n = 2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots\cdots p_k^{\alpha_k}$ where p_i are distinct odd primes and $\alpha_i > 0$ for $i > 0$, then, mod n, 1 will have 2^k square roots $\alpha_0 \leq 1$, 2^{k+1} square roots if $\alpha_0 = 2$, and 2^{k+2} square roots if $\alpha_0 \geq 3$. [Hint: use the Chinese Remainder Theorem to show that a number is a square root of 1 mod n iff it is a square root of 1 mod each of the prime power factors; show that 1 and -1 are the only square roots of 1 mod a power of an odd prime; finally, find the square roots of 1 mod a power of 2.]

Additional questions on ECC:
1. Prove ECDSA is correct

2. What is the additive identity of regular integers?

3. What are the negatives of the following elliptic curve points over real numbers?
P(-4,-6), Q(17,0), R(3,9), S(0,-4)
4. In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)?

[Assignment 4]
1. In class, we have discussed passive attacks and active attacks to EMSEC. What are they?
Give a brief description of each of them and corresponding countermeasures.

2. In class, we have discussed attacks TRANSSEC. What are they? Give a brief description of each of them and corresponding countermeasures.

3. Based on your observation and understanding, do you think we need TEMPEST? Why or why not?

[Assignment 5]
Chapter 4
4.3 A noted computer security expert has said that without integrity, no system can provide confidentiality.

a. Do you agree? Justify your answer.
b. Can a system provide integrity without confidentiality? Again, justify your answer.

4.4 A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.

4.5 Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or combination thereof. Justify your answers.
a. The file access control mechanisms of the UNIX operating system
b. A system in which no memorandum can be distributed without the author's consent
c. A military facility in which only generals can enter a particular room
d. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.

Chapter 5
5.2 Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

a. Paul, cleared for (TOP SECRECT, {A, C}), wants to access a document classified (SECRET, {B, C}).
b. Anna, cleared for (CONFIDENTIAL, {C}), wants to access a document classified (CONFIDENTIAL, {B}).
c. Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C}).
d. Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).
e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).

Chapter 6
6.1 Suppose a system implementing Biba's model used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?

6.3 In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution?

6.5 The relations certified (see ER1) and allowed (see ER2) can be collapsed into a single relation. Please do so and state the new relation. Why doesn't the Clark-Wilson model do this?

[Assignment 6]
The following questions are listed in the online posted chapter file.
Chapter 7.7
1. Develop a construction to show that a system implementing the Chinese Wall model can support the Bell-LaPadula Model.

2. Show that the Clinical Information System model's principle implement the Clark-Wilson enforcement and certification rules.

3. Consider using mandatory access controls and compartments to implement an ORON control. Assume that there are k different organizations. Organization i will produce $n(i,j)$ documents to be shared with organization j.
a. How many compartments are needed to allow any organization to share a document with any other organization?
b. Now assume that organization i will need to share nm $(i,i_1,…,i_m)$ documents with organizations $i_1,….,i_m$. How many compartments will be needed?

4. Someone once observed that "the difference between roles and groups is that a user can shift into and out of roles, wherease that user has a group identity (or identities) that are fixed throughout the session."
a. Consider a system such as a Berkeley-based UNI system, in which users has secondary group identities that remain fixed during their login sessions. What are the advantages of roles with the same administrative functions as the groups?
b. Consider a system such as a System V-based UNI system, in which a process can have exactly one group identity. To change groups, users must execute the newgrp command. Do these groups differ from roles? Why or why not?

6. A physician who is addicted to a pain-killing medicine can prescribe the medication for herself. Please show how RBAC in general, and Definition 7-11 specifically, can be used to govern the dispensing of prescription drugs to prevent a physician from prescribing medicine for herself.

Chapter 14.8
2. Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z.
a. Write a set of access control lists for this situation. Which list is associated with which file?
b. Write a set capability lists for this situation. With what is each list associated?

