E41-M41 POOL EXAMEN FINAL CRIPTOGRAFIA I AÑO 2017

1. Hallar d = mcd(1020,1920) y expresar d como combinación lineal entera de 1020 y 1920.

2. Un cifrador afín transforma caracteres m (A=00, B=01, … , Z=25) en caracteres cifrados c por medio de la ecuación c = 19 m + 7 (mod 26). Hallar m sabiendo que c = 22.

3. Un administrador de seguridad informática decide incrementar drásticamente la seguridad de logon a la red interna modificando la política de asignación de claves de acceso para los usuarios, actualmente de 5 caracteres alfabéticos (Mayúsculas). ¿Qué le conviene más, permitir el uso de mayúsculas y minúsculas o incrementar la longitud de claves de 5 a 10 caracteres? Justificar la respuesta.

4. ¿Qué condición esencial cumple el 3DES 168 bits (encripción DES → desencripción DES → encripción DES) para ser considerado esencialmente más seguro que DES 56 bits (del que se sabe que está quebrado)? Opinar con fundamento.

5. Hallar la clave K común del algoritmo Diffie-Hellman si partimos de los siguientes parámetros: p=29, alfa = 7, x = 6, y=2

6. Para un sistema RSA con p = 79 y q = 83, nos dicen que podemos usar cualquiera de las siguientes claves públicas:

   a) e = 24
   b) e = 13
   c) e = 25
   d) e = 49

   ¿Cuáles de ellas son válidas y cuáles no? Justificar la respuesta.

7. Determinar si 5 es un elemento primitivo módulo 17.

8. Supongamos que 100 usuarios desean comunicarse entre sí, usando un criptosistema simétrico. Cada usuario insiste en comunicarse con cada uno de los otros, sin que el resto de los 98 usuarios se enteren de lo informado.

   a) ¿Cuántas claves K deben desarrollarse?
   b) ¿Cuántas claves son necesarias si se utiliza un sistema de clave pública?

9. Supongamos que un usuario define claves RSA con un módulo n de 308 dígitos decimales (1024-bits) y define e=3 como su clave pública. Indicar cómo un atacante que desconozca la clave privada, puede recuperar mensajes cifrados cuando dicho mensaje consista en un único número secreto que no supere 10100.

10. Un criptógrafo encripta un texto con DES-56 y al resultado lo reencripta con AES-256. Opinar acerca de la veracidad de los siguientes enunciados:

    a) La preencripción con DES fortaleció al protocolo empleado.
    b) La seguridad del protocolo no varía si se invierte el orden de los cifradores.
    c) El texto cifrado no varía si se invierte el orden de los cifradores (usando las mismas claves).

11. Un administrador de seguridad de una comunidad electrónica decide simplificarle los procedimientos a sus usuarios generando por su cuenta las claves públicas y privadas de cada usuario. Luego le distribuye a cada uno su privada y coloca en un repositorio público todas las claves públicas. ¿Qué problemas legales puede llegar a enfrentar?

12. Un CSP (Cryptographic Service Provider) ha optimizado el tiempo de generación de números seudoprimos aleatorios de 512 bits para su RSA 1024. Para ello, genera un pool de números seudoaleatorios de 32 bits con un generador de calidad criptográfica NBCSPRBG (Algoritmo BBS). Luego multiplica esos números al azar hasta obtener números del rango 512 bits y verifica su seudoprimalidad (Rabin-Miller). ¿Qué opina al respecto?

13. Hallar mediante el algoritmo de Euclides Extendido 213^{-1} mod 2048.

14. Encontrar la menor solución no negativa del siguiente sistema de congruencias:

$$x \equiv 2 \bmod 9$$
$$x \equiv 3 \bmod 10$$
$$x \equiv 4 \bmod 11$$

15. Calcular 5^{579} mod 29

16. Describir los pasos necesarios para configurar y utilizar el Protocolo de Diffie-Hellman de Intercambio de Claves. Detallar las dificultades eventuales en su implementación y todos los pormenores que considere importantes.

17. Describir los pasos necesarios para configurar y utilizar un One Time Pad. Detallar las dificultades eventuales en su implementación y todos los pormenores que considere importantes.

18. Describir los pasos necesarios para configurar y utilizar el Algoritmo de Cifrado RSA. Detallar las dificultades eventuales en su implementación y todos los pormenores que considere importantes.

19. RSA es un algoritmo que presenta simetría en el uso de las claves (se puede encriptar con cualquiera y desencriptar con la otra). Sin embargo, no se aconseja utilizar la misma clave para encriptar y firmar mensajes. Indicar por qué.

20. Demostrar que la composición de dos cifrados Vigenère resulta en un cifrado del mismo tipo. Derivar la clave del cifrado obtenido en función de las claves de los dos cifrado originales.

21. Se dispone de una secuencia binaria que cumple con los tres Postulados de Golomb. ¿Están aseguradas las condiciones para su empleo criptográfico? Justificar brevemente la respuesta.

22. Una secuencia seudoaleatoria generada por un LFSR posee una longitud de 4095 bits. Calcular el número de celdas del LFSR, considerando que el polinomio de conexión del dispositivo es primitivo.

