Tarea 1

Criptografía y seguridad 2020-2

Fecha límite de entrega: 13 de febrero

Indicaciones

- Resuelve cada uno de los ejercicios, todos tienen valor de un punto excepto el 3 y el 7.
- Puede hacerse de forma individual o en pareja, en caso de hacerla en pareja basta que se entregue una solución.
- **Sube tu tarea solo cuando estés completamente seguro de que es correcta, ya que solo se puede subir una vez.**
- Escribe los cálculos que realizaste, o en caso de haber usado otra herramienta (como un programa) indícalo en tu respuesta.
- Para los ejercicios que requieren programar utiliza un lenguaje de los siguientes: Python, Java, C o Haskell. Anexa tu código fuente.
- Organiza tus archivos en un archivo `.zip`, incluyendo los datos de los alumnos, y súbelo en `https://forms.gle/ubLqDKRgNsmdZ6Sw5`

Ejercicios

1. Descifra los siguientes mensajes que fueron cifrados con el método de César, probando diferentes desplazamientos hasta que el mensaje tenga sentido. Escribe el mensaje claro y la llave (desplazamiento) que se usó para cifrar.

   a) `SLYDPYQCGLQNGPYBMPY`

   b) `CVVCEMVJGKORNGOGPVCVKQP`

   c) El archivo `imagen.enc` que originalmente era una imagen.

2. Considera la siguiente tabla de cifrado de sustitución simple

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	P	U	B	A	Q	O	Y	G	C	Z	E	F	M	J	V	D	K	I	R	H	L	T	S	N	X

a) Encripta el mensaje

`Criptografia y seguridad`.

b) Escribe la tabla correspondiente que se usa para descifrar, la primera fila debe ser el alfabeto en orden.

c) Usando tu tabla del inciso anterior, descifra el mensaje

`RGFGMOWRRWUZIWKAWIGOMGQGUWMRRYKAWRRJUKNVRJGFVEAFAMRWRGJMI`

d) ¿Cómo sería una tabla de cifrado si los mensajes fueran cadenas de bytes (archivos) en vez de las 26 letras del alfabeto? ¿De qué tamaño sería la tabla?

3. (2 pts.) El texto del archivo `texto.enc` fue cifrado con el método de sustitución simple. El original es un texto en español, encuéntralo.

4. En cada inciso encuentra el valor de x entre 0 y $m-1$ que resuelve la congruencia, donde m es el módulo.

a) $123 + 513 \equiv x \pmod{763}$.

b) $222^3 \equiv x \pmod{581}$.

c) $x - 21 \equiv 23 \pmod{37}$.

d) $x^2 \equiv 5 \pmod{11}$.

e) $x^3 - 2x^2 + x - 2 \equiv 0 \pmod{11}$.

5. Sea $m \in \mathbb{Z}$.

a) Supón que m es impar. Encuentra el entero entre 1 y $m-1$ que es igual a $2^{-1} \pmod{m}$.

b) De forma más general, supón que $m \equiv 1 \pmod{b}$. Encuentra el entero entre 1 y $m-1$ que es igual a $b^{-1} \pmod{m}$,

6. Explica por qué las siguientes funciones no sirven para encriptar mensajes considerando que los espacios de mensajes y llaves son iguales a $\mathbb{Z}/N = \{0, 1, \ldots, N-1\}$.

a) $E(k, m) = km \pmod{N}$.

b) $E(k, m) = (k + m)^2 \pmod{N}$.

7. (2 pts.) Considera el cifrado afín con una llave $k = (k_1, k_2)$.

   a) Usando $N = 101$ y $k = (99, 20)$, cifra el mensaje $m = 100$ y descifra el criptotexto $c = 23$.

   b) Describe un ataque de texto claro conocido para recuperar la llave (k_1, k_2). Observa que la función de cifrado es la ecuación de una recta en el plano, donde las coordenadas corresponden a una letra en claro y una letra cifrada, ¿cuántos puntos de una recta se necesitan para determinar su ecuación?

   c) Aplica tu ataque al archivo cifrado `audio.enc`, que originalmente es un audio en formato MP3. Es posible que tengas que modificar un poco el ataque.

8. Muestra que los esquemas de César, sustitución simple y Vigenère pueden romperse fácilmente con un ataque de texto claro elegido. ¿Cuántos mensajes claros se necesitan para recuperar la llave en cada caso?