El Legado de la Sombra

Una aventura de espionaje y criptografía

Encriptación de mensajes por aplicación lineal

Capítulo 1: La Ciudad en la Penumbra

En una época de crisis, la corrupción y la traición han tejido una red que amenaza con desestabilizar la nación. En este oscuro panorama, la Agencia Eclipse opera en las sombras, custodiando secretos vitales para la supervivencia del país.

Tú eres **La Sombra**, un agente de élite conocido por resolver los casos más imposibles. Tu reputación en la Agencia Eclipse es legendaria, pero esta vez, la misión es diferente.

Capítulo 2: El Método de Encriptación Lineal

El Oráculo: "Buenas noches, agente. Hemos detectado que varios de nuestros mensajes han sido interceptados y nuestras formas de comunicación se han vuelto vulnerables."

Tú: "Eso nos deja en una situación crítica, ¿cómo lo piensan solucionar?"

El Oráculo: "Los espías en las filas han creado un nuevo método de encriptación basado en álgebra lineal. Ve con el Profesor, él te explicará el proceso en detalle."

El Profesor: "Un placer conocer al famoso agente 'La Sombra'. El **Oráculo** te envió para que te explique nuestro nuevo método de encriptación lineal, ¿no?"

Tú: "Sí, él me envió."

El Profesor: "Bueno, prepárate porque te voy a explicar cómo encriptamos y desencriptamos mensajes. Es bastante sencillo una vez que entiendes las matemáticas detrás de todo esto. Empecemos, ¿listo?"

Tú: "Adelante, te escucho."

Podemos codificar un mensaje realizando una pequeña biyección entre las letras del alfabeto y los números naturales, donde el cero no tendrá asignado ningún carácter:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

T	U	V	W	X	Y	Z	–
20	21	22	23	24	25	26	27

Cuadro 1: Tabla de codificación del alfabeto

Sea entonces un mensaje compuesto de $m \in \mathbb{N}$ caracteres, donde dado la tabla anterior podemos obtener un arreglo con los números que componen el mensaje. Teniendo entonces que los elementos en el arreglo, son los $x_i \in [0, 27]$ que representan los caracteres del mensaje. Donde el cero está reservado para espacios vacíos.

x_1	$\cdots$	x_i	$\cdots$	x_m

Esta sería una encriptación muy sencilla, pues podría descifrarse investigando qué letra le corresponde a cada número. Ahora dividamos el arreglo en partes iguales, supongamos que dividimos en $n \leq m$

partes iguales, con $n \in \mathbb{N}$, donde si el arreglo no puede ser divisible exactamente podemos aumentar el arreglo. Si $n\lceil \frac{m}{n} \rceil > m$ entonces el arreglo será de $m + (n\lceil \frac{m}{n} \rceil - m)$ entradas, donde estas últimas entradas añadidas a la cadena serían llenadas por el valor cero. Ahora nuestro arreglo sería de longitud $m_1 = m + (n\lceil \frac{m}{n} \rceil - m) = n\lceil \frac{m}{n} \rceil$, donde la longitud de cada subarreglo será $\lceil \frac{m}{n} \rceil$.

x_1	$\cdots$	x_i	$\cdots$	x_m	0_{m+1}	$\cdots$	$0_{n\lceil \frac{m}{n} \rceil = m_1}$

En todo caso, ahora el arreglo es divisible y por lo tanto podemos particionarlo de la siguiente manera.

$(x_1$	$\cdots$	$x_{\frac{m_1}{n}})_1$	$(x_{\frac{m_1}{n}+1}$	$\cdots$	$x_{\frac{2m_1}{n}})_2$	$\cdots$	$(x_{\frac{(n-1)m_1}{n}+1}$	$\cdots$	$x_{\frac{nm_1}{n}})_n$

Ahora hemos armado vectores en $\mathbb{R}^{\frac{m_1}{n}}$, con $n, \frac{m_1}{n} \in \mathbb{N}$.
Notemos que podemos armar una matriz, tomando el elemento inicial de cada subarreglo hasta su último elemento y escribiéndolo de manera vertical.

$$M_{\frac{m_1}{n} \times n} = \begin{array}{|cccc|} \hline x_1 & x_{\frac{m_1}{n}+1} & \cdots & x_{\frac{(n-1)m_1}{n}+1} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline x_{\frac{m_1}{n}} & x_{\frac{2m_1}{n}} & \cdots & x_{\frac{nm_1}{n}} \\ \hline \end{array}$$

Obteniendo así una matriz de $\frac{m_1}{n} \times n$. Ahora podemos modificar la matriz para hacerla más difícil de descifrar. Esto mediante transformaciones lineales.

