Computer and Network Security (400127)
Spring 2006

Instructions:

- The answers to the questions must be in English.
- Students in **grading scheme 1**, who have completed all the assignments, must answer **questions 1 to 8** only (for 70 marks).
- Students in **grading scheme 2** must answer all **questions 1 to 10** (for 100 marks).
- The contribution of each question to the final mark is indicated at the end of each question.

Question 1 [13 marks]

Block cipher algorithms such as the Data Encryption Standard (**DES**) apply two simple transformation functions, substitution and permutation, to their input over multiple rounds.

1. The input block size of DES is 64-bits but the substitution function operates on 8 blocks of size 6-bits. Explain the reason for this smaller block size for substitution function. [3 marks]
2. The permutation function in a DES round operates on a block of size 32-bits. Explain the reason for this larger block size for permutation function. [2 marks]
3. The DES cipher has 16 rounds. Explain the criteria by which the number of rounds for the cipher was decided. [3 marks]
4. Explain the Cipher Feedback Mode (**CFB**) of operation of the DES cipher using a clearly labeled diagram. [3 marks]
5. The chief technical officer of streaming video company Stroogle has suggested using DES in CFB mode to encrypt their online real-time video feeds to subscribers over the Internet. Give one advantage and one disadvantage for this choice. [2 marks]

Question 2 [9 marks]

Some of the required properties of cryptographically secure hash functions are **preimage resistance**, **second-preimage resistance** and **collision resistance**.

1. Explain each of the above three properties. You may explain with respect to what an attacker get as input and what he is expected to produce as output. [3 marks]
2. The Unix password based login authentication function use a modified version of the DES cipher as a hash function. Explain the operation of this function using a clearly labeled diagram. [3 marks]
3. In addition to the standard security properties of a hash function, give two other security features of the DES-based Unix password based login authentication function. [3 marks]

Question 3 [7 marks]

The investigative reporter Ms Lois at the Planeetkrant newspaper has decided to use **Lamport's hash** based authentication scheme to correctly identify her informant Mr Bib who contacts her through payphones and pass on information.

1. Explain how this scheme would operate. [4 marks]
2. Some criminals who have been recording all the telephone conversions of Ms Lois have broken into her office and stolen all her documents. What is the effect of these criminal activities on the security of the authentication scheme used between Ms Lois and Mr Bib? [3 marks]

Question 4 [10 marks]

Alice, Bob and Charlie have agreed on certain values for use in public key cryptography computations. These include a large prime number p and a generator g of Z_p^*.

1. Explain how Alice and Bob can establish a shared secret key using the **Diffie-Hellman** public key cryptosystem. [4 marks]
2. Explain why it is hard for an observer who monitors all the communications between Alice and bob to determine the shared secret key they establish. [2 marks]
3. Explain how Charlie can mount a man-in-the-middle attack on the above key establishment interaction between Alice and Bob. [4 marks]

Question 5 [5 marks]

Alice has decided to use **RSA** public key cryptosystem to send short messages securely to Bob. For this, she has created her public key (e, n) where n is a large prime composite and e is an integer relatively prime to $\phi(n)$. The corresponding RSA private key is the integer d which Alice keeps secret.

1. Explain the **homomorphism property** of the RSA public key cryptosystem function. [3 marks]
2. It is well known that the homomorphism property of the RSA function allows secure communications done using the RSA public key cryptosystem to be attacked. Give one countermeasure to prevent this attack. [2 marks]

Question 6 [8 marks]

An application software package requires each of its users to login before it can be used. Each user is asked to choose a username and then is prompted to enter a password. The program restricts the type of characters the user is allowed to use in her password but does not restrict the length of the password.

1. If the user is allowed to use all lowercase characters, all uppercase characters, all digits and the punctuation characters ? and !, what would be a safe length for the password that the user should chose. Explain the reasoning for the password length decision. [3 marks]

2. Explain the user authentication scheme called **two-factor authentication.** [3 marks]
3. An example Internet banking application is where a user connects to the bank's server computer from her home computer to check bank account details and do fund transfers. Why two-factor authentication would be more suitable than standard Unix-like password authentication for an Internet banking application? [2 marks]

Question 7 [9 marks]

Alice is designing a new Unix-like operating system and wants to decide on an access control model for use in implementing security features.

1. Briefly explain why a discretionary access control (**DAC**) model is more suitable for use in Alice's OS in comparison to a mandatory access control (**MAC**) model. [5 marks]
2. The classic **Bell-La Padula** (BLP) MAC model is used mainly to provide *confidentiality* guarantees by preventing unauthorized information flow. Describe a version of BLP model that can be used to provide *integrity* guarantees. You may use a clearly labeled diagram in your answer. [4 marks]

Question 8 [9 marks]

The notation $\{m\}_{Alice}$ is used to denote the public key encryption of message m by Alice and the notation $[m]_{Alice}$ for digital signing of message m. The public key certificate C_{Alice} contains the public keys of Alice that have been certified by a well-known certification authority (CA). Similarly, Bob also has a public key certificate C_{Bob} that contain his public encryption key and signature verification key. Assume that Alice and Bob have loosely synchronized clocks. A secure message transfer from Alice to Bob has the following set of interactions:

Alice $\rightarrow$ Bob	:	$[m]_{Alice}$, C_{Alice}
Bob	:	Verify the signature on the message m.
		Accept m only if signature is correct.

