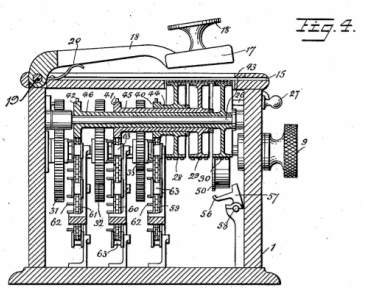
El cifrado de Hill



Una aproximación desde el álgebra lineal modular

Diego González Ventura

Lucía Hermosilla Tamayo

Brais López Rodríguez

Trabajo realizado en el bachillerato **STEMbach**

Bienio 2019/2021

Bajo la dirección conjunta de:

Prof. Manuel Ladra González

Departamento de Matemáticas

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Prof. Carlos Ferreiro García

IES Blanco Amor de Ourense

Ourense, abril de 2021

Resumen

Los cifrados de Hill son una aplicación del álgebra lineal a la criptología (la ciencia de crear y romper códigos y cifrados). A continuación describimos qué son los cifrados de Hill y cómo se rompen. Y discutimos las nociones y hechos necesarios sobre la aritmética modular y sobre el álgebra lineal cuando los escalares ya no son los números reales, sino los enteros módulo algún m o los enteros gaussianos. El Cifrado Hill es un criptosistema de clave simétrica que utiliza una matriz K como clave secreta. Debemos elegir la matriz clave K de forma que tenga una inversa módulo m. Esta matriz clave secreta será utilizada por el emisor y el receptor del mensaje para cifrar y descifrar el mensaje. En este proyecto se discutirá la generalización del Cifrado de Hill utilizando matrices sobre números complejos que hará más seguro al cifrado. Se utilizará la aplicación SageMath para generar cifrados.

Abstract

Hill ciphers are an application of linear algebra to cryptology (the science of making and breaking codes and ciphers). Below we describe what Hill ciphers are and how they are broken. And we discuss the necessary notions and facts about modular arithmetic, and about linear algebra when the scalars are no longer the real numbers but instead the integers modulo some m or the Gaussian integers. The Hill Cipher is a symmetric key cryptosystem that uses a matrix K as the secret key. We must choose the key matrix K in such a way that it has an inverse modulo m. This secret key matrix will be used by the sender and recipient of the message to encrypt and descript the message. In this project we will discuss the generalization of Hill Cipher using matrices over complex numbers that will make the cipher more secure. The SageMath application will be used to generate ciphers.

Índice

1. Introducción

La criptografía es tan antigua como la misma escritura: siempre que ha habido una comunicación entre un par de personas o grupos de personas, ha habido un tercero que podía estar interesado en interceptar y leer esa información sin el permiso y la voluntad de las personas que establecen dicha comunicación. Así, las personas han estado interesadas en escribir mensajes secretos casi desde que han podido escribir. La Escítala, el cifrado de César, Alberti, Vigenère, Enigma están entre los cifrados más importantes, algunos de ellos con más de 2500 años de antigüedad. La esteganografía se utiliza a menudo para aumentar la criptografía, y también está relacionada con la "marca de agua digital". Durante el siglo XX, quedó claro que la criptografía tenía mucho que ver con las matemáticas, y el papel de cifrar y descifrar mensajes ha aumentado drásticamente en el ejército desde la Primera Guerra Mundial. Muchas personas, incluido el propio Churchill, han afirmado que si los aliados no hubieran descifrado el código Enigma alemán, el resultado de la Segunda Guerra Mundial habría sido diferente. La criptografía también desempeña un papel en la mayor parte de nuestra vida cotidiana. Cuando hacemos una compra por Internet, nuestro navegador utiliza la encriptación para mantener nuestros datos financieros seguros. Los cajeros automáticos, la televisión por satélite y otros servicios cotidianos utilizan la encriptación.

En primer lugar, vamos a introducir algo de terminología. La disciplina de cifrar y descifrar mensajes secretos se llama criptografía (o criptología), de las palabras griegas *kryptos*, que significa oculto o secreto, y *graphia*, que significa escritura. El mensaje original, legible, se denomina texto claro o plano. La codificación del mensaje se denomina encriptación o cifrado, y el resultado difícil de leer se llama texto cifrado o mensaje encriptado. Convertir el texto cifrado en texto claro se denomina descifrar. Normalmente, el proceso de conversión depende de una información adicional, que suele llamarse clave o contraseña; la clave constituye la base de la seguridad y debe mantenerse de forma privada. A veces se utilizan diferentes claves para cifrar y descifrar los mensajes. Si es inviable determinar la clave utilizada para el descifrado sin conocer la clave utilizada para el cifrado, este método puede utilizarse para la criptografía de clave pública. Por último, descifrar un mensaje sin conocer la clave correspondiente se denomina descifrar o romper el cifrado.

Con la llegada a principios del siglo pasado de las máquinas mecánicas, se proporcionó métodos de cifrado más sotisficados y eficientes, que ayudaron en gran medida al desarrollo de la Primera y Segunda Guerra Mundial. Hoy en día, la introducción de la electrónica y la computación ha permitido sistemas elaborados que siguen teniendo gran complejidad (y de la que depende la seguridad digital a nivel mundial).

El problema de la criptografía de clave secreta es básicamente el siguiente: tenemos dos individuos, clásicamente notados A (Alicia) y B (Bernardo) que quieren establecer un canal seguro de comunicación, y un tercer individuo E (Eva) (o, en términos más genéricos, el adversario), que tiene la capacidad de interceptar y leer los mensajes que se intercambian por este canal.

Para simplificar los problemas de logística, supondremos que los mensajes que Alicia y Bernardo se quieren intercambiar son números enteros, en una base previamente acordada (típicamente 2) y conocida por todos los actores, o bien una congruencia módulo un cierto entero $m > 1$, también conocido por todos (incluida Eva). Hay muchas formas de hacer esto, la más simple es asignar a cada símbolo de texto un número (como por ejemplo en el código ASCII o Unicode) y luego yuxtaponer los números para conseguir un mensaje

numérico. Si, por el motivo que fuera, el mensaje fuese demasiado largo (por ejemplo, si estamos trabajando en un anillo de congruencias) se puede dividir el mensaje cuantas veces sea necesario.

Para lograr que su correspondencia sea confidencial, Alicia y Bernardo crean un *protocolo criptográfico* que no es, fundamentalmente, más que una aplicación biyectiva. Alicia halla la imagen por esta aplicación de su mensaje para Bernardo, y esto es lo que se envía por el canal de comunicación. Posteriormente Bernardo recibe la imagen y calcula el original, hallando así el mensaje de Alicia. Veamos la formulación precisa.

Para facilitar la comprensión del protocolo, notaremos con letras minúsculas los objetos (enteros, aplicaciones,...) que sólo conocen Alicia y Bernardo, y con mayúsculas aquellos objetos a los que Eva tiene acceso (no necesariamente de forma legal). En estas condiciones, en un protocolo de clave privada, los objetos involucrados son:

1. El mensaje que Alicia quiere hacer llegar a Bernardo: p.
2. Una clave para cifrar y descifrar, que han acordado Alicia y Bernardo: k.
3. Una función de encriptación conocida, que toma dos valores (clave y mensaje): $F(\cdot,\cdot)$.
4. El mensaje cifrado $F(k,p)=C$.
5. Una función de descifrado $G(\cdot,\cdot)$, que es la inversa de la anterior en el sentido de que verifica: $G(k,C)=p$.

Idealmente, se deben dar las siguientes condiciones:

1. Los cálculos $F(k,p)$ y $G(k,C)$ deben ser rápidos (esto es, *algoritmos polinomiales*).
2. No es posible (en la práctica) para Eva averiguar p a partir de C sin conocer k (esto es, el cálculo de p requiere un *algoritmo exponencial*, como mínimo).

Se podría razonar que supone una pérdida innecesaria de seguridad el que Eva conozca F y G. Esto es, a priori, resulta mucho más seguro que Eva no sepa cómo se cifra y se descifra. Pero en la práctica esto no es así. Muchos protocolos criptográficos han basado su seguridad en la opacidad del cifrado y, cuando éste ha sido desvelado (y, tarde o temprano, sucede), todo el sistema se ha visto comprometido. Una postura de cifrado abierto, donde todo el mundo es retado a derrotar al protocolo, garantiza mucha más fiabilidad.

Formalmente, éstas son sólo parte de las exigencias que debe cumplir un protocolo. Tradicionalmente, se asumen los denominados *Principios de Kerckhoffs*:

1. Si el sistema no es teóricamente irrompible, debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los mensajes cifrados deberán dar resultados alfanuméricos.
5. El sistema debe ser operable por una única persona.

6. El sistema debe ser fácil de utilizar.

Evidentemente, algunos de estos principios no son de aplicación ahora (los principios de Kerckhoffs datan de finales del siglo XIX).

En criptografía clásica, uno de los cifrados más conocido es el cifrado de Hill que fue inventado por Lester S. Hill en 1929 y aparece explicado en su artículo *Cryptography in an Algebraic Alphabet*, publicado en The American Mathematical Monthly ([2]). Hill estaba interesado en la aplicación de las matemáticas en las comunicaciones, como también puede verse en [3]. Se trata de un famoso poligrama y un cifrado simétrico clásico basado en la transformación de matrices, pero que sucumbe al ataque de texto plano conocido, como veremos en este trabajo. Aunque su vulnerabilidad al criptoanálisis lo ha hecho inutilizable en la práctica, sigue desempeñando un importante papel pedagógico en la criptología como en álgebra lineal. El cifrado de Hill es un cifrado en bloque que tiene varias ventajas, como la de ocultar las frecuencias de las letras del texto plano, su simplicidad al usar la multiplicación e inversión de matrices para el cifrado y el descifrado, y su alta velocidad y alto rendimiento.

El cifrado de Hill es, por tanto, el eje central de este proyecto de investigación, en el cual hemos procurado ahondar en su metodología. Es un sistema criptográfico de sustitución polialfabético, es decir, un mismo signo, en este caso una misma letra, puede ser representado en un mismo mensaje con más de un carácter. Una última parte de la terminología que debemos cubrir es la elección del alfabeto para el texto plano (y el texto cifrado). Tenemos que acordar por adelantado en qué caracteres escribiremos nuestros mensajes. Antes de la llegada de los ordenadores, los mensajes solían constar únicamente de las 27 letras del alfabeto; todos los espacios, la puntuación, los números y demás se eliminaban del mensaje antes del cifrado. No se distinguía entre mayúsculas y minúsculas. Hoy en día, el ordenador suele realizar el cifrado y el descifrado, y el alfabeto es mucho más amplio y suele contener 128, 256 o más códigos de caracteres. Adoptaremos la convención de utilizar sólo 27 y 29 caracteres para los ejemplos más simples. Para los cifrados más sofisticados, utilizaremos 256 caracteres, concretamente, *Unicode*, que es un estándar universal de codificación de caracteres que se utiliza para admitir caracteres no compatibles con ASCII. Para dichos cálculos utilizaremos *SageMath*, un software libre basado en Phyton que es una herramienta muy potente para la realización de cálculos complejos.

Los cifrados de Hill son una aplicación del álgebra lineal a la criptología. Describiremos qué son los cifrados de Hill y cómo se rompen. Y discutiremos las nociones y hechos necesarios sobre la aritmética modular, y sobre el álgebra lineal cuando los escalares ya no son los números reales, sino los enteros módulo m o, con más generalidad, enteros gaussianos módulo m. Al final, expondremos algunas ideas para mejorar la seguridad del cifrado Hill. En general, dichas mejoras intentan frustrar el ataque de texto plano conocido, consumir poco tiempo, equilibrar la cantidad de manipulaciones matemáticas y ser eficiente especialmente cuando se trata una gran cantidad de datos.

2. Teoría de números

En esta sección utilizaremos como referencia principal [5].

2.1. Aritmética modular

Definición 1. *Dado un número entero $m > 1$. Decimos que a y b son* ***congruentes módulo*** **m** *si ambos dejan el mismo resto al dividirlos entre m, o equivalentemente si $a-b$ es múltiplo de m. Escribiremos $a \equiv b \pmod{m}$.*

Ejemplo 1. *Decimos que $5 \equiv 17 \pmod{3}$ porque al dividir 5 entre 3 da el mismo resto 2 que al dividir 17 entre 3.*

Evidentemente $a \equiv b \pmod{m}$ siempre que $a = b$ (pues, entonces, $a - b = 0 = 0 \cdot m$), pero no se cumple la recíproca. Así, la idea de "igualdad" expresada por la equivalencia módulo m generaliza la idea habitual de igualdad. Las propiedades más básicas de la igualdad también se trasladan a la equivalencia módulo m:

$$\begin{aligned} &a \equiv a \pmod{m} \\ &a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m} \\ &a \equiv b \pmod{m} \ \text{ y } \ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}. \end{aligned}$$

Se observa que no es posible que dos enteros a y b que difieran en menos de m sean congruentes módulo m. En particular, no hay dos enteros $0, 1, \ldots, m-1$ congruentes entre sí módulo m. Se observa, también, que un entero arbitrario a puede dividirse por m para obtener un cociente q y un resto r, es decir, $a = q \cdot m + r$, con $0 \leq r < m$. (Por ejemplo, $23 = 3 \cdot 6 + 5$). En ese caso, por supuesto, $a \equiv r \pmod{m}$. (En el ejemplo que acabamos de dar, $23 \equiv 5 \pmod{m}$).

De las dos observaciones anteriores se deduce ahora que cada entero es congruente módulo m con exactamente uno de los enteros $0, 1, ..., m-1$. Esto justifica la siguiente definición:

Definición 2. *Sea m un número entero con $m > 1$. Para un entero arbitrario a, el* ***resto de a módulo*** *m es el único entero r entre $0, 1, ..., m-1$ al que a es congruente módulo m.*

Por ejemplo, 5 es el resto de 29 módulo 12. Y 5 es también el resto de -7 módulo 12.

Para indicar que sustituimos un número entero dado por su resto módulo m, a veces decimos que **reducimos** el número entero módulo m.

Para nuestros propósitos, la propiedad más importante es que la equivalencia módulo m preserva las sumas, es decir, la adición de un par de enteros que son congruentes módulo m a un segundo par de enteros, da una suma del primer par que es congruente con la suma del segundo par:

$$a \equiv c \pmod{m} \ \text{ y } \ b \equiv d \pmod{m} \Longrightarrow a + b \equiv c + d \pmod{m}.$$

Por ejemplo, de $29 \equiv 5 \pmod{12}$ y $-8 \equiv 4 \pmod{12}$, concluimos que $21 = 29 + (-8) \equiv 5 + 4 = 9 \pmod{12}$.

Del mismo modo, la equivalencia módulo m preserva los productos, es decir, la multiplicación de un par de enteros que son congruentes módulo m a un segundo par de enteros da un producto del primer par que es congruente con el producto del segundo par:

$$a \equiv c \pmod{m} \ \text{ y } \ b \equiv d \pmod{m} \Longrightarrow a \cdot b \equiv c \cdot d \pmod{m}.$$

Por ejemplo, de $29 \equiv 5 \pmod{12}$ y $-8 \equiv 4 \pmod{12}$, concluimos que $-232 = 29 \cdot (-8) \equiv 5 \cdot 4 = 20 \pmod{12}$.

Como la equivalencia módulo m conserva tanto las sumas como los productos, podemos hacer aritmética módulo m de la siguiente manera: después de sumar o multiplicar dos enteros, se sustituye su suma o producto, respectivamente, por su resto módulo m. Si hacemos cualquier combinación de sumas y multiplicaciones de un número de enteros y luego sustituimos el resultado final por su resto módulo m, obtendremos el mismo resultado que sustituyendo los enteros iniciales por sus restos módulo m (si no están ya entre 0 y $m-1$) y luego sustituir cada suma y producto por su resto módulo m.