Sea

$$T : \mathbb{R}^{\frac{m_1}{n} \times n} \to \mathbb{R}^{\frac{m_1}{n} \times n}, \tag{1}$$
$$M \mapsto (E)M = M' \tag{2}$$

Donde $M \in \mathcal{M}_{\frac{m_1}{n} \times n}(\mathbb{K})$, es decir la matriz de caracteres y $E \in \mathcal{M}_{\frac{m_1}{n} \times \frac{m_1}{n}}(\mathbb{K})$, la matriz de encriptación y por lo tanto M' la matriz encriptada, con lo cual transformamos la matriz original en una mucho más complicada de descifrar, aun así dado de que necesitaríamos desencriptar el mensaje, es necesario que E sea invertible, es decir $\exists E^{-1}$ tal que $EE^{-1} = I$, con $E, I \in \mathcal{M}_{\frac{m_1}{n} \times \frac{m_1}{n}}(\mathbb{K})$.

Ahora bien, podemos partir de la matriz identidad para definir a E como el conjunto de operaciones elementales de matrices aplicadas a la matriz identidad $E = (O_n(\ldots(O_1(I))))$, para construir la matriz que nosotros deseemos mediante operaciones elementales. Donde en efecto $E^{-1} = (O_1^{-1}(\ldots(O_n^{-1}(I))))$, así el proceso de desencriptación vendría dado por:

$$T^{-1} : \mathbb{R}^{\frac{m_1}{n} \times n} \to \mathbb{R}^{\frac{m_1}{n} \times n}, \tag{3}$$
$$M' \mapsto (E^{-1})M' = M \tag{4}$$

Recordando que luego las columnas hay que organizarlas como vectores horizontales consecutivos y traducir con la tabla inicial o tomar la traspuesta de la matriz de valores y traducir directamente los valores, así podremos leer el mensaje de izquierda a derecha y de arriba a abajo. Teniendo así que podemos tener cualquier matriz según lo deseemos para encriptar nuestros mensajes, siempre y cuando se use la inversa correspondiente.

Ejemplo: La cadena

H	O	L	A	$-$	M	U	N	D	O

Tenemos $m = 10$, entonces tomemos $n = 3$, entonces $m_1 = 12$ y por lo tanto subarreglos de $\lceil \frac{m}{n} \rceil = 4$, obteniendo así:

8	15	12	1	27	13	21	14	4	15	0	0

Por lo tanto el mensaje en una matriz cifrada sería:

$$M = \begin{array}{|c|c|c|}\hline 8 & 27 & 4 \\ \hline 15 & 13 & 15 \\ \hline 12 & 21 & 0 \\ \hline 1 & 14 & 0 \\ \hline \end{array}$$

Por lo tanto tomemos nuestra matriz 4x4 siguiente:

$$E = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 5 \\ 2 & 3 & 1 & 1 \\ 1 & 0 & 1 & 3 \end{bmatrix}$$

Y por lo tanto

$$E^{-1} = \begin{bmatrix} \frac{-19}{3} & \frac{11}{3} & 3 & \frac{4}{3} \\ 5 & -3 & -2 & -1 \\ \frac{-20}{3} & \frac{13}{3} & 3 & \frac{2}{3} \\ \frac{13}{3} & \frac{-8}{3} & -2 & \frac{-1}{3} \end{bmatrix}$$

Así que

$$M' = \begin{bmatrix} 78 & 172 & 34 \\ 68 & 167 & 15 \\ 74 & 128 & 53 \\ 23 & 90 & 4 \end{bmatrix}$$

Teniendo por último que el mensaje al desencriptarlo, trasponiendo y traduciendo sería:

$$(E^{-1}M')^T = \begin{array}{|c|c|c|c|}\hline H & O & L & A \\ \hline - & M & U & N \\ \hline D & O & 0 & 0 \\ \hline \end{array}$$

Capítulo 3: Los Mensajes Interceptados

Tres mensajes han sido interceptados, esto proviene de un agente de la agencia. Son urgentes. Si los enemigos los descifran antes que tú, el plan estará perdido. Tu misión es encontrar su verdadero significado. Si aciertas al menos dos de los tres mensajes previos, tendrás una oportunidad de completar la misión con éxito.