23. Un LFSR de 256 celdas genera una secuencia de bits:

    a. cuyo período es de 16 bits. ¿Por qué es tan corta? Aportar alguna explicación.
    b. que consiste exclusivamente de bits nulos. Explicar.
    c. que se repite cada 2^{256} bits generados. ¿Le llama la atención este comportamiento? ¿Por qué?
    d. que posee exactamente n bits 1 y (n-1) bits 0. ¿Es posible que esto ocurra? Explicar.

24. Para crear una función de hash de 256 bits, se decide realizar el siguiente procedimiento: Tomar $H_1(x)$ y $H_2(x)$ dos funciones de hash iterativas de 128 bits Calcular $H(x) = H_1(x)||H_2(x)$, donde || significa concatenar. ¿Es la función de hash H más segura que H_1 y H_2? ¿Por qué?

25. Se decide usar un autómata celular caótico de 1024-celdas para generar una función de hashing iterativa de 512-bits. Explicar cómo se podría concretar.

26. Indicar tres condiciones que deben cumplir las funciones de hashing para ser consideradas criptográficamente seguras.

27. Indicar cómo procedería para generar colisiones de hashing empleando el ataque de cumpleaños.

28. ¿Qué ventajas ofrece la pre-compresión reversible (zipeado) de un mensaje antes de ser cifrado?

29. Si al usar AES-256 en modo operativo CBC se decide mantener en secreto el vector de inicialización (I.V.), generándolo a través de un intercambio Diffie-Hellman. ¿Aporta alguna ventaja a la seguridad del cifrado la combinación elegida? Justificar la respuesta.

30. Un sistema dinámico determinista genera una secuencia de bits supuestamente caótica. ¿Qué método (o métodos) aplicaría para verificar empíricamente este hecho?

31. Se dispone de dos secuencias seudoaleatorias de buena calidad criptográfica cuyos respectivos períodos son seudoprimos. Si en vez de usar alguna de ellas se decide combinar los bits generados con un XOR, se ganaría o no en la seguridad de un cifrador de flujo Vernam?

32. Si la empresa Los Inquebrables S.A. le ofrece implementaciones de métodos simétricos como AES y de asimétricos como RSA, describir en detalle como procedería a evaluarlos.

33. Supongamos que cada usuario de una red de n usuarios desea establecer comunicación con cada uno de los otros. Cada uno tiene una estación de trabajo segura, pero cualquiera puede observar los mensajes enviados a través de la red. Cada usuario insiste en que sus mensajes lleguen a destino sin que ninguno de los n-2 restantes usuarios tenga acceso a él. Determinar la menor cantidad de claves que se necesita establecer (fuera de la red) para satisfacer estos requerimientos, utilizando por una parte un algoritmo simétrico, y por la otra utilizando un algoritmo de clave pública.

34. Sean p=13 y q=11. Elegir exponentes privado y público (d y e) de forma adecuada para un RSA. Cifrar luego el mensaje UBA letra por letra, según la correspondencia A=0, B=1, ...etc.. (el sistema puede cifrar únicamente caracteres alfabéticos)

    a) ¿Qué ocurre con el cifrado de la B y la A? ¿Cómo modificaría el sistema para evitar mensajes fácilmente criptoanalizables?
    b) ¿Cómo modificaría el sistema para ocultar la distribución de los elementos del texto plano?

35. Los parámetros públicos de un cierto RSA son n=1919 y e=7. Factorizar n y calcular el entero d a partir de φ(n). Determinar una codificación que permita cifrar textos conteniendo caracteres en mayúscula y cifrar la palabra POOL. Luego descifrarla explícitamente.

36. Supongamos que trabajamos con un esquema RSA determinado por los siguientes parámetros:

    (e; n) = (31; 69932689)

    Dados los siguientes mensajes con sus firmas asociadas:

    $(M_1; S_1) = (1997; 4530763)$ y $(M_2; S_2) = (1453; 40142461)$,

    obtener las firmas de los siguientes mensajes:

    $M_3 = 2901641 = M_1.M_2$
    $M_4 = 3988009 = M_1^2$
    $M_5 = 2111209 = M_2^2$

37. Alicia y Pedro suelen comunicarse utilizando RSA y la siguiente clave pública (e, n) = (5, 967331). Por un descuido de Alicia, Oscar se apodera de φ (n) = 965352. Se pide:

    b. Mostrar cómo puede hacer Oscar para hallar la clave privada (d, n)

    c. Ahora que Oscar tiene (d, n), ¿qué daños puede ocasionar a Alicia y Pedro, sin que estos se den cuenta?

    d. Es claro que se necesita φ(n) para determinar valores válidos de e y de d. ¿Qué tenemos que hacer con φ(n) una vez que ya no lo utilizamos?

38. Consideremos la siguiente implementación de RSA. Una autoridad confiable elige dos primos grandes p y q y computa n = p*q que será utilizado por todos los usuarios. La autoridad le brinda a cada usuario una clave privada d_i y una clave pública e_i tal que $e_i \neq e_j$ si $i \neq j$.

    a. Probar que si dos usuarios, i y j, para los cuales $(e_i,e_j)=1$ reciben el mismo mensaje m, un intruso puede reconstruir m usando $n, e_j, e_j, m^{ei}, m^{ej}$
    b. Deducir conclusiones acerca de la seguridad de este sistema.