Por ejemplo, trabajando módulo $m = 29$. Podemos calcular el resto de $8 \cdot 16 + 7 \cdot 19$ bien haciendo los cálculos de la forma habitual y luego tomando el resto

$$8 \cdot 16 + 7 \cdot 18 = 128 + 126 = 254 \equiv 22 \pmod{29},$$

o bien tomando los restos en cada paso del proceso:

$$8 \cdot 16 + 7 \cdot 18 = 128 + 126 \equiv 12 + 10 \equiv 22 \pmod{29}.$$

Hemos visto, entonces, que la aritmética modular se basa en una relación de equivalencia, y las clases de equivalencia de un entero a se denota con $[a]_m$, o simplemente $[a]$ si sobreentendemos el módulo.

El conjunto cociente de todas las clases de equivalencia módulo m se denota como:

$$\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}.$$

Nótese que representa el conjunto de restos de la división entre m.

Sean $[a]_m$ y $[b]_m$ las clases de equivalencia módulo m de a y b, respectivamente. Parafraseando las propiedades vistas, se definen las operaciones suma y multiplicación mediante:

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

De este modo, $\mathbb{Z}_m$ se convierte en un "anillo" con m elementos. Por ejemplo, en el anillo $\mathbb{Z}_{12}$, se tiene: $[11] \cdot [4] + [6] = [50] = [2]$.

2.2. El sistema de números $\mathbb{Z}_m$

En general, para cualquier módulo m, la suma y la multiplicación módulo m tienen muchas –pero no todas– las propiedades conocidas de la suma y la multiplicación de los números reales ordinarios. Por razones de simplicidad y siempre que no genere confusión en el contexto, utilizaremos sencillamente a en lugar de $[a]$. De esta forma

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}.$$

Proposición 1. *Sea m un número entero con $m > 1$. Entonces en $\mathbb{Z}_m$:*

1. *Para todo $a, b, c \in \mathbb{Z}_m$, $(a+b)+c = a+(b+c)$.*
2. *Para todo $a, b \in \mathbb{Z}_m$, $a+b = b+a$.*
3. *Para cada $a \in \mathbb{Z}_m$, $a+0 = a = 0+a$.*
4. *Para cada $a \in \mathbb{Z}_m$, existe un único $x \in \mathbb{Z}_m$, llamado inverso aditivo de a, tal que $a+x = 0 = x+a$.*

5. *Para todo* $a, b, c \in \mathbb{Z}_m$, $(ab)c = a(bc)$.

6. *Para todo* $a, b \in \mathbb{Z}_m$, $ab = ba$.

7. *Para cada* $a \in \mathbb{Z}_m$, $1 \cdot a = a = a \cdot 1$.

8. *Para todo* $a, b, c \in \mathbb{Z}_m$, $a(b + c) = ab + ac$.

9. *En* $\mathbb{Z}_m$, $1 \neq 0$.

Dado un $a \in \mathbb{Z}_m$, su inverso aditivo $x \in \mathbb{Z}_m$, como se da en la propiedad 4 de la proposición, no es el entero negativo $-a$ (excepto en el caso trivial de que $a = 0$). Más bien, el inverso aditivo de a es el resto de $-a$ módulo m. Como ejemplo, mostraremos las tablas de suma y multiplicación para $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Según la tabla, el inverso aditivo de 3 en $\mathbb{Z}_4$ es 1, porque $3 + 1 \equiv 0 \pmod 4$, que confirma la equivalencia $-3 \equiv 1 \pmod 4$.

En el caso multiplicativo se podría establecer la propiedad (10*): para cada $a \in \mathbb{Z}_m$ con $a \neq 0$, existe un único $x \in \mathbb{Z}_m$, llamado inverso multiplicativo o recíproco de a, tal que $a \cdot x = 1 = x \cdot a$. Sin embargo, dicha afirmación no es cierta en general. Por ejemplo, no es cierta en $\mathbb{Z}_4$. Mirando la tabla de multiplicación de $\mathbb{Z}_4$, se observa que 2 no tiene un recíproco en $\mathbb{Z}_4$, ya que 1 no está entre sus productos con cada uno de los elementos de $\mathbb{Z}_4$. En cambio, 3 sí tiene un recíproco en $\mathbb{Z}_4$, el propio 3, porque en $\mathbb{Z}_4$ tenemos $3 \cdot 3 = 1$. Así, algunos elementos no nulos de $\mathbb{Z}_4$ tienen recíprocos, pero otros no. El teorema general relevante aquí es el siguiente:

Teorema 1. *Un número entero* a *tiene un inverso multiplicativo módulo* m *si y sólo si* $mcd(a, m) = 1$, *es decir,* 1 *es el único entero positivo que divide tanto a como a* m.

La demostración de este teorema es elemental utilizando el algoritmo de Euclides. Cuando trabajemos con cifrados de Hill, necesitaremos hacer operaciones elementales de fila en las matrices para ponerlas en forma escalonada reducida, y tendremos que hacer toda la aritmética módulo una longitud de alfabeto dada m. La reducción de fila irá sin problemas hasta que necesitemos operar una fila para hacer un elemento pivote 1. Entonces tendremos que "dividir" cada entrada de la fila por el pivote módulo m, es decir, multiplicar cada entrada por el recíproco del pivote. Desafortunadamente, en general, el pivote no tiene por qué ser invertible. Esto ocurrirá, por ejemplo, si el pivote es 2 y estamos trabajando módulo 4.

A continuación, observemos las tablas de suma y multiplicación de $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Excepto la fila que muestra la multiplicación por 0, cada fila de la tabla de multiplicación incluye un 1, y eso significa que cada elemento no nulo de $\mathbb{Z}_5$ tiene un inverso multiplicativo. En otras palabras, la propiedad de existencia del inverso multiplicativo se cumple en $\mathbb{Z}_5$. La diferencia entre $\mathbb{Z}_5$ y $\mathbb{Z}_4$ –en lo que respecta a la existencia de inversos multiplicativos– es que el módulo 5 es un primo y el 4 no.

Ejemplo 2. *En $\mathbb{Z}_{12}$, sólo $1, 5, 7$ y 11 son primos relativos al módulo 12 y son, por lo tanto, los elementos invertibles. Si queremos, por ejemplo, hallar el inverso de 5, procedemos mediante el algoritmo de Euclides:*

$$\begin{aligned} 12 &= 5 \cdot 2 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2. \end{aligned}$$

Luego, recorriendo al camino inverso:

$$\begin{aligned} 1 &= 5 - (2 \cdot 2) = 5 - 2 \cdot (12 - 5 \cdot 2) \\ &= 5 - (12 \cdot 2 - 5 \cdot 4) = 5 \cdot 5 - 12 \cdot 2. \end{aligned}$$

Sabemos que $mcd(a, m) = 1 \iff \exists b, k \in \mathbb{Z}$ tales que $ab + km = 1 \iff ab \equiv 1 \pmod{m}$. En este ejemplo, en consecuencia, 5 es el inverso de 5 en $\mathbb{Z}_{12}$.

La siguiente definición es conveniente para extender los resultados conocidos en espacios vectoriales sobre cuerpos:

Definición 3. *Un sistema numérico cerrado bajo dos operaciones de adición y multiplicación se llama **cuerpo** cuando las propiedades 1-9 de la proposición anterior y (10*) se cumplen en él.*

Los ejemplos de $\mathbb{Z}_5$ y $\mathbb{Z}_4$ discutidos anteriormente ilustran el siguiente resultado:

Proposición 2. *Sea m un número entero con $m > 1$. Entonces $\mathbb{Z}_m$ es un cuerpo si y sólo si m es primo.*

En particular, $\mathbb{Z}_5$ es un cuerpo mientras que $\mathbb{Z}_4$ no lo es (aunque sí es un anillo). Para todo m primo, el cuerpo $\mathbb{Z}_m$ es finito. El sistema de números reales $\mathbb{R}$ es un ejemplo de cuerpo infinito. También lo es el sistema numérico $\mathbb{Q}$ que consiste sólo de los números racionales.

El conjunto $\mathbb{Z}_{29}$ es un cuerpo pues 29 es primo. Por conveniencia para uso posterior, enumeramos en la tabla siguiente los recíprocos (inversos multiplicativos) de los elementos no nulos de $\mathbb{Z}_{29}$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

3. Cifrado de Hill clásico

Los cifrados de Hill son una aplicación del álgebra lineal a la criptología. A continuación describimos qué son los cifrados de Hill y cómo se rompen. Y discutiremos las nociones y hechos necesarios sobre la aritmética modular, y sobre el álgebra lineal cuando los escalares

ya no son los números reales, sino los enteros módulo m. Para el desarrollo de esta sección se ha consultado los libros [6] y [7].

Es un sistema criptográfico de sustitución polialfabético, es decir, un mismo signo, en este caso una misma letra, puede ser representado en un mismo mensaje con más de un carácter. Así, en el ejemplo que vamos a analizar a continuación, la letra A del mensaje original aparece representada en el mensaje codificado de cuatro formas distintas, como I, ?, R y Z. El siguiente cifrado que veremos, conocido como el cifrado Hill, se basa en matrices. Es una forma de cifrado por sustitución, salvo que no sustituye simplemente una letra por otra, sino un bloque de letras por otro. Por ejemplo, puede cambiar un bloque de tres letras por otro de tres letras.

Empezaremos con una visión general de los tipos de cifrados.

3.1. Cifrados polialfabéticos

Los cifrados son métodos para transformar un mensaje dado –el *texto plano*– en una nueva forma ininteligible para cualquiera que no conozca la regla –la *clave*– para realizar la transformación o, lo que es más importante, que no conozca la regla secreta –la *clave inversa*– para revertir la transformación y recuperar el *texto plano* original.[1] Los cifrados pueden utilizarse junto con métodos para ocultar la existencia misma del mensaje, como la tinta secreta o los micropuntos (*Esteganografía*). O bien, los mensajes transformados por cifrados pueden comunicarse al aire libre, por ejemplo, transmitidos por radio de onda corta o impresos en un anuncio de periódico.

3.1.1. Cifrado por sustitución

En el caso de un cifrado, por el contrario, la clave transforma letras individuales del texto plano y otros caracteres, o grupos de longitud fija de varios caracteres, en nuevos caracteres: el texto cifrado. Utilizar la clave para transformar el texto plano en texto cifrado es cifrar ese texto plano; utilizar la clave inversa para transformar el texto cifrado en texto plano es descifrar ese texto cifrado.

Un tipo de cifrado podría simplemente reordenar las letras del texto plano dado. Sin embargo, los cifrados que estudiaremos son sustituciones, en las que las letras del texto plano se sustituyen por otras del alfabeto.

Un ejemplo de cifrado por sustitución es un "criptograma" como el que se puede haber visto en una revista de acertijos. Este es un ejemplo (el texto cifrado está agrupado arbitrariamente en conjuntos de seis letras):

U G R L Y Ñ L G U U G W U F R V Ñ L

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

Se puede resolver un criptograma de este tipo, es decir, descubrir el significado secreto, si se conoce la clave. En el caso de este criptograma, la clave viene dada por la Tabla

[1] No es necesario mantener la clave en secreto. En un cifrado de clave pública, como el sistema RSA ideado en 1978 por Rivest, Shamir y Adleman, la clave puede publicarse abiertamente, porque recuperar la clave inversa a partir de ella es extremadamente difícil. Normalmente, sólo alguien que tenga la clave inversa secreta puede descifrar un mensaje cifrado con un sistema de este tipo.

anterior, en la que debajo de cada letra del texto plano está la letra correspondiente del texto cifrado. ¿Cuál es el texto plano secreto en este ejemplo?

Por supuesto, no es un reto descifrar un mensaje si se conoce la clave. Lo que realmente es interesante es averiguar cuál es la clave y su inversa, es decir, descifrar el cifrado (en términos técnicos, "criptoanalizarlo"). Una simple sustitución letra por letra, como en el ejemplo anterior, puede ser bastante fácil de descifrar si se tiene suficiente texto cifrado. Porque entonces se puede analizar estadísticamente el texto cifrado, buscando letras (o incluso pares o triples de letras) que aparezcan con frecuencia o con poca frecuencia en el texto cifrado y luego utilizar de las frecuencias conocidas de las letras (o pares o triples) en un texto en español. Por ejemplo, una tabla estándar de frecuencias de letras en español incluye "e, a, o, l, s, n, d" como las más frecuentes, en ese orden.

3.1.2. Cifrado por sustitución polialfabético

El defecto básico de esta simple sustitución letra por letra es que las mismas letras del texto plano siempre se sustituyen por las mismas letras del texto cifrado (hasta que se cambie la clave, por supuesto), y eso es lo que hace que el análisis estadístico de las frecuencias de las letras sea efectivo. Un cifrado más difícil de analizar es un cifrado polialfabético, en el que el texto plano se divide en grupos de letras adyacentes de la misma longitud fija n, y luego cada grupo se transforma en un grupo diferente de n letras. Si n no es demasiado pequeño, esta sustitución polialfabética puede hacer inútil el análisis de la frecuencia de las letras.

Se han ideado muchos tipos de cifrado polialfabético. Uno de los más famosos, por ejemplo, es el cifrado Playfair, inventado en 1854, que utiliza dígrafos (dos letras por grupo). Los primeros cifrados polialfabéticos sistemáticos y sencillos que utilizan más de dos letras por grupo son los que estudiaremos a continuación: los **cifrados Hill**. Los cifrados Hill constituyen el primer método general de aplicación del álgebra –específicamente, el álgebra lineal– a los cifrados polialfabéticos de una manera práctica.

En el caso de una sustitución polialfabética, el cambio de sólo una o dos letras del texto plano puede cambiar completamente el texto cifrado correspondiente. En el caso de un cifrado de Hill que se analizará más adelante (en el que nuestro "alfabeto" incluye . y ?), a los dos textos planos

EN LA CAJA ESTÁ LA QUE COBRA y EN ESA CAJA ESTÁ LA COBRA

les corresponden, respectivamente, los dos textos cifrados

TUXAGAQTEMROAGPKNBJZVLJV y BPNAQAMGWQZADTYZEJUR

como veremos más adelante. Esto ilustra por qué los cifrados de Hill son tan difíciles de descifrar, a menos que se tenga la suerte de haber "capturado" algunas piezas de texto plano junto con las correspondientes piezas de texto cifrado.

3.1.3. Nuestro alfabeto

En los ejemplos que siguen con los cifrados Hill, nuestro alfabeto consiste en las 27 letras mayúsculas del alfabeto español, seguidas del punto (.) y del signo de interrogación (?), en ese orden. En el texto plano, el punto y el signo de interrogación tienen su significado habitual. Más adelante, cuando presentemos ejemplos de cifrado más sustanciales, usaremos el código ASCII y Unicode de 256 letras, símbolos y caracteres.

Al cifrar o descifrar, representaremos los 29 caracteres de nuestro alfabeto, en orden, por los enteros no negativos 0, 1, . . . , 28, como se muestra en la siguiente Tabla.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Siempre que no necesitemos referirnos al alfabeto específico anterior, denotaremos la longitud del alfabeto por $m > 1$, con la finalidad de presentar el cifrado de Hill susceptible de ser usado en distintos alfabetos. Además, a menudo nos referiremos a cualquier carácter de dicho alfabeto como una "letra", incluso cuando sea un símbolo de puntuación (como en nuestro alfabeto de 29 caracteres) o algún otro carácter que no sea realmente una letra en el sentido ordinario. No hay nada en especial en numerar las letras de nuestro alfabeto en orden ascendente (empezando por 0). En la práctica, sin duda, se mezclarían los números en un orden arbitrario (conocido tanto por el emisor como por el receptor de un mensaje cifrado) para dificultar un poco más el descifrado. Para simplificar, nos quedaremos con el esquema de numeración dado.

