Part I. (40%) Multiple choice questions on theory and practices

Your answers to the following 16 multiple choice questions shall be clearly marked (use ✘ or ✔) on the attached preprinted sheet, where the evaluation rules are also explained.

On theory

1. The course lectures presented two main approaches to modeling of information security, which were they? Check the one statement that applies:
   A. Confidentiality and integrity.
   B. Communication-oriented and computer-oriented.
   C. Top-down and bottom-up.

2. Which fields of information are used by a typical packet-filtering router in its security decisions? Check the one statement that applies:
   A. Link interface address, IP address, and TCP port number.
   B. IP address, IP header checksum, and digital certificate.
   C. URL address, IP address, and TCP port number.

3. What has been the use of encryption in some software viruses? Check the one statement that applies:
   A. To achieve virus code variation and thereby evade detection.
   B. To achieve virus code variation and thereby modify operation.
   C. To hide the virus code in the application program.

4. What services are provided by IPsec? Check the one statement that applies:
   A. Confidentiality, peer authentication, connectionless integrity and access control.
   B. Confidentiality, authentication of origin, connectionless integrity, replay detection, and access control.
   C. Confidential and authentic channels in transport mode, tunnel mode and node-to-intermediate mode.

5. What is a "replay attack"? Check all statements that apply:
   A. Resending of intercepted, possibly modified, communication to produce an unauthorized effect.
   B. Resending a set of messages continuously to produce a denial of service effect.
   C. Repeating a client-server transaction already accepted by the server.

6. What is Kerberos? Check all statements that apply:
   A. A client-server authentication service for a distributed computing environment.
   B. A mythical three-headed dog.
   C. A public-key based client-server access control system developed at MIT.

7. Why does PGP generate a digital signature prior to message compression? Check all statements that apply:
   A. The design allows for different compression algorithms in various implementations.
   B. PGP does not make use of message compression.
   C. The designers wanted to make it possible to verify the original readable message.

8. What is S/MIME? Check all statements that apply:
   A. An alternative to PGP for the MIME Internet email format standard.
   B. A non-repudiation enhancement to the MIME Internet email format standard.
   C. A confidentiality enhancement to the MIME Internet email format standard.

9. The Norwegian Data Inspectorate (Datatilsynet), an independent administrative body under the Norwegian Ministry of Labour and Government Administration (Arbeids- og administrasjonsdepartementet), ensures enforcement of the Personal Data Act of 2000 (Personopplysningsloven). Check all statements that apply:
   A. The purpose is to protect persons from violation of their right to privacy through the processing of personal data.
   B. The purpose is to help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.
   C. The purpose is to keep a systematic, private record of all processing that is reported or for which a license has been granted with respect to processing of personal data.

On practice

10. Consider the statement: *A firewall is not needed if you only have a dial-up connection.* Select True or False.

11. Consider the statement: *You are secure from computer viruses if you do not open email attachments*. Select True or False.

12. Consider the statement: *Commercial software companies have released "spyware" functionality in their software products.* Select True or False.

13. *MyDoom* is the name of a piece of malicious software that emerged early in 2004 as a Windows OS threat, and became categorized as a (check the one statement that applies):
    A. Worm.
    B. Virus.
    C. Trojan horse.

14. *Melissa* is the name of a software virus that first emerged in March 1999. This malicious software spread by employing (check all statements that apply):
    A. MS Word macro program.
    B. Email MS Word attachment sent by MS Outlook.
    C. Email MS Word attachment received by any email client on Windows.

15. In 2001, Microsoft provided free software to block the *Code Red II* worm. As a result (check the one statement that applies):
    A. Most users and system administrators downloaded CodeRedCleanup and quickly patched the security hole in the operating system; so far less damage than originally feared occurred because of this concerted efforts.
    B. Some users did not bother to install the security patch, resulting in estimated €650 000 in total business damage worldwide.
    C. Many users and system administrators initially ignored the problem, leading to estimated €2200 000 000 in total business damage worldwide.

16. What is a "honeypot" in computer security terms? Check the one statement that applies:
    A. A dummy computer installation designed to confuse attackers from the real resource or installation.
    B. A game-server distracting juvenile attackers from doing harmful actions to critical information processing.
    C. An intrusion attraction system that collects information about illicit and criminal computer users.

Part II. (25%) Secure Socket Layer (SSL)

17. What is the difference between an SSL connection and an SSL session? (2)

18. Consider the following security threats to HTTP secured by SSL. For each attack: give a short explanation of the attack, and describe how the attack is countered by a particular feature of SSL. (8)
    1) Brute Force Cryptanalytic Attack.
    2) Known Plaintext Dictionary Attack.
    3) Replay Attack on SSL handshake messages.
    4) Man-in-the-Middle Attack.
    5) HTTP Wiretapping of passwords.
    6) Spoofing of IP addresses.
    7) Hijacking of IP addresses.
    8) SYN Flooding.

Part III. (15%) Systems

19. List the three overall design goals for a firewall system.

20. Describe the general model of a PKI distributed system. Make a diagram and explain the functionality of the system (recommended length is 2 pages).

Part IV. (20%) Cryptography

21. Alice and Bob utilize the Diffie-Hellman (DH) crypto-protocol with a common prime $q = 13$ and a primitive root $g = 2$.
    1) Draw a message sequence diagram and describe the essential messages of the DH crypto-protocol. (2)
    2) If Alice computes the public key $Y_A = 9$, what is Alice's private key X_A? (1)
    3) If Bob computes the public key $Y_B = 3$, what becomes their shared secret key K? (1)

22. Cryptographic Feistel structure is used in some block cipher constructions, including LUCIFER and DES.
    1) Show that Feistel decryption is the inverse of Feistel encryption. (2)
    2) Consider the possibility of using a one-way hash function to construct a block cipher with Feistel structure. Remember that a block cipher must be reversible (decryption). What is your proposal for such a construction? (2)
