**Presentado por:**

**Juan Pablo Girón Bastidas - 1004695646**

**Yesid Alberto Ochoa Luque - 1014252907**

**Definición del problema**

El problema con el que se trata es el cifrado de una clave o secreto en un entorno donde no hay confianza mutua entre las personas que tienen las llaves necesarias para acceder a la información secreta. Es frecuente ver esta clase de problemas, donde los interesados en guardar ciertos datos, desconfían de que sus semejantes puedan acceder a estos sin su presencia.

Una solución a un problema así puede volverse fácilmente impráctica, necesitando un cantidad de “candados” y “llaves” que crece de manera exponencial a medida que aumenta la cantidad de personas interesadas en la información.

Consideremos, por ejemplo, una empresa que firma digitalmente todos sus cheques. Si a cada ejecutivo se le entrega una copia de la clave de la firma de la compañía, el sistema es conveniente pero fácil de usar mal. Por otro lado, si es necesaria la cooperación de todos los ejecutivos de la empresa para poder firmar cada cheque, el sistema es seguro pero inconveniente.

Por esta razón lo que se quiere es un sistema en el que la clave pueda ser accedida si se tiene un número lo suficientemente grande de personas que quieran acceder a ella, pero que, sin embargo, esta se bloquee si existe una cantidad considerable de personas que no quieren que se acceda a la clave.

Una vez se tiene una clave o secreto guardado de forma segura, lo que se busca es cifrar información con esta clave mediante algún algoritmo. En este caso se quiere encriptar imágenes, de manera que sea necesaria la cooperación de un grupo de personas tanto para cifrar una imagen como para descifrarla. Para resolver esto, usamos el *Secreto de Shamir* para guardar la clave y *El Algoritmo de Hill* para cifrar la imágen.

**Modelo Matemático y Solución Numérica**

Se tiene una clave que se quiere esconder. lo que se hará es dividir en múltiples piezas . Para poder reconstruir dicha clave son necesarias piezas de información como mínimo. Si se tienen piezas, será sencillo computar , sin embargo, con piezas, no es posible[1].

La combinación de y que se suele utilizar por sus bueno resultados es una en la que se cumple que , de aquí podemos concluir que la cantidad de personas necesarias para descifrar el secreto es la mitad como mínimo, lo cual propicia un sistema de administración de claves robusto.

Nuestro esquema se basa en la interpolación polinomial: dados puntos en el plano bidimensional con distintas , hay un y solo un polinomio de grado tal que para todos los . Sin pérdida de generalidad, podemos asumir que el secreto es (o puede hacerse) un número. Para dividirlo en pedazos , elegimos un polinomio al azar de grado en el que , y evaluamos:

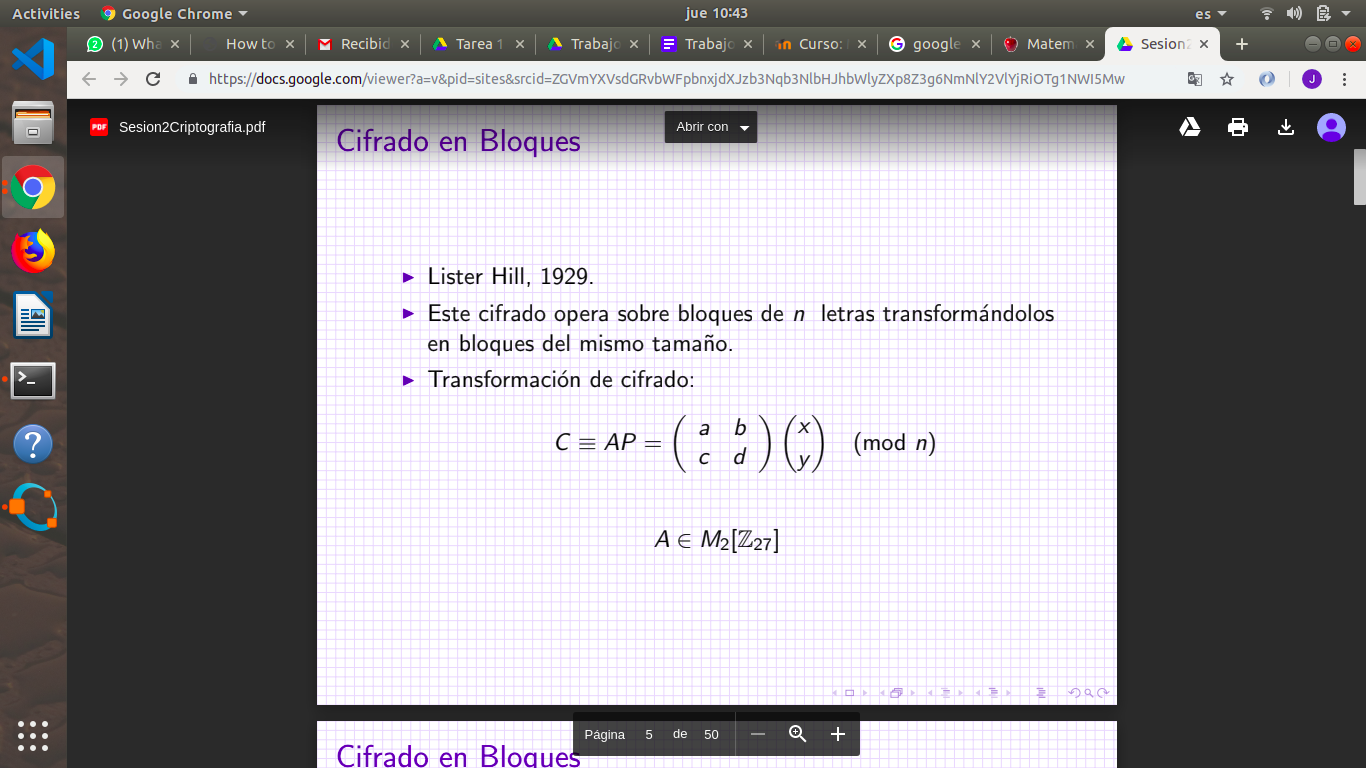
Dado cualquier subconjunto de de estos valores (junto con sus índices de identificación ), podemos encontrar los coeficientes de por interpolación, y luego evaluar . El conocimiento de solo k-1 de estos valores, por otra parte, no es suficiente para calcular D.

Para hacer más preciso el procedimiento, utilizamos aritmética modular en lugar de aritmética real. El conjunto de enteros, módulo a número primo forma un campo en el que es posible la interpolación. Dado un valor entero (el secreto) , escogemos un primo que sea más grande que y . Los coeficientes en se seleccionan al azar, de una distribución uniforme sobre los enteros en , y los valores se calculan módulo . Para la interpolación de puntos utilizamos el método del polinomio interpolador de Lagrange.

Supongamos ahora que de estas piezas son reveladas a un oponente. Para cada valor candidato en se puede construir un y solo un polinomio q '(x) de grado k-1 tal que y para los dados argumentos. Por construcción, estos posibles polinomios son igualmente probables, y por lo tanto no hay absolutamente nada de lo que el oponente pueda deducir sobre el valor real de.

Ahora, se quiere usar esa clave o secreto en el algoritmo de Hill, usado en este caso para cifrar imágenes. Este cifrado opera sobre bloques de n letras transformándolos en bloques del mismo tamaño.

La transformación usada es la siguiente:



*Transformación del Cifrado de Hill. [2]*

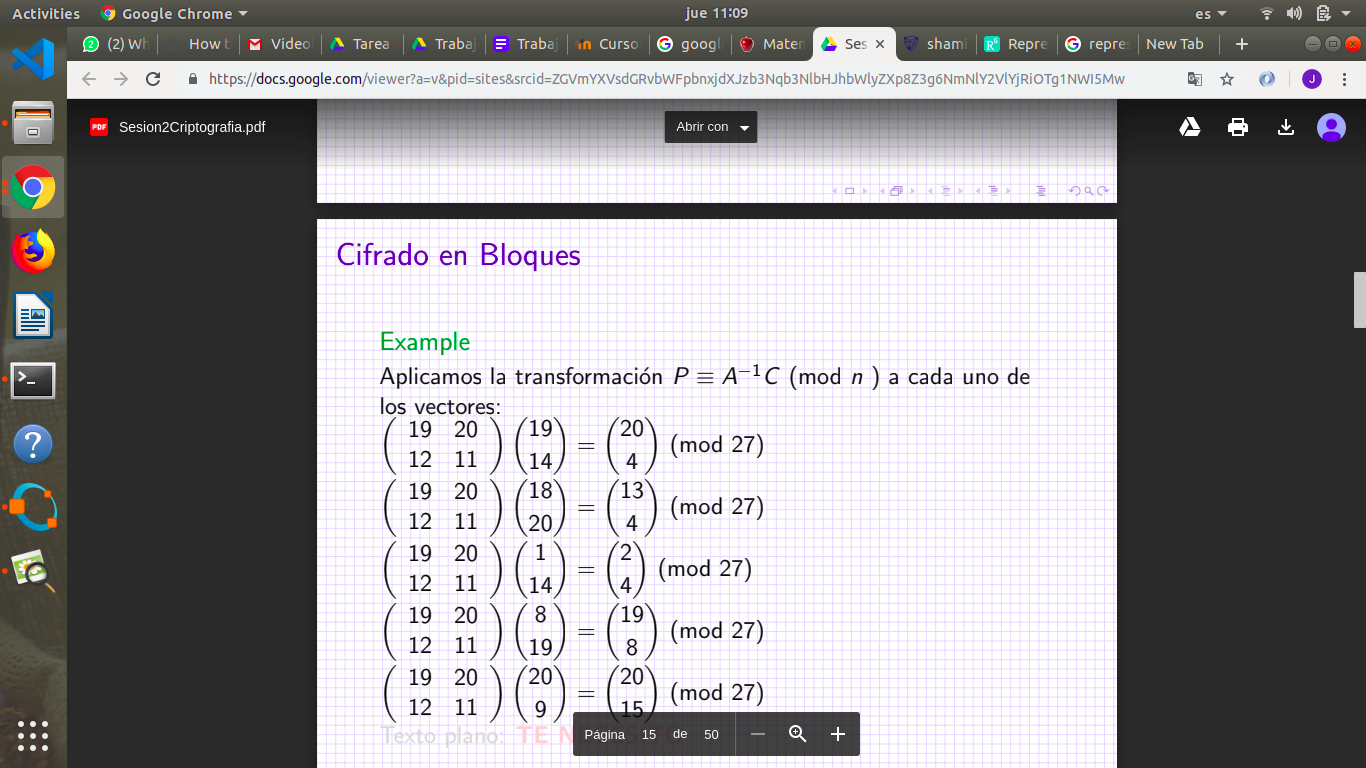
donde P es la entrada: Plano y C es la salida: Cifrado.

Como se puede observar, este algoritmo opera sobre bloques de vectores de y utiliza como clave una matriz de , por defecto se usa con números que van del al , sin embargo, el conjunto de números se puede ampliar, para aceptar la representación numérica del color de un pixel, el cual es un tripla , donde cada uno de los elementos puede ir del al .

La transformación es en sí una congruencia lineal con matrices, la cual es módulo; un número cualquiera entre y .

La transformación funciona si y sólo si la matriz es invertible módulo, y esta es invertible si y sólo si su determinante es invertible en .

