Preguntas sobre Criptografía y cifrado

Leer con atención el tutorial en la página http://www.cert.fnmt.es/popup.php?o=faq (conceptos básicos) y contestar a las siguientes preguntas

1. **En qué consiste el cifrado de un mensaje.**
2. **¿Qué tipos de cifrados digitales conoces?**
3. **Describe el proceso seguido en la criptografía de clave simétrica al enviar un mensaje de la persona A a la B.**
4. **¿Cuál es la principal ventaja y desventaja de la criptografía de clave simétrica?**
5. **¿Qué tiene que conseguir un hacker para descifrar un mensaje cifrado con clave simétrica?**
6. **¿Cuántas claves utiliza el cifrado simétrico? ¿y el asimétrico?**
7. **¿Cuál es la criptografía más apropiada para el cifrado de grandes cantidades de datos?**
8. **Describe el proceso de envío de un mensaje de la persona A a la persona B con criptografía de clave asimétrica.**
9. **¿Qué tipo de criptografía no necesita enviar la clave para poder descifrar el mensaje?**
10. **¿Qué método se utiliza para mejorar la velocidad en el cifrado de clave asimétrica?**
11. **Describe el proceso de utilización de un algoritmo de clave pública junto a uno de clave simétrica cuando A envía un mensaje a B.**
12. **¿Cómo se llama y como se genera la clave simétrica utilizada en el proceso anterior de criptografía asimétrica?**
13. **En el proceso de utilización de clave pública junto a uno de clave simétrica, ¿se envía algún tipo de clave?**
14. **¿Cómo se cifra la clave de sesión en un cifrado asimétrico, en un mensaje enviado de A a B?**
15. **¿Qué garantiza el proceso de utilización de un algoritmo de clave pública junto a uno de clave simétrica?**
16. **¿Qué es una firma digital?**
17. **¿Qué ofrece la firma digital?**
18. **Indica la diferencia entre la firma digital y un cifrado de mensaje con clave asimétrica.**
19. **¿Qué es una función hash?**
20. **Describe el proceso de envío de un mensaje con firma digital de la persona A a la B.**
21. **¿Cómo se garantiza la unicidad de las claves privadas?**
22. **¿Cuál es la función de un certificado digital?**
23. **Define un certificado digital.**
24. **¿Qué información suele contener un certificado digital?**
25. **¿Cómo confiar si un certificado digital es válido o está falsificado?**
26. **¿Qué es una Autoridad de certificación?**
27. **¿Cuál es la diferencia entre exportar el certificado con clave privada o sin ella?**
28. **¿Qué es una infraestructura de clave pública?**
29. **¿Cuáles son los principales servicios ofrecidos por las infraestructuras de clave pública?**
30. **¿Quién compone las infraestructuras de clave pública?**