3.2. Álgebra lineal modular

Lo que estamos haciendo, en efecto, al trabajar con cifrados de Hill es utilizar matrices y vectores cuyas entradas pertenecen a $\mathbb{Z}_m$ para algún número entero $m > 1$, y haciendo toda la aritmética módulo m. Con todo, mucho de lo que conocemos sobre matrices y álgebra lineal sigue teniendo sentido en el contexto de $\mathbb{Z}_m$: suma y multiplicación de matrices, operaciones elementales de fila, independencia lineal y transformaciones lineales.

Sin embargo, dentro de $\mathbb{Z}_m$ no podemos, en general, hallar siempre una matriz en una forma escalonada equivalente reducida por filas, a menos que se garantice que cada elemento de $\mathbb{Z}_m$ tiene una inversa multiplicativa, es decir, a menos que m sea primo. Por esta razón, hemos añadido dos "letras" adicionales al alfabeto español normal de 27 letras. El sistema numérico $\mathbb{Z}_{29}$ es un cuerpo, mientras que $\mathbb{Z}_{27}$ no lo es. Por supuesto, siempre es posible utilizar como clave de un cifrado Hill una matriz con entradas en $\mathbb{Z}_m$ para un valor arbitrario $m > 1$. Pero a menos que las entradas de la matriz se elijan con especial cuidado, no será posible calcular una matriz inversa módulo m, es decir, obtener una clave inversa para el descifrado.

Los cifrados de Hill para el español suelen utilizar $m = 27$. Este módulo no primo sólo hace que los cifrados Hill sean técnicamente más difíciles de trabajar. Así que, por razones de simplicidad, en los ejemplos que trabajaremos solemos utilizar un módulo primo, a menudo con 29.

Cuando m es un primo como 29, $\mathbb{Z}_m$ es un cuerpo. Para cualquier cuerpo de escalares (ya sean los reales $\mathbb{R}$ o $\mathbb{Z}_m$ o cualquier otro), prácticamente toda la teoría y los cálculos sobre los espacios vectoriales y sus transformaciones lineales, incluyendo prácticamente todo lo relativo a las matrices, puede ser transferido.

Dada una matriz A cuadrada $n \times n$, si existe otra matriz B de $n \times n$ de modo que $AB = I_n$ y $BA = I_n$, donde I_n es la matriz identidad de orden n, decimos que A es invertible. Solemos escribir A^{-1} para la matriz B, y resulta que esta matriz inversa, cuando existe, es única.

Definición 4. *Sea $A = (a_{ij})$ una matriz $n \times n$. Para cada a_{ij}, sea la matriz de orden $(n-1) \times (n-1)$ obtenida a partir de A eliminando la fila i y la columna j y cuyo determinante se designa por α_{ij} (menor complementario del elemento a_{ij}). Entonces, $(-1)^{i+j} \cdot \alpha_{ij}$ se llama **adjunto** de a_{ij} y $Adj(A) = ((-1)^{i+j} \cdot \alpha_{ij})$ se llama la **matriz adjunta** de A.*

La existencia y construcción de la inversa de una matriz se demuestra en el siguiente

Teorema 2. *(Fórmula para la inversa de una matriz) Sea $A = (a_{ij})$ una matriz $n \times n$ y sea $(AdjA)^T$ la traspuesta de su matriz adjunta $Adj(A) = ((-1)^{i+j} \cdot \alpha_{ij})$, $1 \leq i, j \leq n$, entonces $A \cdot Adj(A)^T = Adj(A)^T \cdot A = \det(A) I_n$. Más aún, $det(A)$ es una unidad (invertible) en R si y sólo si A es una unidad (invertible) en $M_{n\times n}(R)$; en ese caso, la matriz inversa es*

$$A^{-1} = \frac{1}{\det(A)} Adj(A)^T.$$

Una demostración de este teorema puede verse en [1, pág. 440].

Al igual que vimos que $a \in \mathbb{Z}_m$ es invertible si y sólo si $mcd(a, m) = 1$, sin tener que encontrar la inversa a^{-1}, hay una manera de comprobar si una matriz es invertible sin encontrar realmente la matriz inversa A^{-1}, usando el determinante. Resulta que, para el caso de matrices con entradas en $\mathbb{R}$, una matriz A es invertible si y sólo si su determinante es una unidad (o invertible). Ya que las unidades en $\mathbb{R}$ son todos los números reales excepto el 0, una matriz con entradas $\mathbb{R}$ es invertible si y sólo si su determinante es distinto de cero. Si las entradas están en $\mathbb{Z}$ y queremos una inversa que también tenga entradas en $\mathbb{Z}$, entonces esto ocurre si y sólo si su determinante es ± 1. Si las entradas están en $\mathbb{Z}_m$, entonces tiene una inversa si y sólo si $mcd(det(A), m) = 1$.

En la siguiente sección ilustraremos la reducción de filas y el cálculo de inversas de matrices, también utilizando determinantes, sobre $\mathbb{Z}_{29}$.

3.3. Cifrado de Hill

La idea del cifrado de Hill es cifrar bloques de caracteres mediante matrices, sustituyendo un bloque de un número reducido de letras por otro del mismo tamaño. Por ejemplo, supongamos que elegimos cifrar por bloques de longitud 3. (Los bloques de texto plano y de texto cifrado deben tener el mismo tamaño para que el cifrado de Hill funcione). Para ello, elegimos una matriz A invertible de 3×3 con coeficientes en $\mathbb{Z}_{29}$ como clave[2]. Una forma común de hacer esto es comenzar con una palabra de 9 letras y luego convertirla en números. Utilizaremos la clave $SENTIDIÑO$. Para convertirla en una clave, escribimos las letras de $SENTIDIÑO$ en una matriz de 3×3, como

$$\begin{pmatrix} S & E & N \\ T & I & D \\ I & \tilde{N} & O \end{pmatrix}.$$

A continuación, convertimos cada letra en un número, sustituyendo la A por el 0, la B por el 1, la C por el 2, y así sucesivamente, hasta la Z por el 26. Obtenemos la matriz clave:

$$K = \begin{pmatrix} 19 & 4 & 13 \\ 20 & 8 & 3 \\ 8 & 14 & 15 \end{pmatrix}.$$

[2]Usaremos el anillo $\mathbb{Z}_{29}$ en estos primeros ejemplos por simplicidad y por coincidir el número de elementos de éste con el número de letras del alfabeto español junto con los símbolos "." y "?".

Utilizamos K para cifrar grupos de 3 caracteres consecutivos –trígrafos– a la vez. Primero cifremos el trígrafo *voy*. En nuestro alfabeto, las letras *v*, *o* e *y* están numeradas como 22, 15 y 25, respectivamente, por lo que representamos *voy* mediante el vector columna

$$\begin{pmatrix} 22 \\ 15 \\ 25 \end{pmatrix}.$$

Para cifrar *voy*, multiplicamos este vector columna por la matriz clave K:

$$\begin{pmatrix} 19 & 4 & 13 \\ 20 & 8 & 3 \\ 8 & 14 & 15 \end{pmatrix} \begin{pmatrix} 22 \\ 15 \\ 25 \end{pmatrix} = \begin{pmatrix} 803 \\ 635 \\ 761 \end{pmatrix}.$$

¿Qué letras representan el 803, el 635 y el 761? Nuestro alfabeto de 29 letras está numerado desde el 0 hasta sólo el 28. Lo que hacemos es simplemente calcular los restos correspondientes módulo 29. Así, $803 \equiv 20 \pmod{29}$ representa la misma letra que 20, es decir, *t*; $635 \equiv 26 \pmod{29}$ representa la misma letra que 26, es decir, *z*; y $761 \equiv 7 \pmod{29}$ representa la misma letra que 7, es decir, *h*. Finalmente, obtenemos de *voy* el correspondiente texto cifrado *tzh*.

En términos generales, en el cifrado de Hill, el texto cifrado se obtiene a partir del texto plano mediante una transformación lineal. La matriz del texto plano P se cifra como

$$C \equiv KP \pmod{m}$$

en donde C es la matriz texto cifrado, K es una matriz clave $n \times n$ con entradas en $\mathbb{Z}_m$ para $m > 1$.[3] Se supone que la matriz clave K se comparte de forma segura entre los participantes. El texto cifrado C se descifra como

$$P \equiv K^{-1}C \pmod{m}$$

donde todas las operaciones se realizan módulo m. Para que el descifrado sea posible, la matriz clave K debe ser invertible o, lo que es lo mismo, debe satisfacer

$$mcd(det(K) \pmod{m}, m) = 1.$$

Sin embargo, muchas de las matrices cuadradas no son invertibles módulo m. El riesgo de que el determinante tenga factores comunes con el módulo puede reducirse tomando un número primo como módulo. Esta selección también aumenta el espacio de claves del criptosistema.

A continuación, presentaremos el cifrado y descifrado de Hill detalladamente.

3.3.1. Cifrando con el cifrado de Hill

Supongamos que tenemos un alfabeto de longitud $m > 1$ y un número entero $n > 1$. Entonces un **n-cifrado de Hill** viene dado por una matriz K de $n \times n$ con entradas en $\mathbb{Z}_m$. Esa matriz representa la clave del cifrado.

Para una matriz clave K dada, el *algoritmo de Hill para cifrar un texto plano* dado es el siguiente:

[3] El valor del módulo m en el cifrado original de Hill era 26 (número de letras del alfabeto inglés), pero su valor puede seleccionarse arbitrariamente.

1. Separe el texto plano de izquierda a derecha en un determinado número k de grupos (polígrafos) de n letras cada uno. Si queda sin letras al formar el último grupo, repita la última letra del texto plano tantas veces como sea necesario para completar ese grupo final hasta las n letras.

2. Sustituya cada letra por el número correspondiente a su posición (de 0 a $m-1$) en el alfabeto para obtener k grupos de n enteros cada uno.

3. Represente cada uno de los k grupos de enteros en un vector columna de n filas y a su vez multiplique K por cada uno de esos k vectores columna módulo m.

4. Después de ordenar todos los k vectores columna de n filas del producto resultante en un único vector de $k \cdot n$ componentes (con entradas en $\mathbb{Z}_m$), sustituya cada una de estas $k \cdot n$ entradas por la letra correspondiente del alfabeto.

5. El resultado es el texto cifrado correspondiente al texto plano original.

Cuando se implemente el algoritmo anterior en el ordenador, puede ser más conveniente invertir los pasos 1 y 2, es decir, sustituir primero las letras por números, y sólo entonces hacer la agrupación (y repetir el número final según sea necesario para completar el grupo final).

Los vectores columna de n filas formados en el paso 3, para representar grupos de letras de texto plano, se llaman **vectores de texto plano**, aunque estos vectores están compuestos de números, no de letras. Del mismo modo, los vectores columna de n filas que se obtienen multiplicando por K módulo m en el paso 3 se denominan **vectores de texto cifrado**; estos vectores de texto cifrado representan numéricamente grupos de letras de texto cifrado.

El texto plano podría ser, en principio, cualquier mezcla de letras de nuestro alfabeto, tenga o no sentido, y así también el texto cifrado. De esta forma, el conjunto de todos los vectores de texto plano –y también el conjunto de todos los vectores de texto cifrado– no es otra cosa que el conjunto que denotaremos por $\mathbb{Z}_m^n$ y que consiste en todos los vectores columna de n filas con entradas en $\mathbb{Z}_m$. Y es razonable llamar "vectores" a los elementos de $\mathbb{Z}_m^n$, porque podemos sumarlos y multiplicarlos por escalares (es decir, por elementos de $\mathbb{Z}_m$) para obtener de nuevo elementos de $\mathbb{Z}_m^n$, siempre que reduzcamos los resultados módulo m. En vista de la proposición 1, las ocho propiedades fundamentales de los vectores en $\mathbb{R}^n$, también se satisfacen en $\mathbb{Z}_m^n$. Por tanto, podemos hablar de $\mathbb{Z}_m^n$ como un "espacio lineal" o "espacio vectorial".[4]

Llegados a este punto, podemos decir qué es "realmente" un n-cifrado de Hill con matriz clave K: la transformación lineal de $\mathbb{Z}_m^n$ en $\mathbb{Z}_m^n$ cuya representación matricial es K. Incluso aunque el dominio y el codominio de esta transformación lineal son los mismos, es sugerente referirse al dominio como consistente en todos los vectores de texto plano, y el codominio como consistente en todos los vectores de texto cifrado.

En el paso 3 del algoritmo, en lugar de multiplicar K por separado por cada una de las k matrices de columnas, podemos, por supuesto, multiplicar K por la única matriz $n \times k$ formada por esas columnas. También lo ilustraremos en el siguiente ejemplo.

[4]Técnicamente, debemos referirnos a Z_m^n como un espacio vectorial sólo cuando el conjunto Z_m de escalares es un cuerpo, es decir, cuando m es primo. En el caso general, cuando los escalares no forman un cuerpo, es más apropiado llamar a Z_m^n un *módulo*.

A lo largo de todos nuestros ejemplos, seguiremos utilizando nuestro alfabeto de 29 letras, pero el tamaño de la matriz de claves n será bastante pequeño. En un cifrado Hill "real", n podría ser bastante grande, para hacer más difícil el romper el cifrado.

Ejemplo 3. *La matriz clave con* $n = 3$ *es*

$$K = \begin{pmatrix} 19 & 7 & 22 \\ 25 & 11 & 5 \\ 13 & 3 & 14 \end{pmatrix}.$$

El texto plano es el mensaje de 16 letras:

$$ESTO\ NO\ SE\ ENTIENDE$$

Primero, agrupamos el texto plano en polígrafos de longitud 3, repitiendo la letra final (E) dos veces para completar el sexto grupo:

$$EST \quad ONO \quad SEE \quad NTI \quad END \quad EEE$$

En segundo lugar, sustituimos las letras por los números correspondientes (véase la Tabla del alfabeto):

$$4 \quad 19 \quad 20 \quad 15 \quad 13 \quad 15 \quad 19 \quad 4 \quad 4 \quad 13 \quad 20 \quad 8 \quad 4 \quad 13 \quad 3 \quad 4 \quad 4 \quad 4$$

Tercero, aplicamos la clave:

$$\begin{aligned} K \begin{pmatrix} 4 & 15 & 19 & 13 & 3 & 4 \\ 19 & 13 & 4 & 20 & 13 & 4 \\ 20 & 15 & 4 & 8 & 3 & 4 \end{pmatrix} &= \begin{pmatrix} 19 & 7 & 22 \\ 25 & 11 & 5 \\ 13 & 3 & 14 \end{pmatrix} \begin{pmatrix} 4 & 15 & 19 & 13 & 3 & 4 \\ 19 & 13 & 4 & 20 & 13 & 4 \\ 20 & 15 & 4 & 8 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 649 & 706 & 477 & 563 & 214 & 192 \\ 409 & 593 & 539 & 585 & 233 & 164 \\ 389 & 444 & 315 & 341 & 120 & 120 \end{pmatrix} \\ &\equiv \begin{pmatrix} 11 & 10 & 13 & 12 & 11 & 18 \\ 3 & 13 & 17 & 5 & 1 & 19 \\ 12 & 9 & 25 & 22 & 4 & 4 \end{pmatrix} \pmod{29}. \end{aligned}$$

En cuarto lugar, los números:

$$11 \quad 3 \quad 12 \quad 10 \quad 13 \quad 9 \quad 13 \quad 17 \quad 25 \quad 12 \quad 5 \quad 22 \quad 11 \quad 1 \quad 4 \quad 18 \quad 19 \quad 4$$

de las columnas alineadas que se acaban de obtener representan las letras:

$$L \quad D \quad M \quad K \quad N \quad J \quad N \quad Q \quad Y \quad M \quad F \quad V \quad L \quad B \quad E \quad R \quad S \quad E$$

Para este 3-cifrado de Hill, el texto cifrado correspondiente al texto plano ESTO NO SE ENTIENDE es, por tanto, LDMKNJNQYMFVLBERSE.

