Alumno: Rodrigo Vila

# Modulo 1 Unidad 3

## Introducción a la Criptografía

### Ejercicio Número 1 Unidad 1:

Seleccionar un solo ejercicio para exponer en el foro:

1- Buscar en Internet información sobre el “birthday problem” y exponer que piensan del mismo, aplicándolo en otros ejemplos.

2- Escribir 3 frases de no más de 10 palabras y pasarlas por los mecanismos de algoritmos, postearlo en el foro (al final de la unidad, links de ayuda)

3- ¿Te animas a inventar un tipo de cifrado? (en caso de afirmativo, exponer con ejemplos, pero siempre recordar que es importante demostrar el reverso para saber que descifrar correctamente.

**Ejercicio seleccionado:** Inventar un tipo de cifrado.

Voy a realizar un cifrado por sustitución polialfabética, similar en concepto al cifrado Vigenère pero con un giro diferente para añadir complejidad.

### Que es el cifrado Vigenère?:

El cifrado de Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado por sustitución simple polialfabético.

Fuente: https://es.wikipedia.org/wiki/Cifrado_de_Vigen%C3%A8re

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

Esta tabla contiene un alfabeto de letras en la parte superior y lateral. Cada fila del cuadro corresponde a una posible clave de cifrado, y cada columna corresponde a una letra del alfabeto plano del mensaje.

## Descripción del Cuadro de Vigenère:

Filas y Columnas:

Las columnas están numeradas del 0 al 26 en la parte superior.

Las filas están etiquetadas con letras del alfabeto desde “A” hasta “Z”. Este incluye la “Ñ”, otras versiones no la incluyen.

## Cifrado:

- Para cifrar un mensaje, se necesita una palabra clave.
- Cada letra de la palabra clave determina una fila en el cuadro.
- Para cada letra del texto original (en claro), se busca la columna correspondiente.
- La intersección de la fila (determinada por la letra de la clave) y la columna (determinada por la letra del texto original) proporciona la letra cifrada.

## Ejemplo de Uso:

Supongamos que queremos cifrar el mensaje "HOLA" usando la clave "KEY":

Mensaje: HOLA

Clave: KEYK (la clave se repite para que coincida con la longitud del mensaje)

## Ahora ciframos cada letra del mensaje usando la tabla:

La primera letra del mensaje es “H” y la primera letra de la clave es “K”:

Fila “K”, columna “H”: “Q”.

La segunda letra del mensaje es “O” y la segunda letra de la clave es “E”:

Fila “E”, columna “O”: “S”.

La tercera letra del mensaje es “L” y la tercera letra de la clave es “Y”:

Fila “Y”, columna “L”: “J”.

La cuarta letra del mensaje es “A” y la cuarta letra de la clave es “K”:

Fila “K”, columna “A”: “K”.

Por lo tanto, el mensaje cifrado queda: " QSJK".

# MENSAJE

CLAVE

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

## Nuevo Cifrado: Cifrado Polialfabético con Desplazamiento Alternado

Similar al método del cuadro Vigenère pero con una característica adicional: un desplazamiento alternado. En este esquema, cada letra del texto se desplazará no solo según la clave, sino también se le aplicará un desplazamiento adicional alternado (-1 para posiciones impares, +1 para posiciones pares) en cada carácter.

**Método**: Sustitución

**Mensaje a cifrar:** HOLA

**Clave:** KEYK

## Pasos del Cifrado:

1. Convertir cada letra del texto y la clave a su posición numérica en el alfabeto. (La “A” es “0”, la “Z” es “26”).
2. Sumar la posición de la letra del texto y el desplazamiento de la clave.
3. Aplicar el desplazamiento alternado:
    - Si la posición del carácter es impar (1, 3, 5, ...), restar 1.
    - Si la posición del carácter es par (2, 4, 6, ...), sumar 1.
4. Ajustar el resultado para mantenerse dentro del rango de 27 letras (0-26).
5. Convertir el número resultante de vuelta a una letra.

## Numeración de cada letra:

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

## Numeración correspondiente de la Clave "KEYK":

K = 10, E = 4, Y = 25, K= 10.

## Cifrado con Desplazamiento Alternado:

Vamos a cifrar la palabra "HOLA" paso a paso. El desplazamiento de la clave se va a ir repitiendo, como “HOLA” tiene 4 letras, la clave “KEY” quedaría “KEYK”, ósea la numeración de los desplazamientos va a ser: 10, 4, 25, 10.

