Examen.pdf

user_2709007

Seguridad de la Información

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

Preguntas del examen de febrero 2022

No están escritas exactamente de la misma manera pero tenéis la idea general (lo siento por los errores de idioma soy erasmus).

1. ¿Cuáles son los 5 servicios de seguridad ?
2. ¿Por qué se usa una clave de sesión en criptografía simétrica ?
3. Como se puede descifrar Ek1(Ek2(Ek3(H(M)))) ?
4. Esquema de la función central del DES, se debe explicar los parámetros
5. Explica que es el modo ECB y porque se prefiere usar el CBC y porque GCM es el mayor
6. Explicar el funcionamiento de la firma digital y de la función MAC
7. Protocolo de la compartición de clave de Diffie Hellman (esquema)
8. Diferencia entre modelos pull y push y dar un ejemplo
9. Que tipo de ataque se puede hacer en esta transmisión y como evitar esto ?
10. Explica rápidamente el modelo RBAC y Explica rápidamente el modelo DAC y la diferencia con RBAC
11. Cálculo de protocolo de compartición de secreto (2,3) con un valor secreto 4, dar los valores para los 3 usuarios
12. Si un atacante roba una bbdd con contraseña cifradas solas, que puede hacer y cómo evitarlo ?
13. Cuales la firma en grupo y que diferencias tiene con la firma en anillo
14. Modelo normal de autenticación de IKE (esquema)
15. Muestra como esta el paquete con ESP y AH en modo transporte de IPSec (esquema a hacer)