4. Explain why some UNIX-based systems with access control lists do not allow root to alter the ACL. What problems might this raise?

6. Suppose a user wishes to edit the file xyzzy in a capability-based system. How can he be sure that the editor cannot access any other file? Could this be done in an ACL-based system? If so, how? If not, why not?

8. Consider Multics procedure p and data segment d. Procedure p is executing and needs to access segment d. Segment d's access bracket is (5,6). Assume that d's access control list gives p full (read, write, append, and execute) rights to d. In which ring(s) must p execute for the following to happen?
a. p can read, write to, and append to d.
b. p can read d but not write to or append to d.
c. p cannot access q.

The following questions are listed in our textbook
Chapter 9
1. As stated in §9.2 Address-Based Authentication, UNIX requires a request from system A for a resource at B to explicitly state the desired account name at B if it is not identical to the account name at A. Why do you suppose it makes that requirement? How would one implement this feature without the requirement?
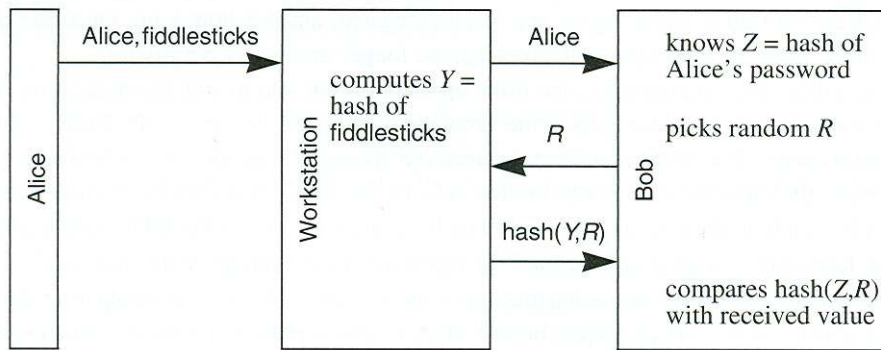
Chapter 10
1. Design a password hash algorithm with the property stated in Password Hash Quirk on page 242. It should be impossible to reverse, but for any string S it should be easy to find a longer string with the same hash.

[Assignment 7]
Chapter 9
2. In §9.6 Eavesdropping and Server Database Reading we asserted that it is extremely difficult, without public key cryptography, to have an authentication scheme which protects against both eavesdropping and server database disclosure. Consider the following authentication protocol (which is based Novell version 3 security). Alice knows a password. Bob, a server that will authenticate Alice, stores a hash of Alice's password. Alice types her password (say fiddlesticks) to her workstation. The following exchange takes place:

Chapter 11

1. Suppose Trudy hijacks a conversation between Alice and Bob. This means that after the initial handshake, Trudy sends messages with source address equal to Alice's source address. Suppose the network allows Trudy to insert a fake source address (Alice's source address), but does not deliver packets destined for Alice's address to Trudy. What are the problems involved in having Trudy transmit a file to Bob as if she were Alice? Consider potential problems with flow control and file transfer protocols when Trudy cannot see return traffic from Bob.

3. In §11.2 Shared Secret we discuss various possibilities for forming a session key. Remember that R is the challenge sent by Bob to Alice, and A is Alice's secret, which Bob also knows. Which of the following are secure for a session key?