Primera letra: H

H = 7 (Número para la H en el alfabeto)

7 + 10 = 17 (Le sumamos 10 que es el número correspondiente para “K”)

17 - 1 = 16 (Desplazamiento alternado: como es impar le restamos 1). (Al ser el 1er digito de la clave, es impar, por eso restamos. El 2do digito de la clave va a ser par y por eso sumamos y así sucesivamente).

Letra cifrada: “P” (16 en el alfabeto)

Segunda letra: O

O = 15

15 + 4 = 19

19 + 1 = 20 (Desplazamiento alternado: como es par le sumamos 1)

Letra cifrada: “T”

Tercera letra: L

L = 11

11 + 25 = 36

36 - 1 = 35 (Desplazamiento alternado: como es impar le restamos 1)

Ajustar a rango 27: 35 mod 27 = 8

Letra cifrada: “I” (8 en el alfabeto)

Cuarta letra: A

A = 0

0 + 10 = 10

10 + 1 = 11 (Desplazamiento alternado: como es par le sumamos 1)

Letra cifrada: “L”

Mensaje cifrado

Juntando todas las letras cifradas obtenemos el mensaje cifrado final:

HOLA se convierte en PTIL.

Por lo tanto, el mensaje "HOLA" cifrado con la clave "KEYK" utilizando el cifrado polialfabético con desplazamiento alternado es PTIL.

**Proceso inverso: Descifrado**

Ahora, para descifrar, hay que seguir los pasos inversos del cifrado:

1. Convertir cada letra del mensaje cifrado y la clave a su posición numérica en el alfabeto.
2. Aplicar el desplazamiento alternado inverso:
3. Si la posición del carácter es impar (1, 3, 5, ...), sumar 1.
4. Si la posición del carácter es par (2, 4, 6, ...), restar 1.
5. Restar la posición de la clave de la posición ajustada del carácter cifrado.
6. Ajustar el resultado para mantenerse dentro del rango de 27 letras (0-26).
7. Convertir el número resultante de vuelta a una letra.

Vamos a aplicar estos pasos para descifrar el mensaje PTIL usando la clave KEYK.

**Numeración de cada letra:**

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

**Numeración correspondiente de la Clave "KEYK":**

K = 10, E = 4, Y = 25, K= 10.

Primera letra: P

P = 16 (Número para la P en el alfabeto)

Aplicar el desplazamiento alternado inverso: 16 + 1 = 17 (Como es la primera letra, es impar, le sumamos 1)

Restar el valor de la clave: 17 - 10 = 7 (Restamos 10 que es el número correspondiente a “K”)

Letra descifrada: H

Segunda letra: T

T = 20

Aplicar el desplazamiento alternado inverso: 20 - 1 = 19 (Como es la segunda letra, es par, le restamos 1)

Restar el valor de la clave: 19 - 4 = 15

Letra descifrada: O

Tercera letra: I

I = 8

Aplicar el desplazamiento alternado inverso: 8 + 1 = 9 (Como es la tercera letra, es impar, le sumamos 1)

Restar el valor de la clave: 9 - 25 = -16

Ajustar a rango 27: (-16 + 27) = 11

Letra descifrada: L

Cuarta letra: L

L = 11

Aplicar el desplazamiento alternado inverso: 11 - 1 = 10 (Como es la cuarta letra, es par, le restamos 1)

Restar el valor de la clave: 10 - 10 = 0

Letra descifrada: A

Mensaje descifrado

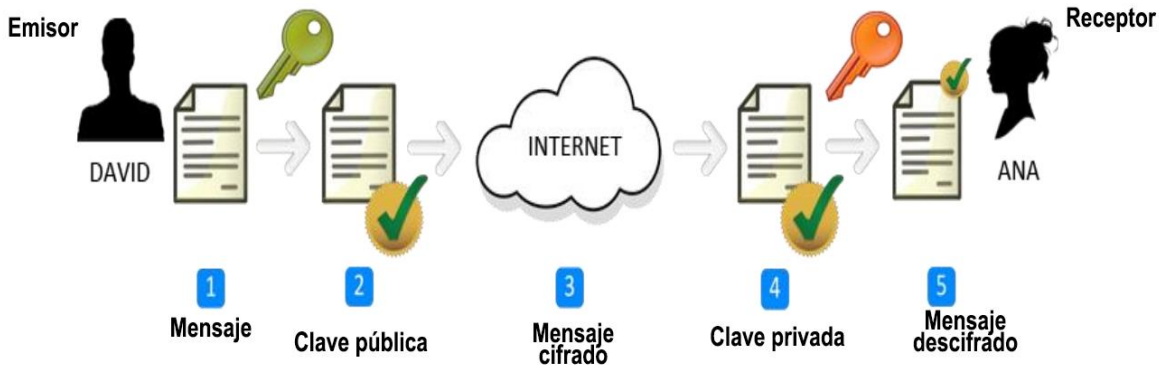
Juntando todas las letras descifradas obtenemos el mensaje descifrado final:

PTIL se convierte en HOLA.