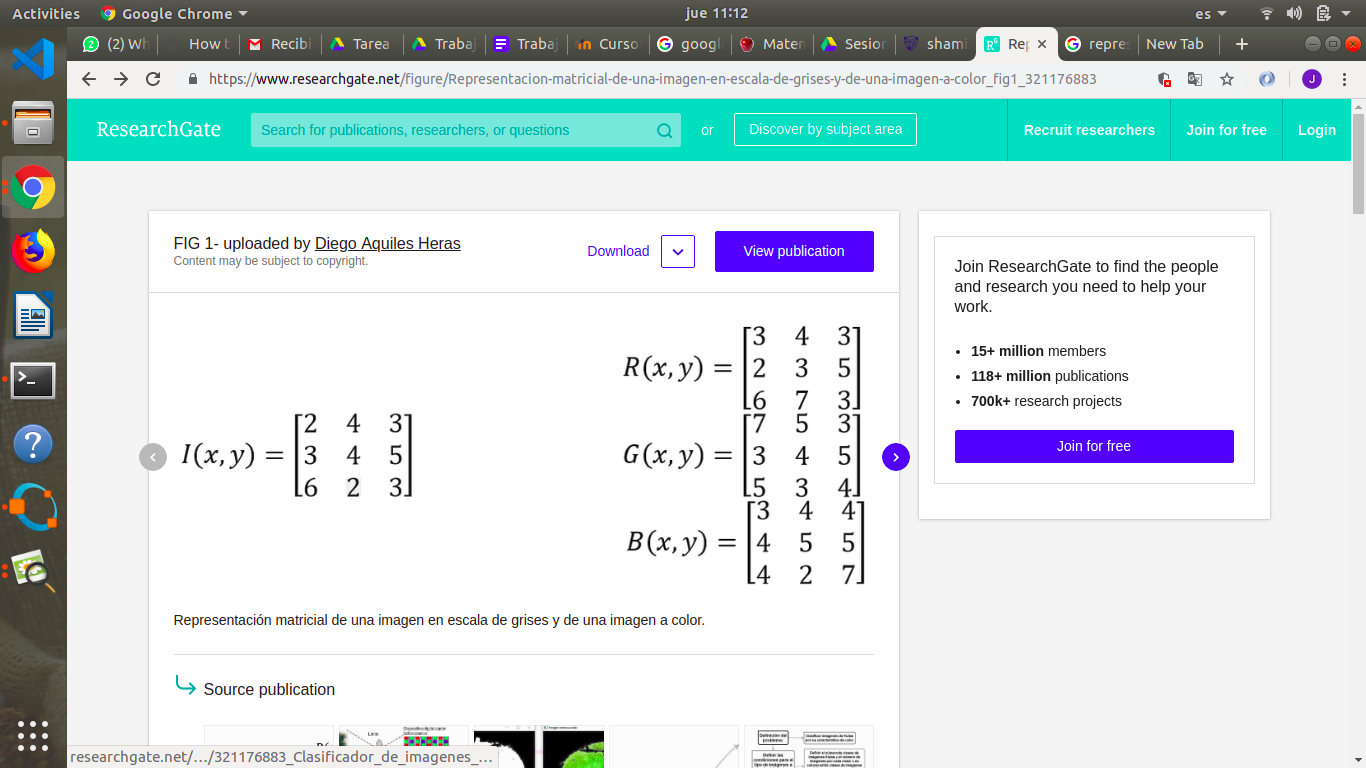
Para descifrar la información cifrada se usa la transformación inversa:



*Transformación del Cifrado de Hill. [2]*

donde es la inversa de módulo .

Finalmente, para la representación matricial de la imágen, se utilizan las triplas para cada píxel. A manera de ejemplo se tiene:



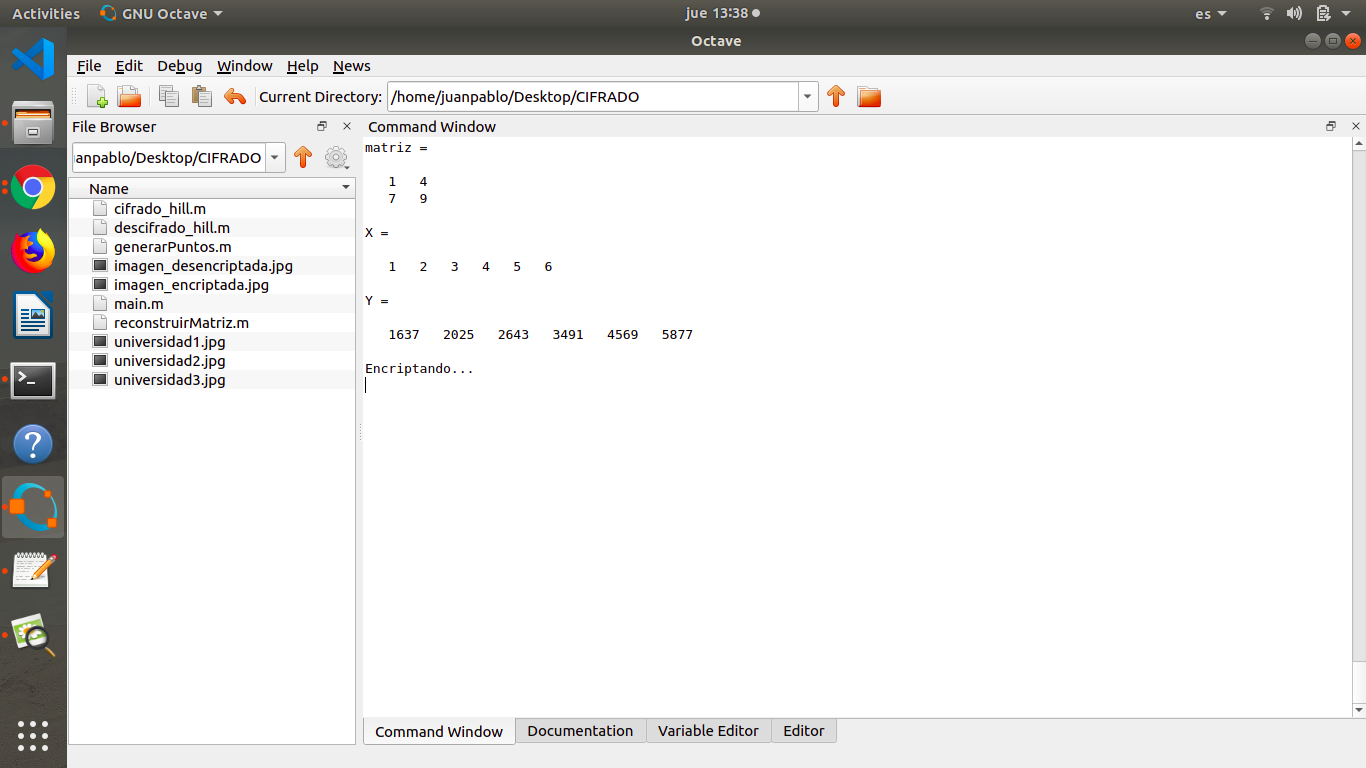
Representación matricial de un imágen. [3]

Esta representación utiliza una matriz tridimensional: las primeras dos dimensiones para representar las coordenadas del píxel, y la otra para obtener el color en una tripla , la cual se puede ver como tres capas de una matriz .

