CSH6 Ch 37 (PKI) Review Questions

1. The organizations that issue digital signatures for public keys in the PKI are ___
2. The most widely-used standard for public-key certificates is ___
3. The fundamental purpose of the public-key infrastructure is ___
4. If a group of 100 people need to engage in pairwise encrypted communications using secret-key cryptography, how many secret keys will the group need?
5. Which of the following statements is/are correct?
6. It is important to enable the name constraint extension in X.509 ___
7. Which type of CRL is most likely to be the shortest among the following?
8. What is the maning of the acronym RA in discussions of the PKI?
9. Public-key certificates are often encoded for use in email using ___
10. Which of the levels of trust defined by the OMB M-04 section 2.1 is this: little or no confidence in asserted identity's validity?
11. Fundamental problems of secret-key cryptography include ___
12. What is the acronym for the list that includes the time a CA was notified of the revocation of a public key?
13. Why should all certificates have an expiration date?
14. The PKC is superior in practical terms to secret-key cryptography because ___
15. In public-key cryptosystems, a message encrypted using a private key can be decrypted by ___
16. Why would two organizations cross-certify their CAs?
17. A user wants to arrange for key recovery of the secret key _S._ However, to increase security, the user wants to send the key to two recipients A and B encrypted using each person's public key (Ka and Kb, respectively) so that they have to cooperate (or collude) to recover the key S. This goal may be achieved by sending both A and B the ciphertext ___
18. What is the correct term for a list of revoked PKI certificates?
19. Certificates and CRLs may be distributed most readily using ___
20. Which of the following fields is/are included in each certificate issued by a CA?
21. If a group of 1000 people need to engage in pairwise encrypted communications using secret-key cryptography, how many secret keys will the group need?
22. The trust model used by PGP is known as a ___
23. If Alice is planning to communicate securely with Bob using PKC and Charlie posts a public key in Alice's name so Charlie can intercept communications between Alice and Bob, this is known as a ___
24. What must PKI software do before trusting any public key?
25. Which of the levels of trust defined by the OMB M-04 section 2.1 is this: high confidence in asserted identity's validity?
26. Which of the following is/are fundamental(s) of the PKI?
27. A CRL is a ___
28. In public-key cryptosystems, a message encrypted using a public key can be decrypted by ___
29. The advantage for the PKI of encoding public-key certificates for inclusion in email is that the encoded certificates ___
30. Which of the following is/are (an) element of the PKI certificate policy for any CA?