Part I. (50%) Multiple Choice Questions on Theory

Your answers to the following 25 multiple choice questions shall be clearly marked (use V or X) on the attached preprinted sheet. All questions are in the category *"Check the one statement that applies"*. Each question is weighted 2% of the exam. One point is assigned if and only if the correct statement is selected and the two incorrect choices are left blank, else zero point is assigned.

.

1. The course lectures have presented two main approaches to information security modeling. What are they?
    a. Confidentiality and authenticity.
    b. Communication-oriented and computer-oriented.
    c. Top-down and bottom-up.
2. What is the most significant difference between a symmetric and an asymmetric cryptosystem?
    a. The key distribution.
    b. The mode of operation.
    c. The strength against attacks.
3. What is a circuit-level gateway?
    a. A MAC layer level point of access.
    b. Access point based on electronic device control mechanism.
    c. A TCP connection relay for access control.
4. In the context of access control, what is the difference between a subject and an object?
    a. The direction of the information flow.
    b. The direction of the access operation.
    c. The direction of the access rights.
5. On which communication stack layer is the SSL/TLS considered to be?
    a. Application.
    b. Transport.
    c. Network.
6. The SSL Record Protocol provides the following services:
    a. Handshake, Change Cipher Spec, Alert.
    b. Data encryption.
    c. Confidentiality and integrity.
7. Which secret key exchange method is supported by SSL?
    a. RSA only.
    b. Diffie-Hellman only.
    c. Both of the above.
8. What is Secure Electronic Transaction (SET)?
    a. A protocol system for credit card payments using public-key mechanisms.
    b. A secure protocol for database transactions over Internet.
    c. A public-key infrastructure (PKI) standard made by Mastercard and VISA.
9. Which fields of information are used by a typical packet-filtering router in its security decisions?

   a. Link interface addresses, IP addresses, and TCP port numbers.
   b. Digital certificates, IP addresses, and IP header checksums.
   c. URL addresses, IP addresses, and TCP port numbers.
10. What is a ‘replay attack’?
   a. Resending of intercepted communication to produce an unauthorized effect.
   b. Resending a set of messages continuously to jam the receiving end.
   c. Repeating a successful crypto-attack.
11. What services are provided by IPsec?
   a. Confidentiality, peer authentication, connectionless integrity and access control.
   b. Confidential and authentic channels in transport mode, tunnel mode and node-to-intermediate mode.
   c. Confidentiality, authentication of origin, connectionless integrity, replay detection, and access control.
12. What is an advantage of applying ESP before AH in IPsec?
   a. Less redundancy is introduced in the IP packet.
   b. Encryption of more fields in the IP packet.
   c. Authentication of more fields in the IP packet.
13. What is a security association (SA) in IPsec?
   a. A security parameter association directed between source and destination IP-node.
   b. A shared security parameter association between two communicating IP-nodes.
   c. A security parameter index used in AH and ESP headers.
14. What is ‘SA bundling’ in the IPsec context?
   a. Packet routing coordination to provide a desired set of IPsec services.
   b. A tunnel mode IPsec service to encapsulate multiple IP packets into a new secured IP packet.
   c. A sequence of security parameters through which packets are processed to provide the desired set of IPsec services.
15. What is a hybrid cryptosystem?
   a. A system combining symmetric and asymmetric crypto.
   b. A system using both block and stream ciphers.
   c. A system using both digital signatures and encryption.
16. Why does PGP generate a signature before applying message compression?
   a. Because the uncompressed message is the readable original.
   b. Because message compression is optional.
   c. Because the compression algorithm may randomize output.
17. What is S/MIME?
   a. A security enhancement to a network management format standard.
   b. A security enhancement to an e-mail standard.
   c. A security enhancement to an integrity management standard.
18. What is the difference between an authoritative and a nonauthoritative SNMP engine?
   a. The difference is who is the generator of an SNMP command.

   b. The difference is who determines the correct clock.
   c. The difference is who is the SNMP manager.

19. What is the purpose of SNMP key localization?
   a. To enable a principal to use locally stored crypto keys.
   b. To enable a principal to share a unique crypto key with each agent from a single locally stored key.
   c. To enable a principal to perform a distinct Diffie-Hellman key exchange with each agent.
20. Why are the public-key certificates used in the lab assignment based on the X.509 standard?
   a. Because this is the best and most flexible format available.
   b. Because this is the only certificate format currently available.
   c. Because this is the most widely applied standard available.
21. What is the purpose of using “nonce” in an interactive authentication protocol?
   a. It enables detection of message replay attack.
   b. It confirms the identity of the sender.
   c. It enables verification of received message integrity.
22. What is a reference monitor?
   a. A security policy that monitors the access control.
   b. A conceptual mechanism that monitors network traffic.
   c. A conceptual mechanism that performs access control.
23. What is a ‘covert channel’ in the context of information security?
   a. Means of communication unintended by the system designers.
   b. Secret group communication channel.
   c. Communication channel protected against traffic analysis.
24. What is ‘discretionary access control’?
   a. A class of security policies that determines access rights of subjects to objects.
   b. A class of access control policies where access rights are set by the owner.
   c. A security policy that must be kept confidential.
25. What is a message authentication code (MAC)?
   a. A secret-key cryptographic function value of a given message input value.
   b. A one-way hash function value of a given message input value.
   c. Can be any of the above.

Part II. (30%) Digital Certificates

Picture yourself given the responsibility of setting up and running a company's SSL enabled web server using mutual client/server authentication by means of digital certificates. Your manager (examiner) wants to get consise answers to the following:

26. What is an X.509 certificate, and what are the main data fields?(3%)
27. Give two validity criteria for X.509 certificates?(3%)
28. Give three good reasons for revoking certificates.(4%)
29. How can X.509 certificates be revoked?(5%)
30. Propose a certificate hierarchy that can be used for the web server. Make a drawing and explain the meaning of the hierarchy relations (1-2 pages). (5%)
31. Explain how the SSL Handshake protocol uses the certificates to establish mutual authentication (1-2 pages). (10%)

Part III. (20%) Asymmetric Cryptography

Alice will use the RSA function to sign a message m:

$$s = m^d \bmod n$$

She sends the signed message (m, s) to Bob.

32. How does Alice compute the parameter values of n and d for her function? (1%)
33. How can Bob authenticate the message from Alice? (1%)
34. Assume there are no specific format requirements on the messages from Alice. Propose a method for Bob to generate a new message m^* with a forged signature of Alice, without using Alice's private key. (3%)
35. Alice will use a hash function $h(.)$ to secure against Bob's method of signature forgery. What five properties should Alice require of this function? (4%)
36. How are signing and authentication performed using this hash function? (1%)

Bob asks Alice to protect the messages sent to him against eavesdropping, by using a randomizing public-key cryptosystem (ElGamal). Bob's private key is k, his public key is $K = g^k \bmod p$, where p is a large prime and g is a generator. Alice receives the parameters (p, g, K) and is now able to encrypt like this:

E (PK, m) := {
Random r;
$c := m\, K^r \bmod p$;
return $(c, g^r \bmod p)$ }

37. Show how Bob can decrypt messages from Alice? (Hint: Use his private key). (10%)