**Análisis de Resultados**

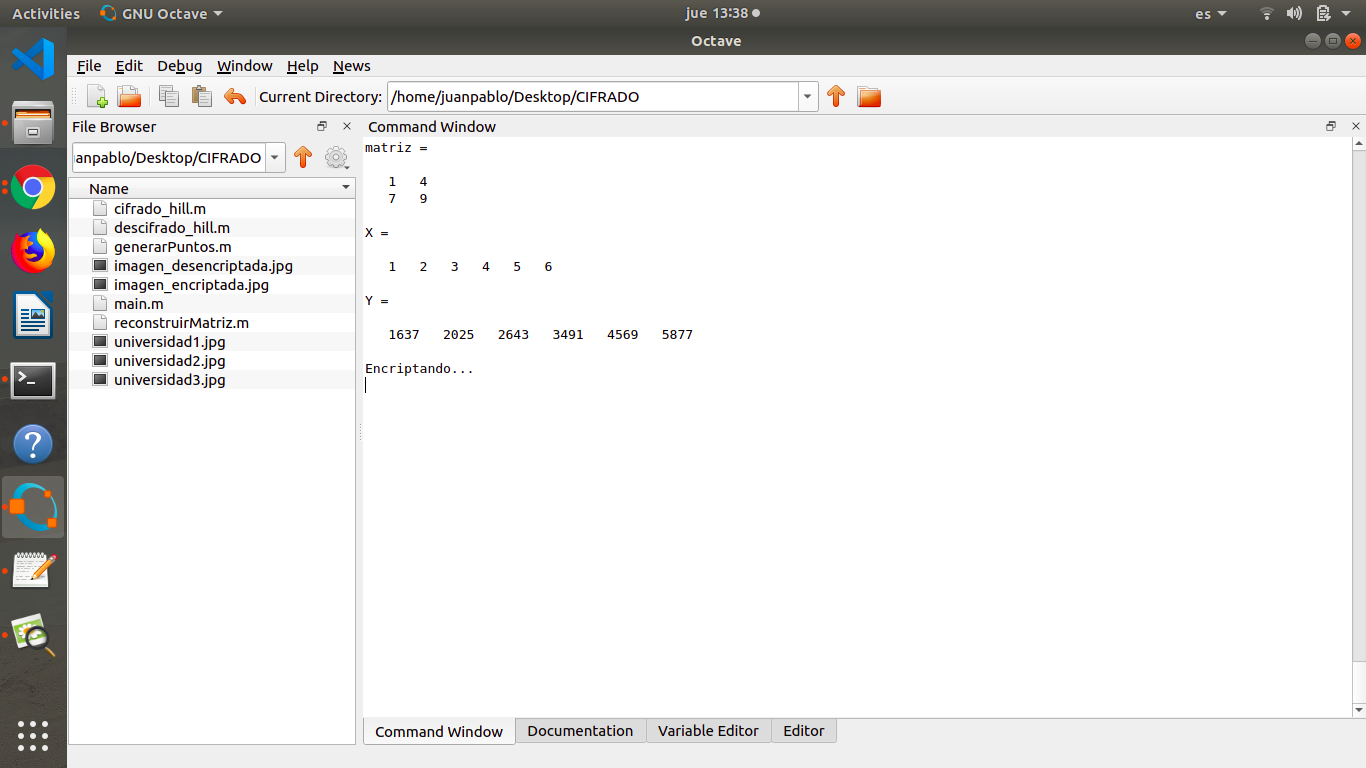
**ejemplo 1**

Para probar el algoritmo usamos la matriz de cifrado siguiente:



*matriz de cifrado.*

La cual cumple con las características dadas en el modelo matemático. Esta matriz es nuestra clave o secreto, por lo que tendremos que usar el algoritmo de Shamir descrito anteriormente para generar los fragmentos de clave.



*fragmentos de clave generados.*

Esto significa que a la persona 1 le tocó el fragmento 1637, a la persona 2 el 2025, y así sucesivamente.

Una vez generados los fragmentos de claves, usamos el algoritmo de Shamir para reconstruir el polinomio con el método de Lagrange. Con el polinomio obtenemos de vuelta nuestra matriz original que podemos usar para aplicar el cifrado de Hill.

La primera imágen que se encriptará será esta:



*Imagen tomada de:* [*https://www.minuto30.com/continua-paro-de-trabajadores-en-universidad-nacional/134620/*](https://www.minuto30.com/continua-paro-de-trabajadores-en-universidad-nacional/134620/)

cuya forma encriptada es la siguiente:

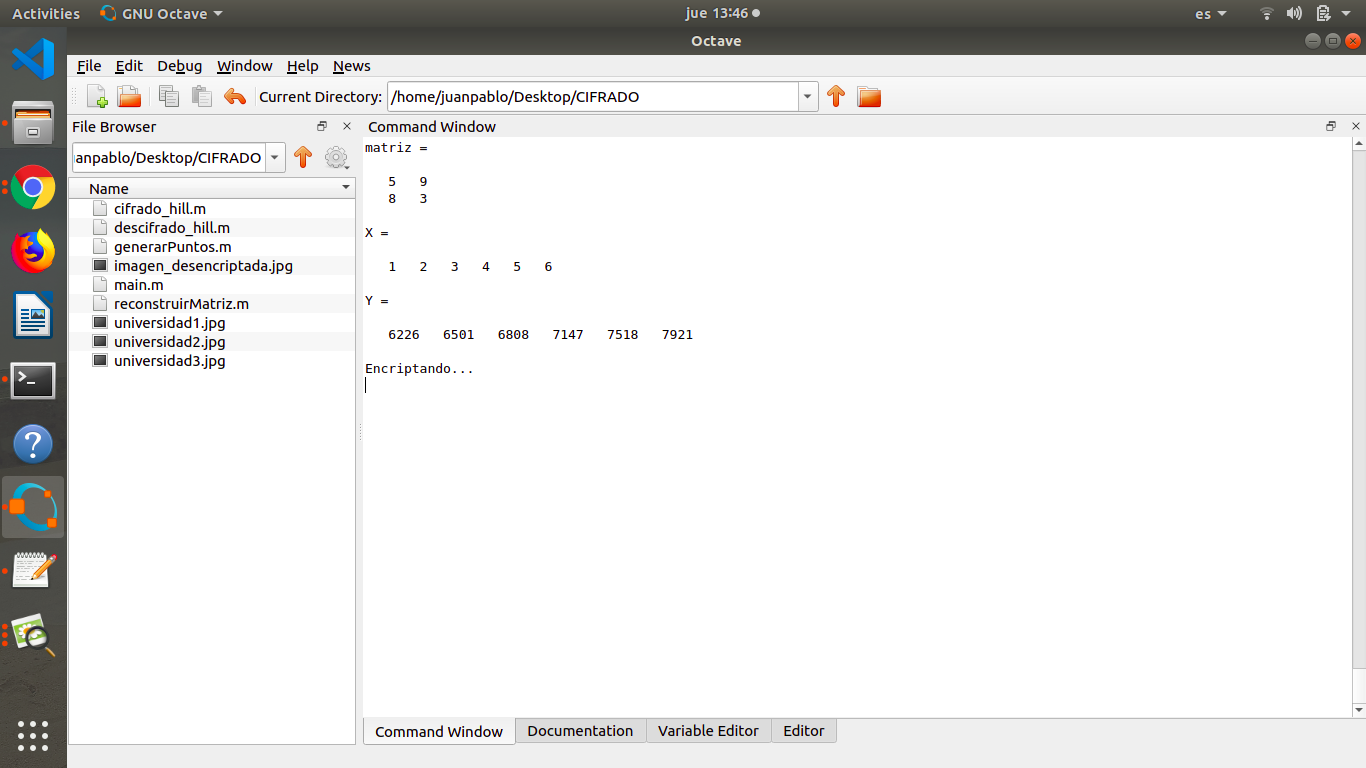


*imagen encriptada.*

con ayuda de la matriz inversa a la de encriptación, podemos obtener de vuelta la imágen.

**ejemplo 2**

Ahora cambiamos ligeramente la matriz:



*matriz de cifrado.*

Con la que obtenemos los siguientes fragmentos:

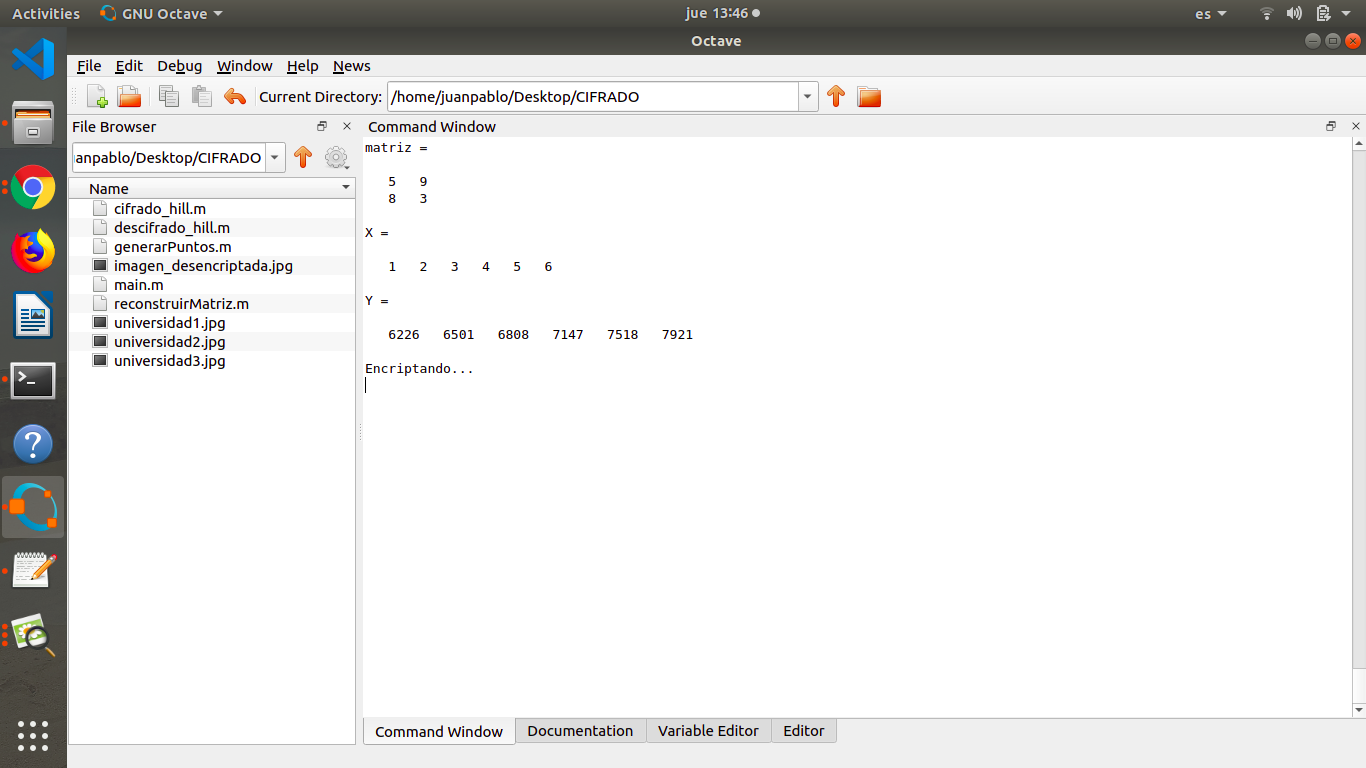
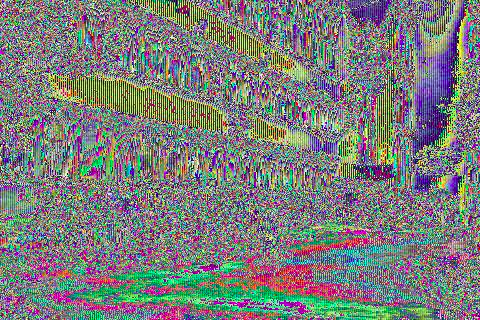


Imagen para encriptar:



*Imagen tomada de:* [*https://www.minuto30.com/continua-paro-de-trabajadores-en-universidad-nacional/134620/*](https://www.minuto30.com/continua-paro-de-trabajadores-en-universidad-nacional/134620/)

Obtenemos el siguiente resultado:



*Imagen encriptada.*

Como se puede observar, obtenemos un resultado ligeramente mejor, puesto que los contornos ahora se notan menos, esto debido a que los elementos de la matriz son ligeramente mayores.

**ejemplo 3**

Ahora, siguiendo con la misma matriz del ejemplo 2, procedemos a encriptar una imagen como la siguiente:



*Imagen tomada de:* [*https://blog.ipler.com/pre-unal-tips-para-examen-adminision-universidad-nacional*](https://blog.ipler.com/pre-unal-tips-para-examen-adminision-universidad-nacional)

Obtenemos la siguiente imagen encriptada:



*imagen encriptada.*

**Referencias**

* [1] Shamir, A (1979). *How to Share a Secret.* Tomado de: <https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf>
* [2] Ramírez, J (2018). *Sistemas Criptográficos Clásicos.* Tomado de: <https://sites.google.com/site/cursosjoselramirez/home/discretasii>
* [3] ResearchGate (2017). *Representación matricial de una imagen en escala de grises y de una imagen a color.* Recuperado de: <https://www.researchgate.net/figure/Representacion-matricial-de-una-imagen-en-escala-de-grises-y-de-una-imagen-a-color_fig1_321176883>