Primer mensaje: Frecuencia 4 (Bloque 4)

Matriz encriptada:

$$\begin{bmatrix} 175 & 59 & 189 & 107 & 120 & 5 \\ 209 & 52 & 206 & 104 & 113 & 1 \\ 74 & 51 & 104 & 88 & 86 & 9 \\ 99 & 36 & 104 & 28 & 86 & 3 \end{bmatrix}$$

Mensaje descifrado: **“LA TRAICION ESTA CERCA”**
Significado: “Un espía doble se ha infiltrado en la Agencia. Necesitamos actuar con precaución.”

Segundo mensaje: Frecuencia 2 (Bloque 2)

Matriz encriptada:

$$\begin{bmatrix} 29 & 29 & 22 & 59 & 59 & 43 & 22 & 37 & 68 & 15 & 24 & 10 \\ 75 & 86 & 65 & 156 & 150 & 110 & 65 & 106 & 177 & 44 & 69 & 29 \end{bmatrix}$$

Mensaje descifrado: **“EL ATAQUE ESTA EN MARCHA”**
Significado: “El enemigo ha iniciado su ofensiva. Debemos tomar decisiones rápidas.”

Tercer mensaje: Frecuencia 3 (Bloque 3)

Matriz encriptada:

$$\begin{bmatrix} 64 & 24 & 120 & 108 & 66 & 123 & 95 & 52 & 48 & 66 & 14 \\ 50 & 13 & 91 & 95 & 63 & 123 & 113 & 26 & 25 & 69 & 0 \\ 129 & 69 & 252 & 180 & 93 & 150 & 50 & 157 & 141 & 69 & 70 \end{bmatrix}$$

Mensaje descifrado: **"PREPARAR CONTRAATAQUE INMEDIATO"**
Significado: "Necesidad de acción urgente."

Capítulo 4: La Misión Crucial

La misión final está en tus manos. El destino de la nación pende de un hilo, y solo tú puedes evitar que todo se derrumbe. Debes enviar un mensaje codificado a la Agencia Eclipse para evitar una catástrofe.

El mensaje a enviar es: **Original:** "ESPIA DOBLE INFILTRADO ATAQUE EN CURSO EVACUACION INMEDIATA"

Matriz numérica completa:

5, 19, 16, 9, 1, 27, 4, 15, 2, 12, 5, 27, 9, 14, 6, ...
9, 12, 20, 18, 1, 4, 15, 27, 1, 20, 1, 17, 21, 5, 27, ...
5, 14, 27, 3, 21, 18, 19, 15, 27, 5, 22, 1, 3, 21, 1, ...
3, 9, 15, 14, 27, 9, 14, 13, 5, 4, 9, 1, 20, 1

Epílogo

Final exitoso

La Agencia Eclipse mantiene la paz, aunque la amenaza sigue latente. Tu precisión matemática salvó la nación. La misión fue un éxito. Lograste mantener la paz, pero todos saben que la calma es solo temporal. La fragilidad de la situación podría desbordarse en cualquier momento, pero por ahora, la victoria es tuya. Has logrado salvar a la nación de un destino oscuro, aunque las sombras siguen acechando. La Agencia Eclipse sigue en pie, pero los enemigos nunca descansan.

Final fallido

El enemigo descifró los mensajes primero. La ciudad cayó en el caos y la Agencia fue desmantelada. La misión falló. El ataque se llevó a cabo y todo quedó en ruinas. Los enemigos lograron descifrar los mensajes antes que tú y la ciudad cayó en el caos. La Agencia Eclipse ha sido desmantelada y los pocos sobrevivientes ahora viven en la clandestinidad. En las sombras, aún queda la esperanza de un contraataque.