Anteriormente, en la sección 3.1.2, hemos ilustrado cómo una sustitución polialfabética como el cifrado Hill puede traducir dos textos planos bastante similares en textos cifrados completamente diferentes. Aquí tenemos de nuevo ese ejemplo:

Ejemplo 4. *Se trata de un 4-cifrado de Hill. La matriz clave es:*

$$K = \begin{pmatrix} 3 & 13 & 21 & 11 \\ 0 & 9 & 15 & 28 \\ 4 & 24 & 7 & 2 \\ 19 & 12 & 22 & 1 \end{pmatrix}.$$

Para esta matriz K, los textos planos EN LA CAJA ESTÁ LA QUE COBRA y EN ESA CAJA ESTÁ LA COBRA se cifran en TUXAGAQTEMROAGPKNBJZVLJV y BPNAQAMGWQZADTYZEJUR, respectivamente. Omitimos los detalles aritméticos del cifrado.

3.3.2. Descifrando con una clave de Hill

Para un cifrado de Hill, la transformación de texto cifrado a texto plano es simplemente la inversa de la transformación original de texto plano a texto cifrado. En otras palabras, si un cifrado de Hill tiene una matriz clave K, entonces la transformación inversa es el cifrado Hill cuya matriz clave es K^{-1}.

Si ya tenemos la inversa de la matriz clave A, entonces podemos utilizarla para descifrar cualquier texto cifrado.

Ejemplo 5. *Consideremos el 3-cifrado de Hill con matriz clave:*

$$K = \begin{pmatrix} 3 & 14 & 15 \\ 13 & 9 & 25 \\ 21 & 7 & 19 \end{pmatrix}.$$

La matriz inversa de K sobre el cuerpo de escalares $\mathbb{Z}_{29}$ es:

$$K^{-1} = \begin{pmatrix} 18 & 14 & 4 \\ 25 & 1 & 11 \\ 6 & 4 & 16 \end{pmatrix},$$

como podemos comprobar por los cálculos

$$K \cdot K^{-1} = \begin{pmatrix} 3 & 14 & 15 \\ 13 & 9 & 25 \\ 21 & 7 & 19 \end{pmatrix} \begin{pmatrix} 18 & 14 & 4 \\ 25 & 1 & 11 \\ 6 & 4 & 16 \end{pmatrix} = \begin{pmatrix} 494 & 116 & 406 \\ 609 & 291 & 551 \\ 667 & 377 & 465 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{29}.$$

Supongamos que hemos recibido el texto cifrado

$$SA?BOCXANMQN$$

que queremos descifrar y que poseemos la clave inversa. Siguiendo el algoritmo de cuatro pasos descrito en la sección 3.3.1, pero utilizando K^{-1} en lugar de K, e intercambiando las palabras "texto cifrado" y "texto plano":

En primer lugar, agrupamos las letras en trígrafos (no es necesario rellenar el grupo final, ya que la longitud del texto es un múltiplo del tamaño de la clave):

$$SA? \quad BOC \quad XAN \quad MQN$$

En segundo lugar, sustituimos las letras por los números correspondientes:

$$19 \;\; 0 \;\; 28 \quad 1 \;\; 15 \;\; 2 \quad 24 \;\; 0 \;\; 13 \quad 12 \;\; 17 \;\; 13$$

En tercer lugar, multiplicamos los vectores columna por K^{-1}*:*

$$K^{-1}\begin{pmatrix} 19 & 1 & 24 & 12 \\ 0 & 15 & 0 & 17 \\ 28 & 2 & 13 & 13 \end{pmatrix} = \begin{pmatrix} 454 & 236 & 484 & 506 \\ 783 & 62 & 743 & 460 \\ 562 & 98 & 352 & 348 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 19 & 4 & 20 & 13 \\ 0 & 4 & 18 & 25 \\ 11 & 11 & 4 & 0 \end{pmatrix} \pmod{29}.$$

En cuarto lugar, las columnas obtenidas, cuando se encadenan en

$$19 \quad 0 \quad 11 \quad 4 \quad 4 \quad 11 \quad 15 \quad 23 \quad 4 \quad 12 \quad 2 \quad 14$$

dan la representación numérica del texto plano original que, utilizando la Tabla para completar el descifrado, desvelamos el mensaje:

$$SALE\ EL\ TREN\ YA$$

Si se conoce la matriz clave K para un cifrado de Hill, entonces ciertamente se puede construir la clave inversa invirtiendo K de la manera habitual mediante la reducción de filas o por determinantes, pero utilizando siempre, por supuesto, la aritmética módulo m.

Ejemplo 6. *Supongamos que conocemos la matriz clave*

$$K = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$$

para un 2-cifrado de Hill (con nuestro alfabeto de 29 letras). Queremos calcular la clave inversa.

Para ello, aumentamos K *con la matriz de identidad a su derecha y procedemos a aplicar operaciones elementales de fila. (Para mantener los números pequeños, tomamos los restos módulo 29 después de cada operación de fila en lugar de esperar hasta el final). Como es habitual, escribimos* $\simeq$ *para la equivalencia de matrices bajo operaciones elementales de*

filas.[5] *Los cálculos se pueden hacer como sigue:*

$$
\begin{aligned}
(K \mid I) &= \left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right) && (1)\\
&\simeq \left(\begin{array}{cc|cc} 30 & 45 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right) && (2)\\
&\equiv \left(\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right) \pmod{29} && (3)\\
&\simeq \left(\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & -59 & -60 & 1 \end{array}\right) && (4)\\
&\equiv \left(\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 28 & 27 & 1 \end{array}\right) \pmod{29} && (5)\\
&\simeq \left(\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 784 & 756 & 28 \end{array}\right) && (6)\\
&\equiv \left(\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 1 & 2 & 28 \end{array}\right) \pmod{29} && (7)\\
&\simeq \left(\begin{array}{cc|cc} 1 & 0 & -17 & -448 \\ 0 & 1 & 2 & 28 \end{array}\right) && (8)\\
&\equiv \left(\begin{array}{cc|cc} 1 & 0 & 12 & 16 \\ 0 & 1 & 2 & 28 \end{array}\right) \pmod{29} && (9)
\end{aligned}
$$

En el paso (2) multiplicamos la fila superior por 15, que es el inverso módulo 29 del primer pivote 2 (véase la tabla de inversos de $\mathbb{Z}_{29}$ *en la sección 2.2). Y en el paso (6) multiplicamos la fila inferior por 28, que es el inverso módulo 29 del segundo pivote 28. De esta forma*

$$K^{-1} = \begin{pmatrix} 12 & 16 \\ 2 & 28 \end{pmatrix}.$$

También podríamos calcular la matriz inversa por determinantes usando

$$K^{-1} = \frac{1}{|K|} \left(Adj\,(K)\right)^T.$$

Como $|K| = -2$ *y* $(-2)^{-1} \equiv -15 \pmod{29} \equiv 14 \pmod{29}$, *se tiene*

$$K^{-1} = 14 \begin{pmatrix} 5 & -4 \\ -3 & 2 \end{pmatrix}^T = 14 \begin{pmatrix} 5 & -3 \\ -4 & 2 \end{pmatrix} = \begin{pmatrix} 70 & -42 \\ -56 & 28 \end{pmatrix} \equiv \begin{pmatrix} 12 & 16 \\ 2 & 28 \end{pmatrix} \pmod{29}.$$

[5] Nótese que dos matrices que son congruentes módulo m son, de hecho, equivalentes por filas con respecto a los escalares $\mathbb{Z}_{29}$.

3.3.3. Rompiendo el cifrado de Hill

¿Cómo se criptoanaliza un cifrado de Hill? En otras palabras, ¿cómo se descubre la clave inversa cuando no se conoce la clave? Si se ha "capturado" suficiente texto plano junto con el correspondiente texto cifrado, entonces se puede utilizar el siguiente teorema.

Teorema 3. *(**Teorema de ruptura**) Supongamos que la longitud m del alfabeto es un número primo. Sean $\overrightarrow{p}_1, \overrightarrow{p}_2, \ldots, \overrightarrow{p}_n$ n vectores de texto plano para un n-cifrado de Hill que tiene una matriz clave K (desconocida), y sean $\overrightarrow{c}_1, \overrightarrow{c}_2, \ldots, \overrightarrow{c}_n$ los vectores de texto cifrado correspondientes. Supongamos que estos vectores de texto plano son linealmente independientes sobre $\mathbb{Z}_m$. Formamos la matriz*

$$P = \left(\overrightarrow{p}_1 \mid \overrightarrow{p}_2 \mid \cdots \mid \overrightarrow{p}_n \right)$$

teniendo como columnas los vectores de texto plano, y la matriz

$$C = \left(\overrightarrow{c}_1 \mid \overrightarrow{c}_2 \mid \cdots \mid \overrightarrow{c}_n \right)$$

con los vectores de texto cifrado como columnas. Entonces la misma secuencia de operaciones elementales de fila que reduce C^T a la matriz identidad I reduce P^T a la traspuesta $(K^{-1})^T$ de la matriz clave inversa K^{-1}.

Daremos una demostración del Teorema de ruptura que implicará matrices elementales. Se dice que una matriz $n \times n$ es **elemental** cuando se puede obtener a partir de la matriz $n \times n$ identidad I_n realizando una única operación elemental de fila en I_n. Las propiedades que hay que conocer sobre las matrices elementales para seguir la desmostración del Teorema son:

- Realizar una única operación elemental sobre una matriz arbitraria M de $n \times k$ da el mismo resultado que multiplicar M por su izquierda por la matriz elemental E formada al realizar esa misma operación elemental sobre I_n.
- Cada matriz elemental es invertible, y su inversa es también una matriz elemental.

El segundo de estos hechos se mantiene, por supuesto, siempre que los escalares no nulos tengan inversos multiplicativos (de lo contrario, una operación elemental sobre una fila no tiene por qué ser una operación reversible). En nuestra situación, esto significa que $\mathbb{Z}_m$ es un cuerpo, es decir, que m es primo.

Teniendo en cuenta el primero de estos hechos, la matriz escalonada equivalente reducida por filas H de una matriz M puede obtenerse en la forma $E_k \cdots E_2 E_1 M = H$ para ciertas matrices elementales $E_1, E_2, ..., E_k$ (estas matrices elementales son sólo las correspondientes a las sucesivas operaciones elementales de fila necesarias para reducir M a H). En particular, para una matriz invertible M, existen matrices elementales $E_1, E_2, ..., E_k$ para las que $E_k \cdots E_2 E_1 M = I$.

Demostración. *(Del Teorema de ruptura) En primer lugar, hay que tener en cuenta que C^T es realmente equivalente por filas a I, porque es la traspuesta de C, y esta última es invertible dado que, por hipótesis, sus columnas son linealmente independientes. Sean $E_1, E_2, ..., E_k$, para cierto k, las matrices elementales correspondientes a las operaciones elementales de fila que reducen C^T a I. Entonces $E_k \cdots E_2 E_1 C^T = I$. Ahora bien, $K\overrightarrow{p}_j =$*

$\overrightarrow{c}_j$ *para cada* $j = 1, 2, ..., n$, *por lo que* $KP = C$. *Tomando traspuestas, se obtiene* $P^T K^T = C^T$. *Multiplicando ambos lados por* $E_k \cdots E_2 E_1$ *y agrupando los resultados como se indica,*

$$\left(E_k \cdots E_2 E_1 P^T\right) K^T = E_k \cdots E_2 E_1 C^T.$$

Pero el lado derecho es sólo I, *por lo que* $\left(E_k \cdots E_2 E_1 P^T\right) K^T = I$. *Esto demuestra dos cosas: en primer lugar,* K^T *es invertible y, por tanto, la propia* K *–que es* $(K^T)^T$*– es invertible. En segundo lugar, la multiplicación de ambos lados de la última ecuación por* $(K^T)^{-1}$ *–que es igual a* $(K^{-1})^T$*– da como resultado*

$$E_k \cdots E_2 E_1 P^T = (K^{-1})^T.$$

Esto significa que las operaciones elementales de fila correspondientes a $E_1, E_2, ..., E_k$ *reducen* P^T *a* $(K^{-1})^T$. ■

Para que este teorema sea aplicable, se debe conocer –o poderse determinar– el tamaño n de la matriz clave desconocida (así como la longitud del alfabeto m). Si es conocido, y si se tiene n vectores de texto plano y los correspondientes vectores de texto cifrado, se puede proceder a aplicar el teorema. Con la notación utilizada allí, el procedimiento para descifrar un cifrado Hill es el siguiente:

- Utilice la reducción de filas (módulo m) en la matriz $n \times 2n$, $\left(C^T \mid P^T\right)$.
- Si la reducción puede completarse hasta ponerla en forma escalonada reducida, y si esa forma es $(I \mid X)$ para alguna X, entonces los vectores de texto cifrado –que son traspuestas de las filas de C^T– son, de hecho, linealmente independientes, la matriz clave K es invertible, y la mitad derecha X de la forma escalonada reducida $(I \mid X)$ es $(K^{-1})^T$. Entonces K^{-1} es la traspuesta de X.

Ejemplo 7. *Supongamos que conocemos el texto plano PERO y el texto cifrado OZWC correspondiente para un 2-cifrado de Hill. Queremos determinar la clave inversa, para poder descifrar cualquier otro mensaje cifrado que podamos interceptar.*

Separando las letras del texto plano y del texto cifrado, como de costumbre, en grupos de 2, se obtiene los números 16 4 18 15 *y* 15 26 23 2 *correspondientes a las letras del texto llano y del texto cifrado, respectivamente, y formándolos en columnas de 2 filas, los vectores del texto plano son*

$$\overrightarrow{p}_1 = \begin{pmatrix} 16 \\ 4 \end{pmatrix}, \quad \overrightarrow{p}_2 = \begin{pmatrix} 18 \\ 15 \end{pmatrix}$$

y los vectores de texto cifrado correspondientes son

$$\overrightarrow{c}_1 = \begin{pmatrix} 15 \\ 26 \end{pmatrix}, \quad \overrightarrow{c}_2 = \begin{pmatrix} 23 \\ 2 \end{pmatrix}.$$

Así, las matrices P *y* C *del teorema son:*

$$P = (\overrightarrow{p}_1 \mid \overrightarrow{p}_2) = \begin{pmatrix} 16 & 18 \\ 4 & 15 \end{pmatrix},$$

$$C = (\overrightarrow{c}_1 \mid \overrightarrow{c}_2) = \begin{pmatrix} 15 & 23 \\ 26 & 2 \end{pmatrix}.$$

Entonces

$$\left(C^T \mid P^T\right) = \left(\begin{array}{cc|cc} 15 & 26 & 16 & 4 \\ 23 & 2 & 18 & 15 \end{array}\right).$$

Tal como se hizo en el ejemplo 6, se obtiene la forma escalonada reducida módulo 29 de la siguiente manera:

$$\left(\begin{array}{cc|cc} 15 & 26 & 16 & 4 \\ 23 & 2 & 18 & 15 \end{array}\right) \overset{2\cdot F_1}{\cong} \left(\begin{array}{cc|cc} 1 & 23 & 3 & 8 \\ 23 & 2 & 18 & 15 \end{array}\right) \pmod{29}$$

$$\overset{F_2-23\cdot F_1}{\cong} \left(\begin{array}{cc|cc} 1 & 23 & 3 & 8 \\ 0 & 24 & 7 & 5 \end{array}\right) \pmod{29}$$

$$\overset{23\cdot F_2}{\cong} \left(\begin{array}{cc|cc} 1 & 23 & 3 & 8 \\ 0 & 1 & 16 & 28 \end{array}\right) \pmod{29}$$

$$\overset{F_1-23\cdot F_2}{\cong} \left(\begin{array}{cc|cc} 1 & 0 & 12 & 2 \\ 0 & 1 & 16 & 28 \end{array}\right) \pmod{29}$$

y como vimos en la demostración del Teorema de ruptura,

$$\left(K^{-1}\right)^T = \begin{pmatrix} 12 & 2 \\ 16 & 28 \end{pmatrix}$$

y, por tanto,

$$K^{-1} = \begin{pmatrix} 12 & 16 \\ 2 & 28 \end{pmatrix}.$$

(Ésta es la misma matriz inversa que encontramos en el ejemplo 6.)