Por lo tanto, el mensaje "PTIL" descifrado con la clave "KEYK" utilizando el cifrado polialfabético con desplazamiento alternado es HOLA.

## Ejercicio Número 2 Unidad 1:

¿Te animas a completar el siguiente ejemplo y subirlo al foro?:

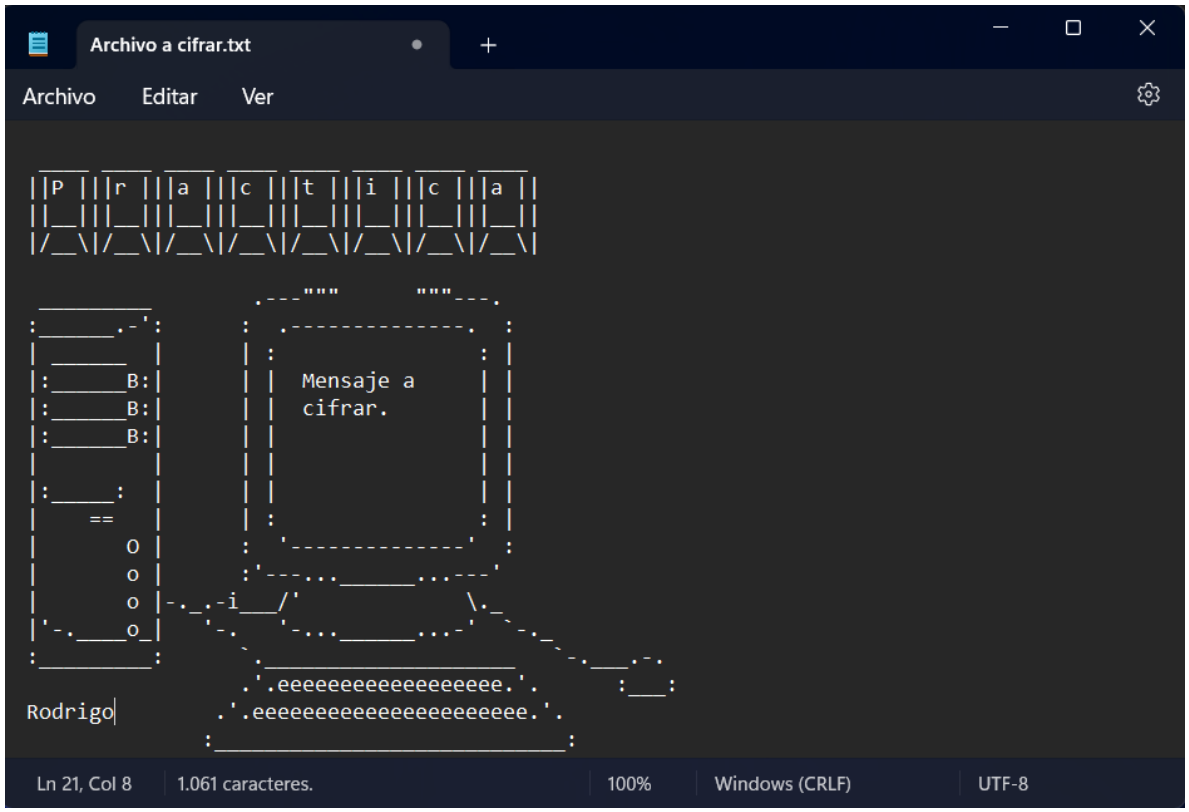



