CSH6 CH 7 Part 2 – PKC

1. How does Charlie send Darlene a message using the PKC that only he can have digitally signed to prove its origin and its integrity?
2. Roughly when was PGP invented?
3. In practice, how does an e-mail system that supports the PKC decrypt e-mail that was sent to many different recipients?
4. What's the acronym of the open-source equivalent of PGP that follows the OpenPGP Internet Standard (RFC 2440)?
5. Using the PKC, we can generate keys K1 and K2. If K1 is designated as the public key, what is the designation of K2?
6. When we encrypt a cleartext with one of the keys created with PKC, how do we decrypt the ciphertext?
7. How many keys are generated in a single operation in the PKC?`
8. How does Albert decrypt a message that was sent to him using the PKC by Betty, who encrypted it so that only Albert can read it?
9. In what decade did cryptographers discover/invent the PKC?
10. How does one validate a public key using PGP?
11. How does a system using the PKC test the digital signature of a received, signed document?
12. What do the initials RSA refer to?
13. Using the PKC, we can generate keys X1 and X2. If X1 is designated as the private key, what is the designation of X2?
14. What's the name of the method used for validating that a published public key was really created by the person associated with it?
15. Who created the first versions of PGP?
16. In practice, how does an e-mail system that supports the PKC encrypt e-mail to allow many different recipients to decrypt the ciphertext?
17. How do we encrypt a message using the PKC so only the desired recipient, Albert, can read it?
18. How does a system using the PKC "sign" a document to ensure authenticity and integrity during transmission?
19. What does PKC mean in information assurance?
20. Which of the following is the name of the open-source equivalent of PGP that follows the OpenPGP Internet Standard (RFC 2440)?
21. Which of the following functions are supported by the PKC?
22. What almost always happens in the PKC when even a single bit of a digitally signed message is altered in transit?
23. What is the key comparison that confirms the integrity and authenticity of a file or message that was signed using the PKC?
24. What is the origin of the name "PGP"?
25. Which of the following scientists was/were involved in creating the PKC?
26. How does Darlene handle a message from Charlie that he encrypted using the PKC to prove its origin and its integrity?
27. What is PGP?