Test

Please answer yourself the following question. This test will hopefully help you to better understand the current level of your knowledge regarding IT security and cryptography.

1. Assume your task is to design a secure IT system. What are the three questions you have to ask yourself / your client (i.e. that are the main areas / things you have to think about)?
2. What are protection goals (other term: security goals)? Name a few of them and describe their meaning
3. What is an attacker / attacker model? Why does one need to think about it?
4. How can we classify / describe attackers / attacker models? Name a few of them or give examples and describe them.
5. What are the fundamental operations of (classical) ciphers?
6. Assume you found a ciphertext and you know, that a classical cipher was used for encryption. How could you find out, which method was (possibly) applied? How can you try to decrypt it?
7. What does perfect security (also known as: information theoretic security) mean? Can we achieve it? If yes, how?
8. How can we classify / categorize cryptographic algorithms? Name and briefly describe the different categories / classes.
9. What does “Kerckhoff’s principle” mean?
10. How can we classify / categorize different types of attacks against cryptographic algorithms? Name and briefly describe the different categories / classes.
11. What does “semantically secure” mean?
12. Describe the main idea / basic concept of security proofs.
13. Describe (e.g. with the help of a drawing) how symmetric encryption works in general. (Assume Alice wants to send a message to Bob). Do the same for asymmetric encryption.
14. What are the requirements with respect to the nonce / initialisation vector then using CBC mode (and why)?
15. Assume you want to protect the integrity of a message sent from Alice to Bob. How does it work (in general) if you would use symmetric cryptography? And how if you would use asymmetric cryptography?
16. Name and describe properties of a cryptographic hash function.
17. Describe the Birthday Paradox and explain its relevance with respect to cryptography.
18. Describe the Merkle-Damgård construction for hashing a message.
19. How can we organise the key exchange?
20. How does the Diffie-Hellman-Key-Agreement work?
21. Explain how and why RSA works.
22. What are problems of using the naïve / plain version of RSA? What measure should one take to enhance the security?
23. What does “hybrid encryption” mean?
24. What does “factoring problem” mean? What does “discrete logarithm assumption” mean?