INGENIERÍA DE SOFTWARE

CRIPTOGRAFÍA

Guía de Estudio Examen Parcial 1

1.- ¿Qué es la criptografía?

2.- Explique los motivos por los cuales la criptografía se considera una ciencia importante hoy en día

3.- ¿De qué manera están involucradas la Teoría de la Información y la Teoría de Números en la criptografía?

4.- ¿Cuál es la diferencia entre la criptografía y el criptoanálisis?

5.- ¿Qué es un criptosistema?

6.- Explique de manera general la forma de funciomaniento de un criptosistema de clave privada

7.- Explique de manera general la forma de funcionamiento de un criptosistema de clave pública

8.- Explique de qué manera se mezclan los criptosistemas de clave privada y los de clave pública para lograr un sistema eficiente en la práctica.

9.- Explique el concepto de “esteganografía”

10.- ¿Por qué es importante tomar en cuenta la vida útil de la información que se pretende proteger al momento de elegir el criptosistema que se utilizará?.

11.- Explique de manera general el concepto de “firma digital”

12.- ¿Cuál es el principio básico de la criptografía?

13.- ¿Cuál se considera el primer caso claro del uso de métodos criptográficos?

14.- ¿A qué se refiere el término “cifrado de sustitución”?

15.- ¿A qué se refiere el término “cifrado polialfabético”?

16.- ¿Cuál es la diferencia entre los ataques pasivos y los ataques activos a la información?

17.- ¿Cuáles de los siguientes conceptos son ofrecidos por los sistemas de cifrado vistos hasta ahora? En cada concepto justifique por qué si o por qué no.

- Confidencialidad
- Integridad de los datos
- Autenticación del origen de los datos

18.- Si se desea cifrar información valiosa para determinada empresa, ¿Usted utilizaría algún algoritmo clásico ya conocido o uno novedoso desarrollado específicamente para ese caso? ¿Por qué?

19.- ¿Qué es la Teoría de la Información?

20.- Explique el concepto de “entropía de la información” dentro de esta área.

21.- Explique el concepto de “confusión” en criptografía

22.- Explique el concepto de “difusión” en criptografía

23.- Explique si el cifrado cesar implementa “confusión” y/o “difusión” y por qué?

24.- Explique el concepto de “Avalancha” en criptografía

25.- ¿Qué es el peso de Hamming?

26.- ¿Qué es la distancia de Hamming?

27.- ¿A qué se refiere el Kerckhoff´s principle/Shannon´s maxim?

28.- ¿Qué es un conjunto reducido de residuos módulo n?

29.- ¿Cuándo se dice que dos números son coprimos?

30.- Escriba 5 ejemplos de pares de números coprimos

31.- Calcular los siguientes conjuntos:

- Z_8
- Z_{10}
- Z_{15}
- Z_{18}
- Z_{19}

32.- Aplicar el algoritmo extendido de Euclides para encontrar las siguientes inversas:

- Inversa de 25 módulo 16
- Inversa de 254 módulo 15
- Inversa de 29 módulo 32
- Inversa de 127 módulo 56
- Inversa de 415 módulo 72

33.- Verificar si se cumplen o no las siguientes congruencias:

- $25 \equiv 7 \mod 4$
- $18 \equiv 27 \mod 3$
- $23 \equiv 51 \mod 7$
- $72 \equiv 30 \mod 4$
- $66 \equiv 21 \mod 6$

34.- Resolver los siguientes sistemas de congruencias utilizando el teorema chino del residuo

- Sistema 1:
    - $X \equiv 1 \mod 2$
    - $X \equiv 5 \mod 7$
    - $X \equiv 1 \mod 3$

- Sistema 2:
  - $X \equiv 2 \bmod 5$
  - $X \equiv 4 \bmod 7$
  - $X \equiv 5 \bmod 9$
- Sistema 3:
  - $X \equiv 2 \bmod 3$
  - $X \equiv 3 \bmod 4$
  - $X \equiv 0 \bmod 5$
- Sistema 4:
  - $X \equiv 6 \bmod 7$
  - $X \equiv 2 \bmod 6$
  - $X \equiv 1 \bmod 5$
- Sistema 5:
  - $X \equiv 8 \bmod 13$
  - $X \equiv 3 \bmod 11$
  - $X \equiv 5 \bmod 8$

35.- ¿Por qué es importante la exponenciación modular en criptografía?

36.- ¿Por qué el método de exponenciación binaria es más eficiente que el método tradicional?

37.- ¿Por qué es importante el concepto de números primos en criptografía?

38.- ¿Por qué es importante el concepto de factorización en criptografía?

39.- Aplicar el algoritmo de factorización de Fermat para factorizar los siguientes números:

- 416
- 724
- 2564
- 10865
- 119360

40.- ¿Qué es una prueba de primalidad?

41.- ¿Cuál es el método más sencillo (pero ineficiente) para comprobar si un número es primo o no?

42.- Aplicar el método “raíz de n” para encontrar si los siguientes números son primos o no:

- 26
- 79
- 117
- 228
- 317

43.- ¿Cuál es la idea general de la prueba de primalidad de Fermat?

44.- ¿Cuál es la idea general de la prueba primalidad de Wilson?