1. After sending the digitally signed message m, Alice wants to **repudiate** her action of sending the m to Bob. Explain a method by which Alice could repudiate her action. [2 marks]
2. Describe a modifications to the above protocol, without involving any third party, that prevents Alice from repudiating her action of sending m to Bob (*Hint: practical rules for entities to follow*). [3 marks]
3. Terry is a trusted time-stamping authority that can be contacted by both Alice and Bob. Describe a modifications to the above protocol that prevents Alice from repudiating her action of sending m using the services of Terry. [4 marks]

Question 9 [15 marks]

The widely used public key infrastructure (**PKI**) model consists mainly of a hierarchy of certification authorities (CA) and registration authorities (RA). The PKI makes it easy to issue public key certificates and to find the certificates we want.

1. Describe the separation of duties for the CA and RA and the reason for this separation. [3 marks]
2. Explain why we need to **revoke** public key certificates. [3 marks]
3. The Internet key Exchange Protocol (**IKE**) is alternative method for key establishment in secure interactive communication. Describe using a clearly labeled diagram, the **Main mode** of the IKE in which mutual authentication of the entities and session key establishment is done. [6 marks]
4. Describe an attack on the IKE for which it is vulnerable only when executed in the **Aggressive mode**. [3 marks]

Question 10 [15 marks]

The Company AliceWare b.v. has a conventional wireline LAN in its office premises that also connects to the Internet for web access and email services as shown in figure 1. The company server contains many important documents containing valuable company intellectual property and business information. The company also allows its employees to connect to the company server from outside the network by dial-in to the modem connected to the server.

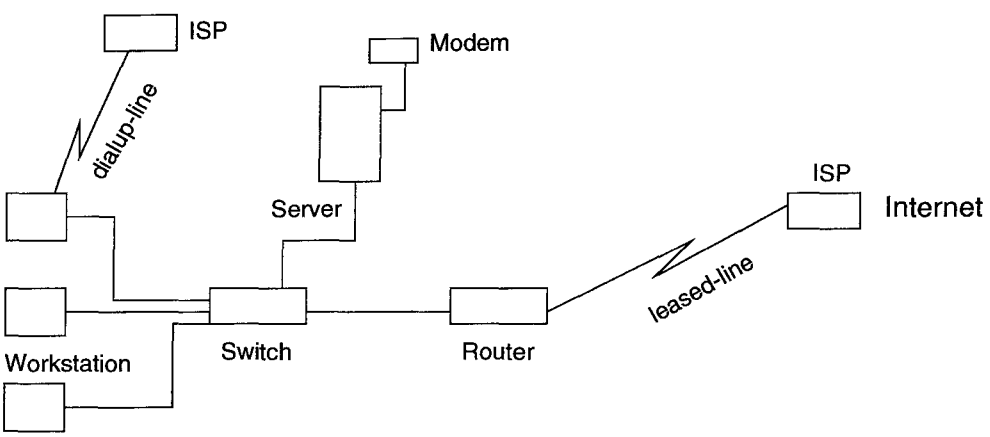

Figure 1: The wireline LAN at AliceWare b.v.

1. Describe how a firewall can be used to secure the AliceWare LAN. You must provide a clearly labeled diagram and provide details on the positioning of the firewall, particular firewall configuration recommended, any other servers required to secure the network and any changes required to the network setup shown in figure 1. [6 marks]
2. The company is moving to a new office premises and is planning to change its network to wireless LAN. The system administrator of the company has prepared preliminary design for the new wireless LAN using an 802.11a access point (AP) as shown in figure 2.

Describe the security vulnerabilities present in this wireless LAN that was not present in the earlier wireline LAN. [4 marks]

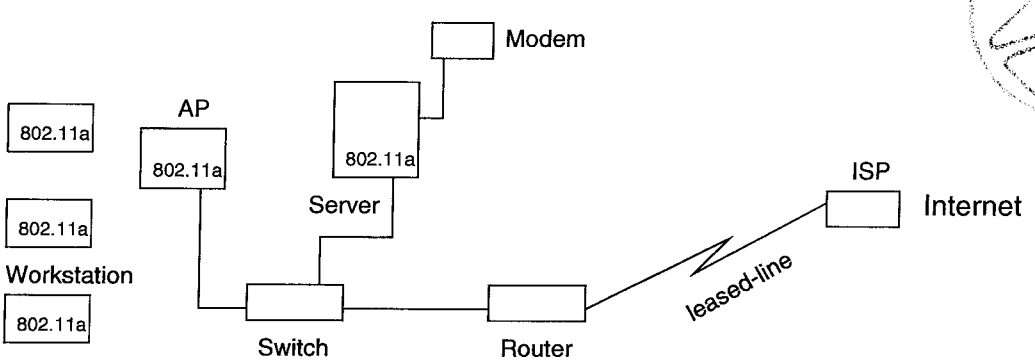

Figure 2: The 802.11a wireless LAN at AliceWare b.v.

3. Describe how a firewall can be used to secure the new wireless LAN at AliceWare. You must provide a clearly labeled diagram and provide details on the positioning of the firewall, particular firewall configuration recommended, any other servers required to secure the network and any changes required to the network setup shown in figure 2. [5 marks]