Criptografía
SERIE TEMA 4: CRIPTOGRAFÍA SIMÉTRICA
MC María Jaquelina López Barrientos

1. Qué algoritmo es el antecesor de IDEA?

2. Por quiénes fue mejorado IDEA y con qué finalidad?.

3. Explique las principales características de IDEA

4. Qué diferencia presenta IDEA con respecto a los cifradores Feistel?

5. Cuáles son las características del algoritmo Blowfish?.

6. De qué tamaño son los bloques de Mcla que puede procesar Blowfish, con cuántas claves y en cuántas rondas?.

7. Argumente las razones por las que se puede decir que el algoritmo Blowfish es un algoritmo compacto.

8. Investigue las mejoras presenta Twofish frente a Blowfish?

9. Haga un cuadro comparativo que permita ver la evolución de los algoritmos RCs.

10. Cuál es el objetivo de los algoritmos A5?

11. En qué año fue desarrollado el algoritmo A5 y cuáles son las versiones en que éste fue creado?

12. Previamente a la transmisión de cualquier trama se lleva a cabo un proceso de sincronización entre los participantes, qué tipos de sincronización se realizan?

13. El algoritmo A5/1 utiliza una clave de usuario y un vector de inicialización que en total suman 86 bits que se almacenan en la tarjeta SIM del celular. Explique cómo y para qué se utiliza esta secuencia binaria.

14. Qué tipo de registros utiliza A5/1 en la generación de la secuencia cifrante para proteger las comunicaciones móviles ?

15. Para reforzar los algoritmos A5/1 y A5/2 se creó A5/3. En qué año, con qué objetivos?

16. Explique de manera general cómo opera A5/3

17. Investigue el algoritmo GOST (principales características)

18. ¿Cuál es el nivel de seguridad que ofrece GOST?

19. En el algoritmo DES ¿qué se logra trabajar con la función *f*?

20. ¿Porqué 3DES y no 2DES?.

21. Mencione las principales características por las que el algoritmo Rijndael fue elegido AES.

22. ¿A qué se llama claves débiles y qué características presentan?

23. ¿Qué son los ataques algebraicos?

24. Compare los métodos criptográficos clásicos y modernos vistos e identifique ventajas, desventajas y las características principales que los distinguen entre sí.

25. ¿Con qué objetivo se desarrolló WEP?

26. Haga una tabla comparativa con las principales características de WEP-40, WEP-104, WEP-232 ?

27. Cuáles son los métodos de autenticación que utiliza WEP?

28. Qué mejoras presentan respectivamente WPA y WPA2?

29. Cómo es que SSH hace las comunicaciones seguras?

30. Qué servicios de seguridad proporciona SSH?

31. Cuáles son los principales algoritmos que utiliza SSH y cómo la hace?

32. Cuál es el propósito de PKI?

33. Qué es un certificado digital y cuá es su importancia?

34. Qué es una autoridad certificadora?