Nota: ..... Parciales: ..... Final: .....

Apellidos: ..... Grupo: .....

Nombre: ..... nif: ..... nº hojas: .....

Asiste a revisión: Sí □ ..... No □

Seguridad y Protección de Sistemas Informáticos

Grado en Ingeniería Informática

19/01/2021

1. (hasta 2.5 puntos) A lo largo del curso hemos tenido ocasión de estudiar con bastante profundidad el criptosistema de Vigenère. Hoy pretendemos recorrer algo que quedó pendiente y es lo siguiente:

   a) Dado un mensaje M de texto llano a cifrar con el criptosistema de Vigenère, razone e implemente[1] un método para generar una clave "aleatoria" de la misma longitud que M.

   b) Cifre mediante la cifra de Vigenère (implementado en la Tarea 2) el texto llano que obtuvo en el ataque llevado a cabo en la Tarea 4, y hágalo con una clave de su misma longitud obtenida con lo implementado en el apartado anterior.

   c) Aplique las herramientas de laboratorio de sus Tareas 2 y 3 para atacar el criptograma obtenido en el apartado anterior y explique las conclusiones a las que llegue.

2. (hasta 2.5 puntos) En cuanto a AES:

   a) Implemente razonadamente una función, digamos `sbox(x,y)`, que dado un byte `xy` sea capaz de aportar la entrada correspondiente a la fila `x` y la columna `y` en la tabla de la Figura 4.4 de los apuntes (pag. 84).

   b) Utilice el código de la pregunta anterior para construir una matriz que corresponda exactamente con el contenido de la tabla de la Figura 4.4. (Entregue el ejercicio en al menos un fichero `.ipynb`)

3. (hasta 2.5 puntos) Diseñe razonadamente el entorno de un ejemplo realista para la comunicación en un círculo que ha elegido al efecto el criptosistema ElGamal. Después introduzca un personaje, digamos Alice, y dótelo de una clave pública para que otro personaje, digamos Bob, le envíe un mensaje breve de su elección; al recibir el mensaje cifrado haga que Alice lo descifre con éxito. Para llevar a cabo este ejemplo puede usar `sagemath` y `openssl`, pero el ejemplo que construya debe ser distinto en los datos a cualquiera que figure en los apuntes. (Entregue el ejercicio en al menos un fichero `.ipynb`)

4. (hasta 2.5 puntos) Escenifique compartir el secreto de valor 111332 entre 30 partícipes, requiriéndose el acuerdo de 19 de ellos para explicitar dicho secreto. Use en este ejercicio el esquema de Shamir de intercambio de secretos, pudiendo el alumno servirse de `sagemath` implementando o no su propio software.

5. Aporte, debidamente documentado, el software que desee y que haya implementado usted mismo en relación con la asignatura.

---

[1] Los razonamientos deberán estar editados vía Markdown en celdas de un un fichero `.ipynb`. Todo lo que programe en esta prueba deberá ser en ficheros `.ipynb` indicando si invocó un núcleo de Python o de Sagemath. Si alguien desea entregar un fichero `.py` se le valoraría positivamente, pero no es obligatorio. Recuerde que Jupyter admite código Markdown en las celdas y que en ellas puede escribir segmentos a LaTeX.