4. Cifrado de Hill sobre números complejos

El cifrado que se propone a continuación utilizará matrices con entradas en la forma de números complejos ([4]). Más concretamente, en

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \ / \ a, b \in \mathbb{Z}\}.$$

Dado que

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = a\left(a^2+b^2\right)^{-1} - b\left(a^2+b^2\right)^{-1}i,$$

en este caso, $a + bi$ tiene inversa si y sólo si (el cuadrado del módulo) $a^2 + b^2 = 1$. Pero, más aún, trabajaremos con matrices complejas cuyas entradas están en

$$\mathbb{Z}_m[i] = \{a + bi \in \mathbb{C} \ / \ a, b \in \mathbb{Z}_m\},$$

en donde, en consecuencia, $a+bi$ tiene inversa si y sólo si $mcd((a^2+b^2) \pmod m, m) = 1$.

Ejemplo 8. *Sea* $z = 11 - 13i \in \mathbb{Z}_{26}[i]$, *entonces* $a^2 + b^2 = 290 \equiv 4 \pmod{26}$, *y no tiene inversa pues* $mcd((a^2 + b^2) \pmod{26}, 26) = 4 \neq 1$. *Sin embargo, si* $w = -6 + 7i$, *se obtiene* $a^2 + b^2 = 85 \equiv 7 \pmod{26}$, *por lo que existe* w^{-1} *pues* $mcd(7, 26) = 1$. *En este caso,* $7 \cdot 15 = 105 \equiv 1 \pmod{26}$ *y* $7^{-1} = 15$ *en* $\mathbb{Z}_{26}$. *Finalmente, obtenemos*

$$w^{-1} = -6 \cdot 7^{-1} + 7 \cdot 7^{-1}i = -6 \cdot 15 + 7 \cdot 15i = -90 + 105i = (14 + i) \pmod{26}.$$

Supongamos que tenemos un texto plano P ya codificado por números (utilizaremos el alfabeto propuesto):

$$a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7 \quad a_8$$

y una matriz clave K de tamaño 2×2. La ordenación del texto plano se hace mediante la matriz P de texto plano construida por bloques de longitud 2:

$$P = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \end{pmatrix}.$$

Si usamos el cifrado propuesto sobre $\mathbb{C}$, la matriz de texto plano sería:

$$P' = \begin{pmatrix} a_1 + a_2 i & a_3 + a_4 i \\ a_5 + a_6 i & a_7 + a_8 i \end{pmatrix} = \begin{pmatrix} a_1 & a_3 \\ a_5 & a_7 \end{pmatrix} + \begin{pmatrix} a_2 & a_4 \\ a_6 & a_8 \end{pmatrix} i.$$

Así, $P' = M + Ni$, con $M, N \in M_{2\times 2}(\mathbb{Z}_m)$. Nótese que si la matriz clave es de 2×2, la matriz de texto plano será de tamaño $2 \times p$, donde $p = \left\lceil \frac{c}{4} \right\rceil$ y c es el número de caracteres del mensaje de texto plano.[6] En general, si existe una matriz clave K y un texto plano P, el criptosistema de Hill se cifra haciendo $C = KP \pmod{m}$, mientras que con el criptosistema propuesto se entremezclan los cálculos

$$\begin{aligned} C \equiv & \quad KP \pmod{m} \\ \equiv & \quad (M + Ni)(X + Yi) \pmod{m} \\ \equiv & \quad (MX - NY) + (MY + NX)i. \end{aligned}$$

Obsérvese que el algoritmo del criptosistema propuesto aleatoriza más el texto cifrado. Veremos todo el proceso de cifrado y descifrado mediante este criptosistema en el siguiente ejemplo.

Ejemplo 9. *Bernardo enviará un mensaje a Alicia, quienes acordaron utilizar la clave*

$$K = \begin{pmatrix} 4 + 3i & 7 + i \\ 2 + 11i & 5 + 9i \end{pmatrix}.$$

Trabajaremos con el alfabeto propuesto módulo 29. Antes de nada, Bernardo debe asegurarse que K *sea invertible, es decir, que exista* $(\det(K))^{-1}$. *En este caso* $\det(K) = -10 - 28i \equiv (19 + i) \pmod{29}$. *Luego,* $a = 19$ *y* $b = 1$, *y Bernardo calcula* $a^2 + b^2 = 362 \equiv 14 \pmod{29}$, *cuyo inverso* $(a^2 + b^2)^{-1} = 14^{-1} \equiv 27 \pmod{29}$. *De esta forma,*

$$(\det(K))^{-1} = a\left(a^2 + b^2\right)^{-1} - b\left(a^2 + b^2\right)^{-1} i \equiv (19{\cdot}27 - 1{\cdot}27i) \pmod{29} = (20 + 2i) \pmod{29}.$$

[6] En general, si se elige una matriz $n \times n$, entonces $p = \left\lceil \frac{c}{2n} \right\rceil$.

Supongamos que Bernardo quiere enviar el mensaje ESTE MENSAJE ES FALSO. Usando el alfabeto módulo 29, lo convertimos a números:

$$4-19-20-4-12-4-13-19-0-9-4-4-19-5-0-11-19-15$$

A continuación, ordena el texto plano en forma matricial como

$$P=\begin{pmatrix}4+19i & 20+4i & 12+4i & 13+19i & 0+9i\\ 4+4i & 19+5i & 0+11i & 19+15i & 0+0i\end{pmatrix}.$$

***Cifrado**: Bernardo cifra el mensaje calculando*

$$\begin{aligned}C\equiv\ & KP \pmod m\\ \equiv\ & \begin{pmatrix}4+3i & 7+i\\ 2+11i & 5+9i\end{pmatrix}\begin{pmatrix}4+19i & 20+4i & 12+4i & 13+19i & 0+9i\\ 4+4i & 19+5i & 0+11i & 19+15i & 0+0i\end{pmatrix} \pmod{29}\\ \equiv\ & \begin{pmatrix}-17+120i & 196+130i & 25+129i & 113+239i & -27+36i\\ -217+138i & 46+424i & -119+195i & -223+427i & -99+18i\end{pmatrix} \pmod{29}\\ \equiv\ & \begin{pmatrix}12+4i & 22+14i & 25+13i & 26+7i & 2+7i\\ 15+22i & 17+18i & 26+21i & 9+21i & 17+18i\end{pmatrix} \pmod{29}.\end{aligned}$$

Bernardo obtiene, entonces el mensaje cifrado:

$$12-4-22-14-25-13-26-7-2-7-15-22-17-18-26-21-9-21-17-18$$

que, usando de nuevo la tabla del alfabeto, queda como $MEV\tilde{N}YNZH.HOVQRZUJUQR$. Finalmente, Bernardo envía este mensaje cifrado a Alicia.

***Descifrado**: Alicia recibe el texto cifrado de Bernardo. Ella calcula* $(\det(K))^{-1}=20+2i$*. A continuación, halla*

$$\begin{aligned}K^{-1}=\ & (\det(K))^{-1}Adj(K)^T\\ =\ & (20+2i)\begin{pmatrix}5+9i & -(7+i)\\ -(2+11i) & 4+3i\end{pmatrix}\\ =\ & \begin{pmatrix}82+190i & -138-34i\\ -18-224i & 74+68i\end{pmatrix}\\ =\ & \begin{pmatrix}24+16i & 7+24i\\ 11+8i & 16+10i\end{pmatrix} \pmod{29}.\end{aligned}$$

Ahora, Alicia hace el descifrado

$$\begin{aligned} P = & \quad K^{-1}C \pmod{29} \\ = & \quad \begin{pmatrix} 24+16i & 7+24i \\ 11+8i & 16+10i \end{pmatrix} \begin{pmatrix} 12+4i & 22+14i & 25+13i & 26+7i & 2+7i \\ 15+22i & 17+18i & 26+21i & 9+21i & 17+18i \end{pmatrix} \\ = & \quad \begin{pmatrix} -199+802i & -9+1222i & 70+1483i & 71+947i & -377+734i \\ 120+642i & 222+788i & 377+939i & 164+711i & 58+551i \end{pmatrix} \\ = & \quad \begin{pmatrix} 4+19i & 20+4i & 12+4i & 13+19i & 0+9i \\ 4+4i & 19+5i & 0+11i & 19+15i & 0+0i \end{pmatrix} \pmod{29}. \end{aligned}$$

Alicia obtiene, de esta forma, el mensaje

$$P = 4-19-20-4-12-4-13-19-0-9-4-4-19-5-0-11-19-15-0-0.$$

Usando la tabla de conversión, ella consigue el mensaje ESTE MENSAJE ES FALSO AA, descartando las dos últimas letras A.

5. Conclusiones

Estudiamos las propiedades matemáticas de las operaciones matriciales para matrices de restos sobre el plano complejo. La operación de adición en matrices de restos satisface la propiedad conmutativa y la asociativa. Sin embargo, la operación de multiplicación en matrices de restos no satisface las propiedades conmutativa, asociativa y distributiva. La operación de multiplicación escalar sobre matrices de restos satisface la propiedad distributiva sobre la operación de adición pero no respecto a la de multiplicación. Cada matriz de restos tiene tanto inversa aditiva e inversa multiplicativa (bajo ciertas condiciones), y satisface la propiedad de identidad. La nueva implementación del cifrado de Hill sobre plano complejo tiene las propiedades de difusión y confusión más fuertes que los cifrados tradicionales de Hill en los números reales y aumenta la complejidad del texto cifrado debido a transformaciones no lineales. Como consecuencia, el intruso no puede utilizar la relación entre el texto plano y el texto cifrado para encontrar la clave. Por lo tanto, es resistente no solamente a los ataques de texto plano conocido, sino también a los ataques de texto plano elegido y de texto cifrado.

6. Propuesta de continuidad

La seguridad del cifrado Hill depende de la confidencialidad de la matriz clave K y de su rango n. Cuando n es desconocido y el módulo m no es demasiado grande, el adversario podría simplemente probar valores sucesivos de n hasta que encuentre la clave. Si el valor adivinado de n fuera incorrecto, la matriz clave obtenida no sería consistente con otros pares texto plano–texto cifrado. El fallo de seguridad más importante del cifrado de Hill es su vulnerabilidad al ataque de texto plano conocido. Se puede romper tomando sólo n pares distintos de texto plano y texto cifrado (ver teorema 3. En este tipo de ataque, el criptoanalista posee el texto plano de algunos mensajes y el correspondiente texto cifrado

de esos mensajes. Intentará deducir la clave o un algoritmo (ver teorema 3) para descifrar cualquier nuevo mensaje cifrado con la misma clave.

Una propuesta para introducir una variante segura del cifrado de Hill, es ampliarlo mezclándolo con una transformación afín no lineal (ver [7]), por lo que la expresión de cifrado tendrá la forma $C = KP+V \pmod{m}$. Adicionalmente, partiendo de esta estructura de cifrado de Hill afín, y con el fin de dar más aleatoriedad al esquema introducido y fortalecerlo contra los ataques habituales, cada bloque de datos se puede cifrar utilizando números aleatorios,como se propone en [8]. El número aleatorio básico que se genera antes del cifrado debe ser compartido de forma segura entre los participantes.

Referencias

[1] Dummit, D. y Foote, R., *Abstract Algebra*, John Wiley & Sons, 2004.

[2] Hill, L. S., «Cryptography in an Algebraic Alphabet», *The American Mathematical Monthly*, **36**, págs. 306–312, 1929.

[3] Hill, L. S., «Concerning Certain Linear Transformation Apparatus of Cryptography», *The American Mathematical Monthly*, **38**, págs. 135–154, 1931.

[4] Maxrizal, M., «Hill Cipher Cryptosystem over Complex Numbers», *Indonesian Journal of Mathematics Education*, **2**, págs. 9–13, 2019.

[5] Niven, I. y Zuckerman, H., *Introducción a la Teoría de los Números*, Limusa, 1976.

[6] Rubinstein-Salzedo, S., *Cryptography*, Springer, 2018.

[7] Stinson, D., *Cryptography: Theory and Practice*, Chapman & Hall, 2018.

[8] Toorani, M. y Falahati, A., «A Secure Variant of the Hill Cipher», *IEEE Symposium on Computers and Communications*, **2**, págs. 313–316, 2009.

A. Cifrado de Hill en $\mathbb{Z}_m$ con SageMath

Presentamos el algoritmo del cifrado de Hill en el código SageMath, que nos permitió realizar cálculos de mayor complejidad.

Cifrado de Hill en $\mathbb{Z}_m$

April 28, 2021

1 Cifrado de Hill

Veremos un ejemplo del cifrado de Hill con matrices 4x4 y trabajando con aritmética modular, módulo 256.

2 Cifrar

[2]:
```
mensaje_texto="La fecha de defensa de este proyecto ante el tribunal es␣
↪abril de 2021"
```

2.1 Paso 1. Convertimos el texto en una lista de caracteres alfabéticos

[3]:
```
lista_mensaje_texto=list(mensaje_texto)
```

[4]:
```
lista_mensaje_texto
```

[4]:
```
['L',
 'a',
 ' ',
 'f',
 'e',
 'c',
 'h',
 'a',
 ' ',
 'd',
 'e',
 ' ',
 'd',
 'e',
 'f',
 'e',
```

```
'n',
's',
'a',
' ',
'd',
'e',
' ',
'e',
's',
't',
'e',
' ',
'p',
'r',
'o',
'y',
'e',
'c',
't',
'o',
' ',
'a',
'n',
't',
'e',
' ',
'e',
'l',
' ',
't',
'r',
'i',
'b',
'u',
'n',
'a',
'l',
' ',
'e',
's',
' ',
'a',
'b',
'r',
```

```
 'i',
 'l',
 ' ',
 'd',
 'e',
 ' ',
 '2',
 '0',
 '2',
 '1']
```

2.2 Paso 2. Convertimos los caracteres alfabéticos en números.

[5]:
```
lista_mensaje_numeros=list(map(ord,lista_mensaje_texto))
```

Ejemplo con aritmética modular 256 (código UNICODE, diferente del ASCII extendido) y una matriz 4x4.

[11]:
```
M=matrix(Integers(256),[[13,1,3,41],[29,15,9,2],[50,34,57,10],[44,17,4,7]])
 ↪# matriz clave
```

[12]:
```
det(M)  # tiene inversa
```

[12]:
```
51
```

[13]:
```
M^(-1)
```

[13]:
```
[ 81 250 143  91]
[  1 199   2 227]
[ 90 184 243  24]
[205  71  18  70]
```

2.2.1 Paso AJUSTAR TAMAÑO.

Ya que trabajos con matrices 4x4, la lista original tiene que tener una longitud de un múltiplo de 4. En caso de que no lo sea, le añadimos una E; o una T y una E; o una S, una T y una E.