$A \oplus R$ $\qquad$ $\{R+A\}_A$ $\qquad$ $\{A\}_A$ $\qquad$ $\{R\}_{R+A}$

5. Suppose we are using a three-message mutual authentication protocol, and Alice initiates contact with Bob. Suppose we wish Bob to be a stateless server, and therefore it is inconvenient to require him to remember the challenge he sent to Alice. Let's modify the exchange so that Alice sends the challenge back to Bob, along with the encrypted challenge. So the protocol is:
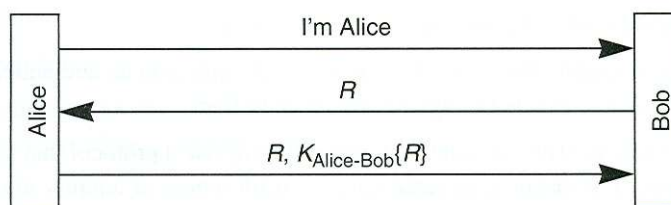
7. In the discussion of Protocol 11-3 on page 261, Bob remembers all the timestamps he's seen within the last 10 minutes. Why is it sufficient for him to remember only 10 minutes worth of timestamps?

9. The expanded Needhan-Schroeder Protocol (page 278) can be shortened to a 6-message protocol without loss of security by merely removing the 7th message. Why is

this true? (Hint: the purpose of the 7th message is to prove to Bob that he is talking to Alice, but he already knows that. Why?)

11. As we pointed out in §9.1 Password-Based Authentication, cellular phones are vulnerable to a fraud known as "cloning". The protocol cellular phones use is that a phone transmits its telephone number followed by a cleartext password. The phone company checks its database of phone number/password to make sure the phone is legitimate before allowing the call to go through. The phone number is the one billed. Suggest a design based on public key, and one based on secret key, technology. Can you guard against the phone company database being stolen?

13. In §11.1.1 Shared Secret, we discussed using MD5($K_{Alice-Bob}|$ R) as the method of encrypting R with $K_{Alice-Bob}$. (When we say $K_{Alice-Bob}|$ R we mean $K_{Alice-Bob}$ concatenated with R.) Suppose instead we used MD5($K_{Alice-Bob}\lor$R). Would that be secure? How about MD5($K_{Alice-Bob}\oplus$R)?

[Assignment 8]
Chapter 11
2. In §11.2 Mutual Authentication, we discuss the reflection attack and note that Protocol 11-8 is susceptible, but Protocol 11-7 is not. How about Protocol 11-11?

4. Design a variant of Otway-Rees (page 279) that only has one nonce generated by Alice and one nonce generated by Bob. Explain why it is still as secure.

6. Let's modify the protocol from the previous problem so that Bob sends both a challenge, and a challenge encrypted with a key that only he knows, to Alice:
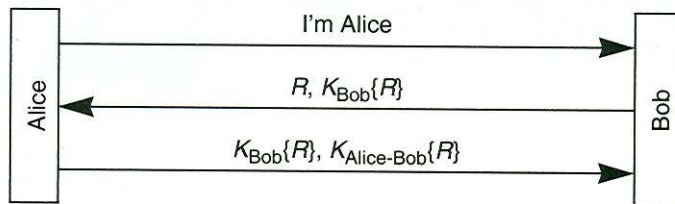
Is this protocol secure?

8. Design a two-message authentication protocol, assuming that Alice and Bob know each other's public keys, which accomplishes both mutual authentication and establishment of a session key.

10. §11.4 Mediated Authentication (with KDC) describes several protocols. For each of those protocols, describe which nonces have to be unpredictable (i.e., sequence numbers would not be good).

12. There is a product which consists of a fancy telephone that, when talking to a compatible fancy telephone, does a Diffie-Hellman key exchange in order to establish a secret key, and the remainder of the conversation is encrypted. Suppose you are a wiretapper. How can you listen to a conversation between two such telephones?

Chapter 12
1. Given that the Lamport hash (see §12.2 Lamport's Hash) value is sent in the clear over the network, why is it more secure than a password?

5. Suppose we are using Lamport's hash, and Bob crashes before receiving Alice's reply. Suppose an intruder. Trudy, can eavesdrop and detect that Bob crashed (maybe Trudy can even cause Bob to crash). Then Trudy has a quantity (whatever Alice replied that Bob did not receive) which Trudy can use to impersonate Alice, if Trudy logs in before Alice attempts to log into Bob again. How can we modify Bob's behavior to prevent this threat? (Exactly when do we overwrite Bob's database, and with what)?

