Information about the exam:

Here is some information about the expected answers to the exam questions and/or where you can find them in the book.

1. Acronyms
    1. 3DES - Triple Data Encryption Standard
    2. DDoS - Distributed Denial of Service
    3. PKI - Public Key Infrastructure
    4. RSA - Rivest-Shamir-Adleman
    5. SNMP - Simple Network Management Protocol
    6. TOR - The Onion Router
2. Security services defined in X.800
    * course book, p.12: authentication, access control, data confidentiality, data integrity, nonrepudiation
3. Symmetric vs. asymmetric cryptography
    * course book, p.29-30, 74-76
4. Link encryption vs. end-to-end encryption
    * course book, p.51-52
5. MAC
    * course book, p.61-62
6. Digital signature
    * course book, p.85
7. Environmental shortcomings of Kerberos v4
    * course book, p.108
8. Services of PGP
    * course book, p.134: digital signature, message encryption, compression, email compatibility, segmentation
9. IPsec scenario
    * course book, p.180
10. Services of IPsec
    * course book, p.183: access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality, limited traffic flow confidentiality
11. Web security threats
    * course book, p.224
12. Approaches to Web security
    * course book, p.225: network level (ex. IPsec), transport level (ex. TLS), application level (ex. S/MIME)
13. Classes of intruders
    * course book, p.301: masquerader, misfeasor, clandestine user
14. Intrusion detection
    * course book, p.305: statistical anomaly detection with threshold detection and profile based detection, rule-based detection with anomaly detection and penetration identification

15. Malicious software
    * course book, p.334: definitions
16. Types of viruses
    * course book, p.339: parasitic, memory-resident, boot sector, stealth, polymorphic, metamorphic
17. Antivirus software
    * course book, p.344-345
18. Firewalls
    * course book, p.358
19. Packet-filtering router
    * If the first fragment is missing, reassembly will be impossible and the packet is discarded.