[19]:
```
def mensaje3(lista):
    if len(lista)%4==1:
        lista.extend([83,84,69])  # añadimos S, T y E
    elif len(lista)%4==2:
        lista.extend([84,69])  # añadimos T y E
    elif len(lista)%4==3:
```

```
        lista.append(69)  # añadimos E
    return(lista)
```

[20]:
```
mensaje3(lista_mensaje_numeros)
```

[20]:
```
[76,
 97,
 32,
 102,
 101,
 99,
 104,
 97,
 32,
 100,
 101,
 32,
 100,
 101,
 102,
 101,
 110,
 115,
 97,
 32,
 100,
 101,
 32,
 101,
 115,
 116,
 101,
 32,
 112,
 114,
 111,
 121,
 101,
 99,
 116,
 111,
 32,
 97,
 110,
```

```
116,
101,
32,
101,
108,
32,
116,
114,
105,
98,
117,
110,
97,
108,
32,
101,
115,
32,
97,
98,
114,
105,
108,
32,
100,
101,
32,
50,
48,
50,
49,
84,
69]
```

[21]:
```
len(mensaje3(lista_mensaje_numeros)) # Nótese que la lista tiene longitud␣
↪un múltiplo de 4
```

[21]: 72

2.3 Paso 3. Convertimos el mensaje en una matriz con 4 filas.

[22]:
```
matriz_plano=matrix(Integers(256),4,len(mensaje3(lista_mensaje_numeros))/
↪4,mensaje3(lista_mensaje_numeros))
```

[23]:
```
matriz_plano
```

[23]:
```
[ 76  97  32 102 101  99 104  97  32 100 101  32 100 101 102 101 110 115]
[ 97  32 100 101  32 101 115 116 101  32 112 114 111 121 101  99 116 111]
[ 32  97 110 116 101  32 101 108  32 116 114 105  98 117 110  97 108  32]
[101 115  32  97  98 114 105 108  32 100 101  32  50  48  50  49  84  69]
```

[24]:
```
matriz_plano.str()  # para ver las entradas de la matriz
```

[24]:
```
'[ 76  97  32 102 101  99 104  97  32 100 101  32 100 101 102 101 110␣
↪115]\n[ 97
32 100 101  32 101 115 116 101  32 112 114 111 121 101  99 116 111]\n[ 32␣
↪ 97
110 116 101  32 101 108  32 116 114 105  98 117 110  97 108  32]\n[101␣
↪115  32
97  98 114 105 108  32 100 101  32  50  48  50  49  84  69]'
```

2.4 Paso 4. Ciframos el mensaje multiplicando por la matriz clave.

[26]:
```
C=M*matriz_plano  # mensaje cifrado
```

[27]:
```
C
```

[27]:
```
[202 155 110 120  34  14 187 241 133 148  20 109 171 169 223 128 194 179]
[ 53  44 154  79 162  38 228 109 235  16 205  63 171   5 187   9 182  50]
[204  73  70 244  75  84  45 158  10 132 238   5  12 185 200  99  56   6]
[196 117 188 180 190  87 246   4 149 220  87 150 117 137  83 202 152 134]
```

[28]:
```
C.str()
```

[28]:
```
'[202 155 110 120  34  14 187 241 133 148  20 109 171 169 223 128 194␣
↪179]\n[ 53
44 154  79 162  38 228 109 235  16 205  63 171   5 187   9 182  50]\n[204␣
↪ 73
70 244  75  84  45 158  10 132 238   5  12 185 200  99  56   6]\n[196 117␣
↪188
180 190  87 246   4 149 220  87 150 117 137  83 202 152 134]'
```

2.5 Paso 5. Ahora convertimos la matriz cifrada en una lista de números.

[29]:
```
cifrado_lista=C.dense_coefficient_list()
```

[30]:
```
cifrado_lista
```

[30]:
```
[202,
 155,
 110,
 120,
 34,
 14,
 187,
 241,
 133,
 148,
 20,
 109,
 171,
 169,
 223,
 128,
 194,
 179,
 53,
 44,
 154,
 79,
 162,
 38,
 228,
 109,
 235,
 16,
 205,
 63,
 171,
 5,
 187,
 9,
 182,
 50,
 204,
```

```
73,
70,
244,
75,
84,
45,
158,
10,
132,
238,
5,
12,
185,
200,
99,
56,
6,
196,
117,
188,
180,
190,
87,
246,
4,
149,
220,
87,
150,
117,
137,
83,
202,
152,
134]
```

2.6 Paso 6. Convertimos la lista cifrada de números en caracteres alfabéticos de UNICODE.

[31]:
```
cifrado_lista_texto=list(map(chr,cifrado_lista))
```

[32]:
```
cifrado_lista_texto
```

[32]:
```
['Ê',
 '\x9b',
 'n',
 'x',
 '"',
 '\x0e',
 '»',
 'ñ',
 '\x85',
 '\x94',
 '\x14',
 'm',
 '«',
 '©',
 'ß',
 '\x80',
 'Â',
 'ɜ',
 '5',
 ',',
 '\x9a',
 'O',
 '¢',
 '&',
 'ä',
 'm',
 'ë',
 '\x10',
 'Í',
 '?',
 '«',
 '\x05',
 '»',
 '\t',
 '¶',
 '2',
 'Ì',
 'I',
 'F',
 'ô',
 'K',
 'T',
 '-',
 '\x9e',
```

```
 '\n',
 '\x84',
 'î',
 '\x05',
 '\x0c',
 '¹',
 'È',
 'c',
 '8',
 '\x06',
 'Ä',
 'u',
 '¼',
 '´',
 '¾',
 'W',
 'ö',
 '\x04',
 '\x95',
 'Ü',
 'W',
 '\x96',
 'u',
 '\x89',
 'S',
 'Ê',
 '\x98',
 '\x86']
```

2.7 Paso 7. Convertimos la lista en una expresión de caracteres de UNICODE.

Este sería el mensaje cifrado

[34]:
```
texto_cifrado= ''.join(cifrado_lista_texto)
```

[35]:
```
texto_cifrado
```

[35]:
```
'Ê\x9bnx"\x0e»ñ\x85\x94\x14m«©ß\x80Â³5,\x9aO¢&ämë\x10Í?
 ↪«\x05»\t¶2ÌIFôKT-\x9e\n\x
84î\x05\x0c¹Èc8\x06Äu¼´¾Wö\x04\x95ÜW\x96u\x89SÊ\x98\x86'
```

Descifrar

Ahora viene el proceso inverso de descifrar. Se repetirían los pasos anteriores, pero en un orden inverso.

2.8 Paso 1. Convertimos el texto en una lista de caracteres alfabéticos.

[36]:
```
lista_mensaje_cifrado=list(texto_cifrado)
```

[37]:
```
lista_mensaje_cifrado
```

[37]:
```
['Ê',
 '\x9b',
 'n',
 'x',
 '"',
 '\x0e',
 '»',
 'ñ',
 '\x85',
 '\x94',
 '\x14',
 'm',
 '«',
 '©',
 'ß',
 '\x80',
 'Â',
 '³',
 '5',
 ',',
 '\x9a',
 'O',
 '¢',
 '&',
 'ä',
 'm',
 'ë',
 '\x10',
 'Í',
 '?',
 '«',
 '\x05',
 '»',
 '\t',
 '¶',
```

```
'2',
'Ì',
'I',
'F',
'ô',
'K',
'T',
'-',
'\x9e',
'\n',
'\x84',
'î',
'\x05',
'\x0c',
'¹',
'È',
'c',
'8',
'\x06',
'Ä',
'u',
'¼',
'´',
'¾',
'W',
'ö',
'\x04',
'\x95',
'Ü',
'W',
'\x96',
'u',
'\x89',
'S',
'Ê',
'\x98',
'\x86']
```

2.9 Paso 2. Convertimos los caracteres alfabéticos en números.

[39]:
```
lista_mensaje_cifrado_numeros=list(map(ord,lista_mensaje_cifrado))
```

[40]:
```
lista_mensaje_cifrado_numeros
```

```
[40]: [202,
       155,
       110,
       120,
       34,
       14,
       187,
       241,
       133,
       148,
       20,
       109,
       171,
       169,
       223,
       128,
       194,
       179,
       53,
       44,
       154,
       79,
       162,
       38,
       228,
       109,
       235,
       16,
       205,
       63,
       171,
       5,
       187,
       9,
       182,
       50,
       204,
       73,
       70,
       244,
       75,
       84,
       45,
       158,
```

```
 10,
 132,
 238,
 5,
 12,
 185,
 200,
 99,
 56,
 6,
 196,
 117,
 188,
 180,
 190,
 87,
 246,
 4,
 149,
 220,
 87,
 150,
 117,
 137,
 83,
 202,
 152,
 134]
```

[41]:
```
len(lista_mensaje_cifrado_numeros)
```

[41]:
```
72
```

2.10 Paso 3. Convertimos el mensaje en una matriz con 4 filas.

[42]:
```
matriz_cifrado=matrix(Integers(256),4,len(lista_mensaje_cifrado_numeros)/
 ↪4,lista_mensaje_cifrado_numeros)
```

[43]:
```
matriz_cifrado
```

[43]:
```
[202 155 110 120  34  14 187 241 133 148  20 109 171 169 223 128 194 179]
[ 53  44 154  79 162  38 228 109 235  16 205  63 171   5 187   9 182  50]
[204  73  70 244  75  84  45 158  10 132 238   5  12 185 200  99  56   6]
```

```
[196 117 188 180 190  87 246   4 149 220  87 150 117 137  83 202 152 134]
```

[44]:
```
(matriz_cifrado).str()
```

[44]:
```
'[202 155 110 120  34  14 187 241 133 148  20 109 171 169 223 128 194␣
 ↪179]\n[ 53
44 154  79 162  38 228 109 235  16 205  63 171   5 187   9 182  50]\n[204␣
 ↪ 73
70 244  75  84  45 158  10 132 238   5  12 185 200  99  56   6]\n[196 117␣
 ↪188
180 190  87 246   4 149 220  87 150 117 137  83 202 152 134]'
```

2.11 Paso 4. Desciframos el mensaje multiplicando por la inversa de la matriz clave.

[45]:
```
MO=M^(-1)*matriz_cifrado
```

[46]:
```
MO.str()
```

[46]:
```
'[ 76  97  32 102 101  99 104  97  32 100 101  32 100 101 102 101 110␣
 ↪115]\n[ 97
32 100 101  32 101 115 116 101  32 112 114 111 121 101  99 116 111]\n[ 32␣
 ↪ 97
110 116 101  32 101 108  32 116 114 105  98 117 110  97 108  32]\n[101␣
 ↪115  32
97  98 114 105 108  32 100 101  32  50  48  50  49  84  69]'
```

2.12 Paso 5. Ahora convertimos la matriz cifrada en una lista de números.

[47]:
```
descifrado_lista=MO.dense_coefficient_list()
```

[48]:
```
descifrado_lista
```

[48]:
```
[76,
 97,
 32,
 102,
 101,
 99,
 104,
 97,
```

```
32,
100,
101,
32,
100,
101,
102,
101,
110,
115,
97,
32,
100,
101,
32,
101,
115,
116,
101,
32,
112,
114,
111,
121,
101,
99,
116,
111,
32,
97,
110,
116,
101,
32,
101,
108,
32,
116,
114,
105,
98,
117,
110,
97,
```

```
 108,
 32,
 101,
 115,
 32,
 97,
 98,
 114,
 105,
 108,
 32,
 100,
 101,
 32,
 50,
 48,
 50,
 49,
 84,
 69]
```

2.13 Paso 6. Convertimos la lista cifrada de números en caracteres alfabéticos de UNICODE.

[49]:
```
descifrado_lista_texto=list(map(chr,descifrado_lista))
```

[50]:
```
descifrado_lista_texto
```

[50]:
```
['L',
 'a',
 ' ',
 'f',
 'e',
 'c',
 'h',
 'a',
 ' ',
 'd',
 'e',
 ' ',
 'd',
 'e',
 'f',
```

```
'e',
'n',
's',
'a',
' ',
'd',
'e',
' ',
'e',
's',
't',
'e',
' ',
'p',
'r',
'o',
'y',
'e',
'c',
't',
'o',
' ',
'a',
'n',
't',
'e',
' ',
'e',
'l',
' ',
't',
'r',
'i',
'b',
'u',
'n',
'a',
'l',
' ',
'e',
's',
' ',
'a',
'b',
```

```
 'r',
 'i',
 'l',
 ' ',
 'd',
 'e',
 ' ',
 '2',
 '0',
 '2',
 '1',
 'T',
 'E']
```

2.14 Paso 7. Convertimos la lista en una expresión de caracteres de UNICODE.

(Este sería el mensaje original).

[51]:
```
texto_original= ''.join(descifrado_lista_texto)
```

[52]:
```
texto_original
```

[52]:
```
'La fecha de defensa de este proyecto ante el tribunal es abril de 2021TE'
```

Todos los pasos del cifrado de Hill lo podemos organizar en un programa.

[53]:
```
def cifrado_Hill(matriz,mensaje_texto):
    lista_mensaje_texto=list(mensaje_texto)
    lista_mensaje_numeros=list(map(ord,lista_mensaje_texto))
    ␣
 ↪matriz_plano=matrix(Integers(256),4,len(mensaje3(lista_mensaje_numeros))/
 ↪4,mensaje3(lista_mensaje_numeros))
    C=matriz*matriz_plano
    cifrado_lista=C.dense_coefficient_list()
    cifrado_lista_texto=list(map(chr,cifrado_lista))
    texto_cifrado= ''.join(cifrado_lista_texto)
    return texto_cifrado
```

[54]:
```
cifrado_Hill(M,mensaje_texto)
```

[54]:
```
'Ê\x9bnx"\x0e»ñ\x85\x94\x14m«©ß\x80Â³5,\x9aO¢&ämë\x10Í?
 ↪«\x05»\t¶2ÌIFôKT-\x9e\n\x
```

```
84î\x05\x0c¹Èc8\x06Äu¼´¾Wö\x04\x95ÜW\x96u\x89SÊ\x98\x86'
```

Todos los pasos del descifrado de Hill lo podemos organizar en un programa.