9. Show how in Protocol 12-3 Alice can be assured that it is Bob, i.e., that the other side has the information stored at Bob. Explain why someone who has stolen Bob's database cannot impersonate Alice to Bob.

13. Show credentials download protocols built upon SPEKE, PDM, and SRP.

[Assignment 9]
Chapter 13
1. Design a variant of Kerberos in which the workstation generates a TGT. The TGT will be encrypted with the user's master key rather than the KDC's master key. How does this compare with standard Kerberos in terms of efficiency, security, etc.? What happens in each scheme if the user changes her password during a login session?

Chapter 14
2. Consider the following variant of Kerberos. Instead of having postdated or renewable tickets, a server which notes that the start-time is older than some limit presents the ticket to the TGS and asks if it should believe the ticket. What are the trade-offs of this approach relative to the Kerberos V5 approach?

Chapter 15
4. Compare the following schemes for obtaining Bob's public key, in terms of bandwidth and computation efficiency, security, flexibility, and any other criteria you can think of: downloading Bob's key from the node located at a particular IP address (via an unauthenticated interaction), looking up Bob's key in a directory via an unauthenticated interaction, having an authenticated conversation to the directory, having the directory sign the information you request, storing and retrieving certificates from the directory,

having no directory but having each principle responsible for keeping its own certificate and sending it to someone who needs to talk to it.

[Assignment 10]
Chapter 16
16.1
Talk about the properties of each of the following protocols, such as perfect forward secrecy, escrow foilage against passive attacks, escrow foilage against active attacks, identity hiding, perfect forward secrecy for identity hiding. Assume private encryption keys are escrowed and private signature keys are not escrowed.

- Protocol 16-2.
- A modified form of Protocol 16-2 in which the first two messages are encrypted with the other end's public key rather than signed by the transmitter's private signature key. So in message 1 Alice sends {"Alice", g^a mod p} encrypted with Bob's public key, and Bob in message 2 sends {"Bob", g^b mod p} encrypted with Alice's public key.
- Protocol 16-4.
- Protocol 16-9, where Alice and Bob share a secret key S.
- Each side sends a nonce encrypted with other's public encryption key, resulting key is $\oplus$ of two nonces.
- Assume Alice and Bob share a secret S. Design a protocol in which they can do mutual authentication and establish a shared secret with PFS. Can it be done without Diffie-Hellman or any other form of public key cryptography?
- Protocol 16-2, but with each side deterministically generating the Diffie-Hellman private numbers as described in §16.4 PFS-Foilage from a seed given to the client machine and escrowed at the server machine.

16.5
As mentioned in §16.6 Endpoint Identifier Hiding, it is possible to design a protocol that will hide both identifiers from an active attacker, assuming that Alice (the initiator) already knows Bob's public key. Show such a protocol.

16.11
In the Protocol 16-6, explain why Bob knows that Alice is the real Alice, and not someone replaying Alice's messages. How does Alice know that it's the real Bob if she uses a different a each time? Modify the protocol to allow both Alice and Bob to reuse their a and b values, and yet have both sides be able to know they are talking to a live partner.

16.15
Describe various methods of having Alice and/or Bob remember state from the last time they authenticated each other that allows them to resume a session and bypass the expensive public key cryptography. Describe a method in which Bob can save computation even if he hasn't kept state. Is there a clever way of having Bob remember state and not Alice?

Chapter 17
17.2
Suppose a company's network is attached to the Internet via two NAT boxes, and packets
might exit via either one. How might a protocol such as FTP complicate implementation
of multiple NAT boxes? Suggest methods of making this work.

17.5
When sending encrypted traffic from firewall, why does there need to be an extra IP
header? Why can't the firewall simply encrypt the packet, leaving the source and
destination as the original source and destination?

