Criptografía y Seguridad

Tarea 2

Noviembre 2023

- Fecha de entrega: 26-Noviembre-2023
- La tarea podrá ser entegrada en equipos de máximo dos personas. Puede ser entregada demanera individual.
- Una vez vencida la fecha de entrega la calificación máxima que se podrá obtener es de 8.
- Resuelvanse solo los problemas necesarios para obtener 10 puntos.
- Prohibido usar algún asistente (E.g., ChatGPT) para solucionar la tarea.
- Buscar ejemplos de código en línea es válido, sin embargo, si es identificado plagio se invalidará la tarea en su totalidad.

1. (2 ptos.) Realiza las siguientes operaciones en $GF(2^4)$. Revisar PDF adjunto (operaciones.pdf) para dudas.
   - Adición $(A(x) + B(x)\ mod\ P(x))$ con $P(x) = x^4 + x + 1$
     - $A(x) = x^2 + 1, B(x) = x^3$
     - $A(x) = x^2 + 1, B(x) = x + 1$
   - Multiplicación $(A(x) \cdot B(x)\ mod\ P(x))$ con $P(x) = x^4 + x + 1$
     - $A(x) = x^2 + 1, B(x) = x^3$
     - $A(x) = x^2 + 1, B(x) = x + 1$
2. (3 ptos.) Empleando alguno de los algoritmos de cifrado por bloques visto en clase (DES/AES), realiza lo siguiente.
   - Toma una imagen y conviertela al formato binario PPM. Te puedes ayudar del editor de imagenes GIMP.
   - Los encabezados de la imagen, los cuales contienen los metadatos necesarios para renderizar correctamente la imagen, deben ser removidos y almacenados por separado. Utiliza utilerias de la terminal como se muestra en https://words.filippo.io/the-ecb-penguin/
   - Emplea openssl para cifrar la imagen con el modo de operación ECB y CBC.
   - Una vez obtenidas ambas imagenes, calcular la entropía de las imagenes con el programa adjunto a esta tarea. (entropia.py y su explicación entropia-explicación.pdf)
   - Describir la relavancia de elegir un modo de operación adecuado tomando como base la entropía.
3. (2.5 ptos.) Cifra este documento con $AES - 128$, en el modo de operación CBC con la contraseña $qawsedrftgyhujik$ y un $IV = 1234567890qwerty$. Lo que se solicita para este problema es el $CBC - MAC$, es decir, el último bloque del documento cifrado en hexadecimal. Se deberá entregar el procedimiento empleado y la cadena en hexadecimal (considerese el tamaño de bloque de AES)
4. (2.5 ptos.) Describe como un modo de operación aporta propiedades de seguridad a un esquema de cifrado por bloques. Y describe por que un esquema de cifrado sigue siendo correcto $(e_k(m) = d_k(e_k(m)))$ tomando como ejemplo un mensaje cifrado con AES-OFB.

5. (2.5 ptos.) Los siguientes hashes fueron generados con diferentes algoritmos. Identifica cuales fueron estos algoritmos y procede a "crackear" los hashes empleando hashcat. Como tip, el primer hash es un número, el segundo es un nombre (iniciando con mayuscula) y el tercero es una contraseña del formato mes, año, caracter especial, y sigue la convención mayuscula, minusculas, numeros y caracter especial en orden. Emplea hash identifier para saber tipo de hash se busca crackear.

   - dc513ea4fbdaa7a14786ffdebc4ef64e
   - 53b1fb446230b347c3f6406cca4b1ddbac60905ba4ab1977179f44b8fb134447
   - 47ae5e703e64d5f0a1b41f34254fdd4bc0865c1cb22b714cdc5726d8e1161e40127219fe63cc6ebcd9917db5720069c6e6

6. (2.5 ptos.) Describe en tus palabras la existencia o no existencia de funciones de una sola via, o funciones irreversibles. Demuestra formalmente.