[55]:
```
def descifrado_Hill(matriz,texto_cifrado):
    lista_mensaje_cifrado=list(texto_cifrado)
    lista_mensaje_cifrado_numeros=list(map(ord,lista_mensaje_cifrado))
    ␣
 ↪matriz_cifrado=matrix(Integers(256),4,len(lista_mensaje_cifrado_numeros)/
 ↪4,lista_mensaje_cifrado_numeros)
    MO=matriz^(-1)*matriz_cifrado
    descifrado_lista=MO.dense_coefficient_list()
    descifrado_lista_texto=list(map(chr,descifrado_lista))
    texto_original= ''.join(descifrado_lista_texto)
    return texto_original
```

[56]:
```
descifrado_Hill(M,texto_cifrado)
```

[56]:
```
'La fecha de defensa de este proyecto ante el tribunal es abril de 2021TE'
```

[0]:
```

```

[0]:
```

```

B. Cifrado de Hill en $\mathbb{Z}_m[i]$ con SageMath

Cifrado de Hill en $\mathbb{Z}_m[i]$

April 28, 2021

1 Enteros Gaussianos módulo n

[2]:
```
G=ZZ[I]  # enteros Gaussianos
```

[3]:
```
J=G.ideal([256])
```

[4]:
```
Gn=G.quotient(J,'x')
```

[5]:
```
i=Gn(I)
```

2 Cifrado de Hill usando enteros gaussianos módulo 256

3 Proceso de cifrado

[107]:
```
M=matrix(Gn,3,3,[113+229*i,134+109*i,141+231*i,11+24*i,12+103*i,24+35*i,63+36*i,177+243
 ↪# matriz clave
```

[108]:
```
show(M)
```

[108]:
$$\begin{pmatrix} -27*I + 113 & 109*I - 122 & -25*I - 115 \\ 24*I + 11 & 103*I + 12 & 35*I + 24 \\ 36*I + 63 & -13*I - 79 & 39*I + 113 \end{pmatrix}$$

[109]:
```
det(M) #  a+b*I tiene inverso en  Z/256Z[i]  si, y solo si, a^2+b^2 es␣
 ↪una unidad en Z/256Z (es decir, es impar)
```

[109]:
```
-2*I - 23
```

[110]:
```
2^2+23^2  # tiene que ser impar para que exista la inversa de M
```

[110]:
```
533
```

[111]:
```
M^(-1)   # matriz clave inversa
```

[111]:
```
[   40*I + 12   21*I - 117   115*I + 88]
[   98*I - 67   113*I - 99   110*I - 14]
[   94*I + 71 -121*I + 102  -118*I + 83]
```

3.1 Ajustar tamaño y completar bloques

Ya que se trabaja con matrices 3x3, la lista del mensaje original tiene que tener una longitud de un múltiplo de 6 (después cambiamos a los enteros gaussianos). En caso de que no lo sea, le añadimos una de estas letras: E, D, U, A, R

[112]:
```
def mensaje3g(lista):
    if len(lista)%6==1:
        lista.extend([69,68,85,65,82])   # añadimos E, D, U, A, R
    elif len(lista)%6==2:
        lista.extend([69,68,85,65])    # añadimos E, D, U, A
    elif len(lista)%6==3:
        lista.extend([69,68,85])    # añadimos E, D, U
    elif len(lista)%6==4:
        lista.extend([69,68])   # añadimos E, D
    elif len(lista)%6==5:
        lista.append(69)  # añadimos E
    return(lista)
```

[113]:
```
list(map(ord,['E','D','U','A','R']))
```

[113]:
```
[69, 68, 85, 65, 82]
```

3.2 Convertir la lista en enteros gaussianos

Ya que se trabaja números en Z/256Z, pasamos a escribir esos números en la lista de la forma x y en x+Iy

[114]:
```
lista=[1,2,3,4,5,6]
```

[115]:
```
lista_i=[lista[2*k]+i*lista[2*k+1] for k in range(len(lista)/2)]
```

[116]:
```
lista_i
```

[116]:
```
[2*I + 1, 4*I + 3, 6*I + 5]
```

[117]:
```

```

```
mensaje_texto="El proyecto STEMbach de Criptografía: El Cifrado de Hill,␣
 ↪realizado por alumnado del IES Eduardo Blanco Amor de Ourense Diego␣
 ↪González, Lucía Hermosilla y Brais López, tutorizados por los␣
 ↪profesores Manuel Ladra, del Departamento de Álgebra de la Universidad␣
 ↪de Santiago de Compostela y Carlos Ferreiro del Departamento de␣
 ↪Matemáticas del IES Blanco Amor. El proyecto STEMbach permite al␣
 ↪alumnado de bachillerato entrar en contacto con la labor investigadora,␣
 ↪a través de su participación en proyectos de investigación científica y␣
 ↪tecnológicos diseñados y dirigidos por profesorado universitario de la␣
 ↪USC. Este proyecto de Criptografía será presentado el 28 de abril del␣
 ↪año 2021 ante la comisión evaluadora"
```

[118]:
```
lista_mensaje_texto=list(mensaje_texto)
```

[119]:
```
lista_mensaje_numeros=list(map(ord,lista_mensaje_texto))
```

[121]:
```
len(mensaje3g(lista_mensaje_numeros))
```

[121]:
```
714
```

[122]:
```
lista_mensaje_numeros_i=[mensaje3g(lista_mensaje_numeros)[2*k]+i*mensaje3g(lista_mensaj
 ↪for k in range(len(mensaje3g(lista_mensaje_numeros))/2)]
```

[124]:
```
matriz_plano=matrix(Gn,3,len(mensaje3g(lista_mensaje_numeros_i))/
 ↪3,mensaje3g(lista_mensaje_numeros_i))
```

[125]:
```
matriz_plano
```

[125]:
```
3 x 120 dense matrix over Quotient of Gaussian Integers in Number Field␣
 ↪in I
with defining polynomial x^2 + 1 with I = 1*I by the ideal (256) (use the
'.str()' method to see the entries)
```

[126]:
```
matriz_plano.str()
```

[126]:
```
'[ 108*I + 69  112*I + 32 111*I + 114 101*I + 121  116*I + 99  32*I + 111␣
 ↪  84*I
+ 83   77*I + 69   97*I + 98  104*I + 99  100*I + 32  32*I + 101  114*I +␣
 ↪67
112*I + 105 111*I + 116 114*I + 103  102*I + 97   97*I - 19   32*I + 58 ␣
 ↪108*I +
69   67*I + 32 102*I + 105  97*I + 114 111*I + 100  100*I + 32  32*I + 101
105*I + 72 108*I + 108   32*I + 44 101*I + 114  108*I + 97 122*I + 105 ␣
 ↪100*I +
```

```
97  32*I + 111 111*I + 112  32*I + 114  108*I + 97 109*I + 117  97*I +␣
 ↪110 111*I
+ 100  100*I + 32 108*I + 101   73*I + 32   83*I + 69   69*I + 32 117*I +␣
 ↪100
114*I + 97 111*I + 100   66*I + 32  97*I + 108  99*I + 110  32*I + 111 ␣
 ↪109*I +
65 114*I + 111  100*I + 32  32*I + 101  117*I + 79 101*I + 114 115*I +␣
 ↪110  32*I
+ 101  105*I + 68 103*I + 101  32*I + 111  111*I + 71 122*I + 110  108*I␣
 ↪- 31
122*I + 101   32*I + 44  117*I + 76  -19*I + 99   32*I + 97  101*I + 72␣
 ↪109*I +
114 115*I + 111 108*I + 105  97*I + 108  121*I + 32   66*I + 32  97*I +␣
 ↪114
115*I + 105   76*I + 32  112*I - 13 122*I + 101   32*I + 44 117*I + 116␣
 ↪111*I +
116 105*I + 114  97*I + 122 111*I + 100  32*I + 115 111*I + 112  32*I +␣
 ↪114
111*I + 108  32*I + 115 114*I + 112 102*I + 111 115*I + 101 114*I + 111␣
 ↪115*I +
101   77*I + 32  110*I + 97 101*I + 117  32*I + 108   97*I + 76 114*I +␣
 ↪100
44*I + 97  100*I + 32 108*I + 101   68*I + 32 112*I + 101  114*I + 97 ␣
 ↪97*I +
116 101*I + 109 116*I + 110  32*I + 111 101*I + 100  -63*I + 32 103*I +␣
 ↪108
98*I + 101  97*I + 114]\n[ 100*I + 32  32*I + 101  97*I + 108   85*I + 32␣
 ↪105*I
+ 110 101*I + 118 115*I + 114 100*I + 105  100*I + 97  100*I + 32  32*I +␣
 ↪101
97*I + 83 116*I + 110  97*I + 105 111*I + 103  100*I + 32  32*I + 101 ␣
 ↪111*I +
67 112*I + 109 115*I + 111 101*I + 116  97*I + 108  121*I + 32   67*I + 32
114*I + 97 111*I + 108  32*I + 115  101*I + 70 114*I + 114 105*I + 101␣
 ↪111*I +
114  100*I + 32 108*I + 101   68*I + 32 112*I + 101  114*I + 97  97*I +␣
 ↪116
101*I + 109 116*I + 110  32*I + 111 101*I + 100   77*I + 32  116*I + 97␣
 ↪109*I +
101  116*I - 31  99*I + 105  115*I + 97  100*I + 32 108*I + 101   73*I +␣
 ↪32
83*I + 69   66*I + 32  97*I + 108  99*I + 110  32*I + 111  109*I + 65␣
 ↪114*I +
```

```
111   32*I + 46  108*I + 69  112*I + 32 111*I + 114 101*I + 121  116*I +␣
 ↪99
32*I + 111   84*I + 83   77*I + 69   97*I + 98  104*I + 99  112*I + 32␣
 ↪114*I +
101 105*I + 109 101*I + 116   97*I + 32  32*I + 108  108*I + 97 109*I +␣
 ↪117
97*I + 110 111*I + 100  100*I + 32  32*I + 101   97*I + 98  104*I + 99␣
 ↪108*I +
105 101*I + 108  97*I + 114 111*I + 116  101*I + 32 116*I + 110  97*I +␣
 ↪114
32*I + 114 110*I + 101   99*I + 32 110*I + 111  97*I + 116  116*I + 99 ␣
 ↪32*I +
111  111*I + 99  32*I + 110  97*I + 108  108*I + 32   98*I + 97 114*I +␣
 ↪111
105*I + 32 118*I + 110 115*I + 101 105*I + 116  97*I + 103 111*I + 100 ␣
 ↪97*I +
114   32*I + 44   32*I + 97 114*I + 116  118*I + 97  115*I - 23  100*I +␣
 ↪32
32*I + 101 117*I + 115  112*I + 32  114*I + 97 105*I + 116]\n[ 105*I + 99␣
 ↪ 97*I
+ 112  105*I + 99  110*I - 13  101*I + 32  32*I + 110 114*I + 112 121*I +␣
 ↪111
99*I + 101 111*I + 116  32*I + 115 101*I + 100  105*I + 32 118*I + 110␣
 ↪115*I +
101 105*I + 116  97*I + 103  105*I + 99  110*I - 13   99*I + 32 101*I +␣
 ↪105
116*I + 110  102*I - 19  99*I + 105   32*I + 97  32*I + 121 101*I + 116 ␣
 ↪110*I +
99 108*I + 111  103*I - 13  99*I + 105 115*I + 111  100*I + 32 115*I +␣
 ↪105 -15*I
+ 101  100*I + 97 115*I + 111  121*I + 32  100*I + 32 114*I + 105 103*I +␣
 ↪105
100*I + 105 115*I + 111  112*I + 32 114*I + 111  112*I + 32 111*I + 114␣
 ↪101*I +
102 111*I + 115  97*I + 114 111*I + 100  117*I + 32 105*I + 110 101*I +␣
 ↪118
115*I + 114 116*I + 105  114*I + 97 111*I + 105  100*I + 32  32*I + 101 ␣
 ↪97*I +
108   85*I + 32   67*I + 83   32*I + 46  115*I + 69 101*I + 116  112*I +␣
 ↪32
111*I + 114 101*I + 121  116*I + 99  32*I + 111 101*I + 100   67*I + 32␣
 ↪105*I +
```

```
114 116*I + 112 103*I + 111  97*I + 114 -19*I + 102   32*I + 97 101*I +␣
 ↪115
-31*I + 114  112*I + 32 101*I + 114 101*I + 115 116*I + 110  100*I + 97 ␣
 ↪32*I +
111 108*I + 101   50*I + 32   32*I + 56 101*I + 100   97*I + 32  114*I +␣
 ↪98
108*I + 105  100*I + 32 108*I + 101   97*I + 32  111*I - 15   50*I + 32  ␣
 ↪50*I +
48   32*I + 49  110*I + 97 101*I + 116  108*I + 32   32*I + 97  111*I +␣
 ↪99 105*I
+ 109 105*I + 115  110*I - 13  101*I + 32  97*I + 118 117*I + 108  100*I␣
 ↪+ 97
114*I + 111   69*I + 97   85*I + 68   82*I + 65          69          68
85]'
```

[127]:
```
C=M*matriz_plano # mensaje cifrado
```

[128]:
```
C
```

[128]:
```
3 x 120 dense matrix over Quotient of Gaussian Integers in Number Field␣
 ↪in I
with defining polynomial x^2 + 1 with I = 1*I by the ideal (256) (use the
'.str()' method to see the entries)
```

