Facultad de Ingeniería y Tecnologías
Departamento de Ciencias
Exactas y Naturales
Álgebra aplicada

Proyecto Criptografía

El objetivo de esta tarea es implementar dos sistemas criptográficos y comparar su eficiencia.

La criptografía consiste en un conjunto de herramientas para garantizar la confidencialidad e integridad de la información, cuando la misma se intenta transmitir por un canal de comunicación que está comprometido. La criptografía moderna tiene múltiples aplicaciones en nuestro mundo moderno en lo que refiere a proteger nuestra información, como por ejemplo, nuestras cuentas bancarias, y mucho más.

En esta tarea utilizaremos la siguiente tabla para conversión de letras a números.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z		*
15	16	17	18	19	20	21	22	23	24	25	26	27	28

El caracter asociado al 27 es el espacio en blanco, y asterisco en el lugar 28 fue agregado para tener un total de 29 letras en nuestro abecedario simplificado. El hecho de que 29 es un número primo simplifica un poco el criptosistema que vamos a presentar a continuación.

Trabajaremos exclusivamente con números enteros, y los reduciremos módulo 29 para poder traducirlos a una letra en nuestro criptosistema. Es decir, si n es un entero que no está entre 0 y 28 (esto incluye el caso n negativo), realizamos la división entera $n = 29 \cdot q + r$ donde r es el resto de la división y cumple $0 \leq r < 29$. Luego definimos la reducción módulo 29 de la siguiente forma

$$n \text{ mód } 29 = r$$

Describiremos ahora los criptosistema que queremos analizar. Supongamos que queremos encriptar el mensaje "LA CULPA ES DE CATARINA"

Criptosistema 1

1. Traducir todos los caracteres del mensaje a números entre 0 y 28.
2. Elegir dos números enteros a y b entre 0 y 28, $a \neq 0$.
3. Defina la función de encriptado para cada caracter

$$E(x) = (ax + b) \text{ mód } 29 \quad \text{para } 0 \leq x \leq 28,\ x \in \mathbb{Z}$$

4. Traducir los números codificados a letras y mostrar el mensaje encriptado.

Para nuestro mensaje de ejemplo, la primera letra es la L, que se corresponde con el número 11. Si usamos $a = 3$, $b = 1$ nuestra función de encriptado calcula $E(x) = 3 \cdot 11 + 1 \text{ mód } 29 = 34 \text{ mód } 29 = 5$ por lo que la primera letra del mensaje encriptado será una F.

Se pide:

1) Elija dos números a y b como indica el criptosistema.

2) Elija un texto de por lo menos 100 caracteres para encriptar.

3) Crear una función en Python que realice el encriptado usando este criptosistema. Ejecute esta función para el texto elegido.

4) ¿Cuál es la letra que más se repite en el texto original? ¿En qué posiciones se encuentra?

5) ¿Cuál es la letra que más se repite en el texto encriptado? ¿En qué posiciones se encuentra?

6) Explique una vulnerabilidad que tiene este criptosistema.

7) Asumiendo que un espía conoce los números a, b e intercepta un mensaje encriptado, encuentre un mecanismo para desencriptar el mensaje.

Sugerencia: para su valor de a elegido, encuentre un número entero $\overline{a}$ entre 0 y 28 que cumpla $a \cdot \overline{a}$ mód $29 = 1$. Es posible construir una función de desencriptado usando $\overline{a}$ y b.

8) Crear una función en Python que realice el desencriptado. Ejecute esta función para el texto encriptado y compruebe que se recupera el texto original.

Criptosistema 2

Ahora propondremos una versión vectorial del criptosistema anterior.

1. Separar el mensaje a encriptar en bloques de tamaño 3. Por ejemplo,

   "LA CULPA ES DE CATARINA"→ "LA " "CUL" "PA " "ES " "DE " "CAT" "ARI" "NA "

   Recuerde que los espacios también cuentan. Si no es posible armar el último bloque de 3, agregar espacios al final.

2. Traducir cada bloque a un vector columna en $\mathbb{R}^3$ usando la tabla anterior. Por ejemplo

$$\text{"LA "} \to \begin{pmatrix} 11 \\ 0 \\ 27 \end{pmatrix}$$

3. La función de encriptado se define de la siguiente forma, si $\vec{x} \in \mathbb{R}^3$ es un vector columna entonces

$$E(\vec{x}) = \left(T(\vec{x}) + \vec{b}\right) \text{ mód } 29$$

   donde $T : \mathbb{R}^3 \to \mathbb{R}^3$ es una transformación lineal y $\vec{b} \in \mathbb{R}^3$ es un vector de coeficientes enteros constante. En esta ecuación el "mód 29" significa reducir módulo 29 todas las entradas del vector columna resultante. Para la transformación lineal T pediremos que su matriz asociada tenga coeficientes enteros y determinante igual a 1.

4. Utilizar la función de encriptado para encriptar los bloques de tamaño 3 y mostrar el mensaje encriptado.

Se pide:

1) Elija una transformación lineal T y un vector b como indica el criptosistema.

2) Elija un texto de por lo menos 100 caracteres para encriptar.

3) Crear una función en Python que realice el encriptado usando este criptosistema. Ejecute esta función para el texto elegido.

4) ¿Cuál es la letra que más se repite en el texto original? ¿En qué posiciones se encuentra?

5) ¿Cuál es la letra que más se repite en el texto encriptado? ¿En qué posiciones se encuentra?

6) ¿Presenta este criptosistema la misma vulnerabilidad encontrada en el criptosistema 1?

7) Asumiendo que un espía conoce la transformación T, el vector $\vec{b}$ e intercepta un mensaje encriptado, encuentre un mecanismo para desencriptar el mensaje. *Sugerencia: hallar la transformación lineal inversa a T puede ser útil.*

8) Crear una función en Python que realice el desencriptado. Ejecute esta función para el texto encriptado y compruebe que se recupera el texto original.

Sobre el informe:

- El tiempo para entregar el informe es hasta el sábado 30 de noviembre inclusive. La entrega se realizará por webasignatura.
- El informe deberá estar en formato pdf, la entrega también deberá incluir el proyecto compartido para su fácil ejecución y testeo.
- El informe deberá contener título, fecha, nombre y cédula del estudiante.
- Se evaluará: prolijidad del informe, utilización correcta del idioma español, redacción, prolijidad del código presentado en los scripts, conclusiones.