[Assignment 11]
Chapter 18:
2. What are the relative advantages of the various key types (pre-shared secret keys,
public signature keys, public encryption keys) as a basis for an authentication exchange?

3. Show how someone who knows both Alice's and Bob's public encryption keys (and
neither side's private key) can construct an entire IKE exchange based on public
encryption keys that appears to be between Alice and Bob.

4. Write out the shortened version of main-mode public signature keys that hides Alice's
ID from an active attacker. Explain why the 6-message version described in §18.5.10.1
Public Signature Keys, Main Mode allows parallel computation of g^{ab} mod p, whereas the
shortened version does not.

7. Design a protocol in which one side has a public signature key and the other side has a
public encryption key.

Chapter 19:
2. Compare the performance of doing PFS as implemented in SSLv3, vs. the
recommended modification in §19.13.2 Exportability in SSLv3 vs. doing a Diffie-
Hellman exchange for each connection. Assume the ephemeral key pair is of adequate
length, rather than done to meet export rules. Assume also that PFS doesn't need to be
"perfect", but rather the ephemeral key can change, say, every hour, and the cost of
generating the key pair can be amortized over all the connection requests that occur
during that hour.

Additional Questions:
1. Describe when is transport model is preferred and when tunnel mode is preferred.
2. Describe the methods on how to work with NAT when ESP is used.
3. Present an example on stack buffer overflow attack.

[Assignment 12]
Chapter 20:
2. If using secret keys for user keys, and sending a multi-recipient message, why is encrypting the MD of the message with the secret key associated with the recipient a more efficient MAC than doing a keyed MD of the message (again, using the secret key associated with the recipient)?

4. Suppose Alice sends an encrypted, signed message to Bob via the mechanism suggested in §20.8.2 Plausible Deniability Based on Public Key Technology. Why can't Bob prove to third party Charlie that Alice sent the message? Why are both cryptographic operations on S necessary? (Alice both encrypts it with Bob's public key and signs it with her private key.)

6. Using the authentication without non-repudiation described in §20.8.2 Plausible Deniability Based on Public Key Technology, Bob can forge Alice's signature on a message to himself. Why can't he forge Alice's signature on a message to someone else using the same technique?

8. Which security features can be provided without changing the mail delivery infrastructure, i.e., by only running special software at the source and destination?

10. Suppose you are a judge trying to decide a dispute between a buyer and a supplier. The buyer claims not to have produced a particular email purchase order, while the supplier shows you the purchase order, and certificates and CRLs demonstrating that the purchase order was signed by the buyer, all signed by a notary. How would the dates on the various pieces of evidence influence your decision? What if only the purchase order was signed by the notary? Note that the security community continues to debate issues such as whether the CRL should be required to have a later date than the notary's signature.

PGP question:
Design a PGP trust management scheme: (1) construct your own trust weighting approach, (2) based on your proposed scheme, present a 10 nodes example for your constructed web of trust.

Chapter 26:
1. Suppose you were able to observer ciphertext that you knew had been encrypted in CBC mode, and you saw that two ciphertext blocks, say c_2 and c_5, were equal. Why would this leak information? (Hint: look at Figure4-5 and compare $c_1 \oplus c_4$ with $m_2 \oplus m_5$. What would happen if you knew one of the plaintexts, say m_2?)

2. Suppose Alice and Bob negotiate a 64-bit key, and use the low-order 40 bits of it for encryption (for export reasons), and use the entire 64 bits for integrity protection. How much work would it be to brute-force break the key and construct a forged encrypted message using that key?

3. Consider the following protocol. Must the challenge be unpredictable, or is it sufficient to ensure Bob never chooses the same challenge twice, for instance, by using a sequence number?

Alice → Bob: I'm Alice

Bob → Alice: $K_{Alice\text{-}Bob}\{R\}$

Alice → Bob: $(K_{Alice\text{-}Bob}+1)\{R+1\}$