[129]:
```
C.str()
```

[129]:
```
'[ -121*I - 51    78*I + 87   -27*I + 10   -53*I + 52    16*I + 75  ␣
 ↪105*I - 40
-23*I + 6  -111*I - 22    -54*I - 5   62*I - 110   -22*I + 97   115*I + 11
-124*I - 86    24*I - 18   50*I + 108   -18*I - 50    -22*I + 5  -99*I +␣
 ↪111
-26*I - 19    65*I + 71  -43*I - 102   -37*I + 64   -54*I + 71  107*I -␣
 ↪110
-28*I + 117     94*I - 1   -59*I + 46    -33*I - 8    87*I - 99   -122*I␣
 ↪+ 8
91*I + 30    63*I - 63   102*I - 93   -71*I + 59  -80*I + 125   -82*I + 31
27*I - 2  -110*I - 94   -71*I + 93      -I + 74   -80*I - 25  -58*I - 119␣
 ↪  94*I
- 109    -5*I + 59  -115*I + 14    48*I - 38  -105*I + 71    22*I + 16   ␣
 ↪51*I +
38  -114*I - 43    75*I - 79   -24*I + 18    27*I + 66    96*I + 77   ␣
 ↪-4*I + 43
```

```
-41*I - 69  -112*I + 85   -57*I + 25     6*I + 53   124*I - 58  -78*I +␣
↪117
-28*I - 76    22*I + 15    -89*I - 4    41*I + 86   -19*I - 53     67*I +␣
↪2
20*I - 9  -79*I + 117    18*I - 31    13*I - 51    28*I + 23   68*I + 111
125*I + 19   98*I - 117    48*I - 18  -16*I + 109    3*I + 126   -22*I +␣
↪70
-41*I - 20   119*I - 26   -10*I + 45   -17*I + 20  -68*I - 121   -33*I -␣
↪44
-36*I - 113 -102*I + 103   32*I + 114    45*I - 70   113*I + 39   -95*I +␣
↪30
-39*I + 100   -86*I - 63   100*I - 17    85*I + 72  -13*I + 104   -86*I +␣
↪94
-51*I - 115   72*I + 115   -97*I + 85  -61*I - 108     74*I + 7   -97*I -␣
↪40
-61*I + 73    32*I - 98     3*I - 42 -107*I - 109    77*I - 90   -49*I +␣
↪64
-58*I + 74   11*I + 116 -118*I - 122  -62*I + 125   -12*I + 14   -21*I -␣
↪75
-9*I - 54   -41*I - 85 -106*I - 102  -16*I - 101   -40*I + 97]\n[    13*I␣
↪+ 8
91*I - 7  -42*I + 116    20*I - 58   74*I + 123    8*I - 102   -90*I - 82
59*I + 76    41*I + 93 -108*I + 120    40*I + 68   -19*I - 59    24*I + 82
-115*I + 22  -31*I + 126  -46*I - 122   -54*I - 36  -19*I + 127   116*I +␣
↪72
-47*I + 61    28*I - 18   36*I + 112    94*I - 27   -52*I - 66  -18*I +␣
↪102
11*I - 74    92*I - 43 -125*I + 103      3*I + 2   119*I - 98    113*I + 9
-101*I + 6  -41*I + 103     -5*I + 8 -113*I - 103         18*I   -23*I +␣
↪35
-10*I - 67  -19*I + 114   89*I + 122    71*I - 48    83*I - 24  -113*I +␣
↪23
-88*I - 64  -53*I - 102    42*I + 27   103*I + 69    31*I - 23   -86*I +␣
↪19
69*I + 26   76*I + 124    24*I - 72  -87*I - 111   -50*I - 87   -45*I + 75
86*I - 124    99*I + 69   -52*I + 97   -44*I + 14   -57*I - 33   -47*I -␣
↪96
-88*I + 25   -82*I + 92   -32*I - 23    26*I + 33   111*I - 35  -112*I +␣
↪40
51*I + 51    74*I + 69   -37*I + 83   108*I + 16    -93*I - 2    115*I - 2
-69*I - 126   -61*I + 31   79*I + 128  -81*I - 106   112*I + 96   -82*I -␣
↪54
```

```
29*I - 112   -20*I - 66   45*I + 109    19*I + 64   -31*I + 74    59*I -␣
 ↪55
40*I - 57    -4*I - 13    60*I + 86   -97*I + 95    46*I + 73   52*I + 115
12*I + 78   -52*I - 56  -37*I + 110  107*I + 108   -30*I + 61   -22*I + 71
107*I - 56   121*I - 62   127*I - 34    36*I + 49   -29*I - 13   -96*I -␣
 ↪10
-107*I + 22  -112*I - 53  -123*I + 87     8*I - 86    29*I - 85   -33*I +␣
 ↪15
84*I + 56   -65*I - 12  -53*I - 105   -63*I - 75    76*I + 83    19*I - 78
30*I + 113  -97*I + 123    28*I - 28    89*I + 53     18*I - 9]\n[   58*I␣
 ↪- 77
-16*I + 62    92*I - 65 -105*I - 123   -16*I + 45    53*I + 54   115*I +␣
 ↪88
-56*I + 100   -12*I + 31   -77*I + 60   -64*I + 40  -65*I + 108   81*I -␣
 ↪120
-24*I + 49    75*I - 38    19*I - 70    63*I - 84    -7*I + 89  -126*I +␣
 ↪84
-69*I + 108  -126*I - 65    105*I - 6    17*I - 62   -58*I - 53  -24*I -␣
 ↪100
-26*I + 51  -127*I - 24   -82*I - 36  -83*I + 123  -41*I - 106  -33*I +␣
 ↪104
-6*I + 93    -49*I + 4   -94*I + 57    36*I + 87    -72*I - 2    17*I + 74
-36*I - 90    -7*I + 68    47*I + 90    83*I - 67  -120*I - 47   106*I +␣
 ↪11
-83*I - 67   125*I + 66    73*I - 40   -91*I + 40     4*I - 41   -51*I -␣
 ↪61
23*I + 80   -14*I + 77    3*I - 104   -89*I - 45    22*I + 17    -70*I - 4
87*I - 126     47*I - 7   -85*I - 72    -12*I - 5   103*I - 32   -95*I +␣
 ↪82
-94*I + 86  -31*I - 106   -20*I - 86  -95*I - 127    53*I - 98  -95*I +␣
 ↪114
78*I + 120    79*I + 22    57*I - 81   -99*I + 48  -67*I - 102   -65*I -␣
 ↪78
68*I - 60     91*I - 8   -37*I - 84   -15*I + 98  -112*I + 74   82*I - 113
42*I + 128    -6*I - 22   -19*I - 40  -124*I - 73 -125*I - 127    88*I -␣
 ↪71
103*I + 92    29*I - 86  -76*I + 117  -102*I + 65    10*I + 23   -49*I +␣
 ↪32
108*I + 14    44*I + 49   -28*I - 45      -I - 61   66*I + 121   -22*I +␣
 ↪30
-22*I + 111     8*I - 54   -31*I + 58    34*I + 51   -45*I + 47    74*I +␣
 ↪90
27*I - 56   103*I + 49     65*I + 2   -26*I + 18    81*I + 54   22*I - 112
```

```
29*I - 28   -80*I - 41    54*I - 65   -61*I + 67   -19*I + 83    60*I + 83
-53*I - 18    38*I + 99   -36*I + 93  -109*I - 14 -113*I + 120]'
```

[130]:
```
Cgauss=C.dense_coefficient_list()
```

[132]:
```
Cgaussi=[(k).lift() for k in Cgauss]
```

[134]:
```
Cgaussi1=[real(k) for k in Cgaussi]
```

[136]:
```
Cgaussi2=[imaginary(k) for k in Cgaussi]
```

3.3 Intercalamos los elementos de las listas anteriores

[138]:
```
def intercala_listas(lista1,lista2):
    # Suponemos que lista1 y lista2 son de la misma longitud
    lista = []
    for k in range(len(lista1)):
        lista.append(lista1[k])
        lista.append(lista2[k])
    return lista
```

[139]:
```
cifrado_neg=intercala_listas(Cgaussi1,Cgaussi2)
```

3.4 Escribimos todos los números en representación positiva módulo 256

[143]:
```
cifrado_256_lista=[256+k if k <0 else k for k in cifrado_neg]
```

[145]:
```
cifrado_lista_texto=list(map(chr,cifrado_256_lista))
```

[147]:
```
texto_cifrado= ''.join(cifrado_lista_texto)
```

[148]:
```
texto_cifrado
```

[148]:
```
'Í\x87WN\nå4ËK\x10Øi\x06éê\x91ûÊ\x92>aê\x0bsª\x84î\x18l2Îî\x05êo\x9díæGA\x9aÕ@ÛG
Ê\x92kuäÿˆ.Åøß\x9dW\x08\x86\x1e[Á?£f;¹}°\x1f®þ\x1b¢\x92]¹Jÿç°\x89Æ\x93ˆ;
 ↪û\x0e\x8
dÚ0G\x97\x10\x16&3Õ\x8e±K\x12èB\x1bMˋ+ü»×U\x90\x19Ç5\x06Æ|u²´ä\x0f\x16ü§V)Ëí\x02
C÷\x14u±á\x12Í\r\x17\x1coD\x13}\x8bbî0mð˜\x03Fêì×æw-ö\x14ï\x87¼Ûß\x8fÜg\x9ar
º-\'q\x1e¡dÙÁªïdHUhóˆª\x8dÍsHU\x9f\x94Ã\x07JØ\x9fIÃ\x9e␣
 ↪Ö\x03\x93\x95¦M@ÏJÆt\x0b
\x86\x8a}Â\x0eôµëÊ÷«×\x9a\x96\x9bðaØ\x08\rù[tÖÆ\x14{J\x9a\x08®¦L;
 ↪])x\x94D(ÅíR\x1
```

```
8\x16\x8d˜á\x86ÙÜÊ\x7fíHt=Ñî\x1cp$å^¾Ìfî¶\x0bÕ\\g\x83\x02\x03\x9ew\tq\x06\x9bg×\
x08û\x99\x8f\x00\x12#é½örízYÐGèS\x17\x8fÀ¨\x9aË\x1b*Egé\x1f\x13ª\x1aE|L¸\x18\x91
©©ÎKÚ\x84VEcaÌ\x0eÛßÇ\xa0Ñ\x19¨\\®éà!
 ↪\x1aÝo(\x9033EJSÛ\x10lþ£þs\x82»\x1fÃ\x80O\x
96¯`pÊ®\x90\x1d¾ìm-@\x13JáÉ;Ç(óüV<_\x9fI.
 ↪s4N\x0cÈÌnÛlk=âGêÈkÂyÞ\x7f1$óãö\xa0\x16
\x95Ë\x90W\x85ª\x08«\x1d\x0fß8Tô¿\x97ËµÁSL²\x13q\x1e{\x9fä\x1c5Y÷\x12³:
 ↪>ð¿\\\x85
\x97-ð65XsdÈ\x1fô<³(Àl¿\x88Q1èÚKº\x13¬?
 ↪YùT\x82l»¿\x82úiÂ\x11ËÆ\x9cè3æè\x81Ü®{\xa
d\x96×hß]ú\x04Ï9¢W$þ¸J\x11¦ÜDùZ/
 ↪½SÑ\x88\x0bj½\xadB}ØI(¥×\x04ÃÍP\x17Mò\x98\x03Ő§\
x11\x16üº\x82Wù/
 ↪¸«ûôàgR¡V¢\x96áªì\x81¡\x9e5r¡xN\x16O¯90\x9d\x9a½²¿ÄDø[¬ÛbñJ\x90\
x8fR\x80*êúØí·\x84\x81\x83¹X\\gª\x1du´A\x9a\x17\n␣
 ↪Ï\x0el1,ÓäÃÿyB\x1eêoêÊ\x08:á3"
/ŰZJÈ\x1b1g\x02A\x12æ6Q\x90\x16ä\x1d×°¿6CÃSíS<îËc&]Üò\x93x\x8f'
```

[149]:
```
def cifradoi_Hill(matriz,mensaje_texto):
    lista_mensaje_texto=list(mensaje_texto)
    lista_mensaje_numeros=list(map(ord,lista_mensaje_texto))
  ␣
 ↪lista_mensaje_numeros_i=[mensaje3g(lista_mensaje_numeros)[2*k]+i*mensaje3g(lista_mens
 ↪for k in range(len(mensaje3g(lista_mensaje_numeros))/2)]
    matriz_plano=matrix(Gn,3,len(mensaje3g(lista_mensaje_numeros_i))/
 ↪3,mensaje3g(lista_mensaje_numeros_i))
    C=matriz*matriz_plano
    Cgauss=C.dense_coefficient_list()
    Cgaussi=[(k).lift() for k in Cgauss]
    Cgaussi1=[real(k) for k in Cgaussi]
    Cgaussi2=[imaginary(k) for k in Cgaussi]
    cifrado_neg=intercala_listas(Cgaussi1,Cgaussi2)
    cifrado_256_lista=[256+k if k <0 else k for k in cifrado_neg]
    cifrado_lista_texto=list(map(chr,cifrado_256_lista))
    texto_cifrado= ''.join(cifrado_lista_texto)
    return texto_cifrado
```

[150]:
```
cifradoi_Hill(M,mensaje_texto)
```

[150]:
```
'Í\x87WN\nå4ËK\x10Øi\x06éê\x91ûÊ\x92>aê\x0bsª\x84î\x18l2Îî\x05êo\x9díæGA\x9aÕ@ÛG
Ê\x92kuäÿ^.Åøß\x9dW\x08\x86\x1e[Á?£f;¹}°\x1f®þ\x1b¢\x92]¹Jÿç°\x89Æ\x93^;
 ↪û\x0e\x8
dÚ0G\x97\x10\x16&3Õ\x8e±K\x12èB\x1bMˋ+ü»×U\x90\x19Ç5\x06Æ|u²´ä\x0f\x16ü§V)Ëí\x02
```

```
C÷\x14u±á\x12Í\r\x17\x1coD\x13}\x8bbî0mð˜\x03Fêì×æw-ö\x14ï\x87¼Ûß\x8fÜg\x9ar
º-\'q\x1e¡dÙÁªïdHUhó^ª\x8dÍsHU\x9f\x94Ã\x07JØ\x9fIÃ\x9e␣
 ↪Ö\x03\x93\x95¦M@ÏJÆt\x0b
\x86\x8a}Â\x0eôµëÊ÷«×\x9a\x96\x9bðaØ\x08\rù[tÖÆ\x14{J\x9a\x08®¦L;
 ↪])x\x94D(ÅíR\x1
8\x16\x8d˜á\x86ÙÜÊ\x7fíHt=Ñî\x1cp$å^¾Ìfî¶\x0bÕ\\g\x83\x02\x03\x9ew\tq\x06\x9bg×\
x08û\x99\x8f\x00\x12#é½örízYÐGèS\x17\x8fÀ¨\x9aË\x1b*Egé\x1f\x13ª\x1aE|L¸\x18\x91
©©ÎKÚ\x84VEcaÌ\x0eÔßÇ\xaOÑ\x19¨\\®éà!
 ↪\x1aÝo(\x9033EJSÛ\x10lþ£þs\x82»\x1fÃ\x80O\x
96¯`pÊ®\x90\x1d¾ìm-@\x13JáÉ;Ç(óüV<_\x9fI.
 ↪s4N\x0cÈÌnÛlk=âGêÈkÂyÞ\x7f1$óãö\xa0\x16
\x95Ë\x90W\x85ª\x08«\x1d\x0fß8Tô¿\x97ËµÁSL²\x13q\x1e{\x9fä\x1c5Y÷\x12³:
 ↪>ð¿\\\x85
\x97-ð65XsdÈ\x1fô<³(Àl¿\x88Q1èÚKº\x13¬?
 ↪YùT\x82l»¿\x82úiÂ\x11ËÆ\x9cè3æè\x81Ü®{\xa
d\x96×hß]ú\x04Ï9¢W$þ¸J\x11¦ÜDùZ/
 ↪½SÑ\x88\x0bj½\xadB}ØI(¥×\x04ÃÍP\x17Mò\x98\x03Ú§\
x11\x16üº\x82Wù/
 ↪¸«ûôàgR¡V¢\x96áªì\x81¡\x9e5r¡xN\x16O¯90\x9d\x9a½²¿ÄDø[¬ÛbñJ\x90\
x8fR\x80*êúØí·\x84\x81\x83¹X\\gª\x1du´A\x9a\x17\n␣
 ↪Ï\x0el1,ÚäÃÿyB\x1eêoêÊ\x08:á3"
/ÚZJÈ\x1b1g\x02A\x12æ6Q\x90\x16ä\x1d×°¿6CÃSíS<îËc&]Üò\x93x\x8f'
```

[151]:
```
texto_cifrado=cifradoi_Hill(M,mensaje_texto)
```

4 Proceso de descifrado

[152]:
```
def descifradoi_Hill(matriz,texto_cifrado):
    lista_mensaje_cifrado=list(texto_cifrado)
    lista_mensaje_cifrado_numeros=list(map(ord,lista_mensaje_cifrado))
   ␣
 ↪lista_mensaje_cifrado_numeros_i=[mensaje3g(lista_mensaje_cifrado_numeros)[2*k]+i*mens
 ↪for k in range(len(mensaje3g(lista_mensaje_cifrado_numeros))/2)]
    matriz_cifrado=matrix(Gn,3,len(lista_mensaje_cifrado_numeros_i)/
 ↪3,lista_mensaje_cifrado_numeros_i)
    MO=matriz^(-1)*matriz_cifrado
    MOgauss=MO.dense_coefficient_list()
    MOgaussi=[(k).lift() for k in MOgauss]
    MOgaussi1=[real(k) for k in MOgaussi]
    MOgaussi2=[imaginary(k) for k in MOgaussi]
    descifrado_neg=intercala_listas(MOgaussi1,MOgaussi2)
    descifrado_256_lista=[256+k if k <0 else k for k in descifrado_neg]
```

```
    descifrado_lista_texto=list(map(chr,descifrado_256_lista))
    texto_original= ''.join(descifrado_lista_texto)
    return texto_original
```

[153]:
```
descifradoi_Hill(M,texto_cifrado)
```

[153]:
```
'El proyecto STEMbach de Criptografía: El Cifrado de Hill, realizado por
alumnado del IES Eduardo Blanco Amor de Ourense Diego González, Lucía␣
 ↪Hermosilla
y Brais López, tutorizados por los profesores Manuel Ladra, del␣
 ↪Departamento de
Álgebra de la Universidad de Santiago de Compostela y Carlos Ferreiro del
Departamento de Matemáticas del IES Blanco Amor. El proyecto STEMbach␣
 ↪permite al
alumnado de bachillerato entrar en contacto con la labor investigadora, a␣
 ↪través
de su participación en proyectos de investigación científica y␣
 ↪tecnológicos
diseñados y dirigidos por profesorado universitario de la USC. Este␣
 ↪proyecto de
Criptografía será presentado el 28 de abril del año 2021 ante la comisión
evaluadoraEDUARE\x00D\x00U\x00'
```