## Ejercicio Tools – LABS:

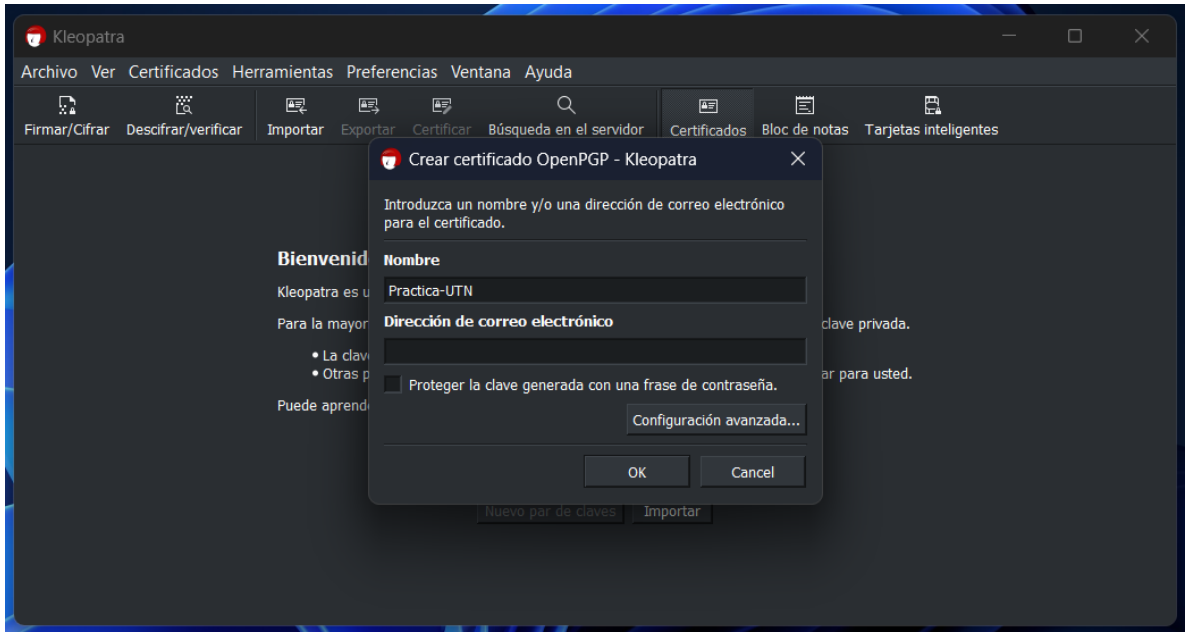
Mediante una máquina virtual, hacer uso de estas 2 herramientas, cifrando un directorio personal y realizando un cifrado de un archivo. (VeraCrypt y Gpg4win).

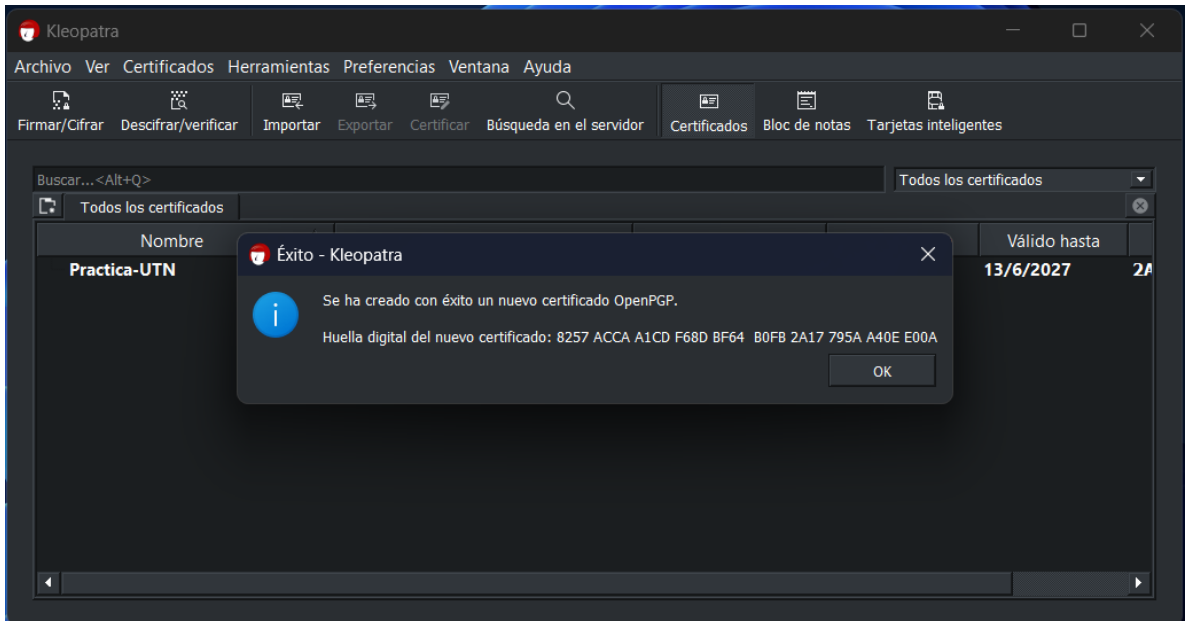
## Cifrando un archivo con Gpg4win:

Creando archivo a cifrar:

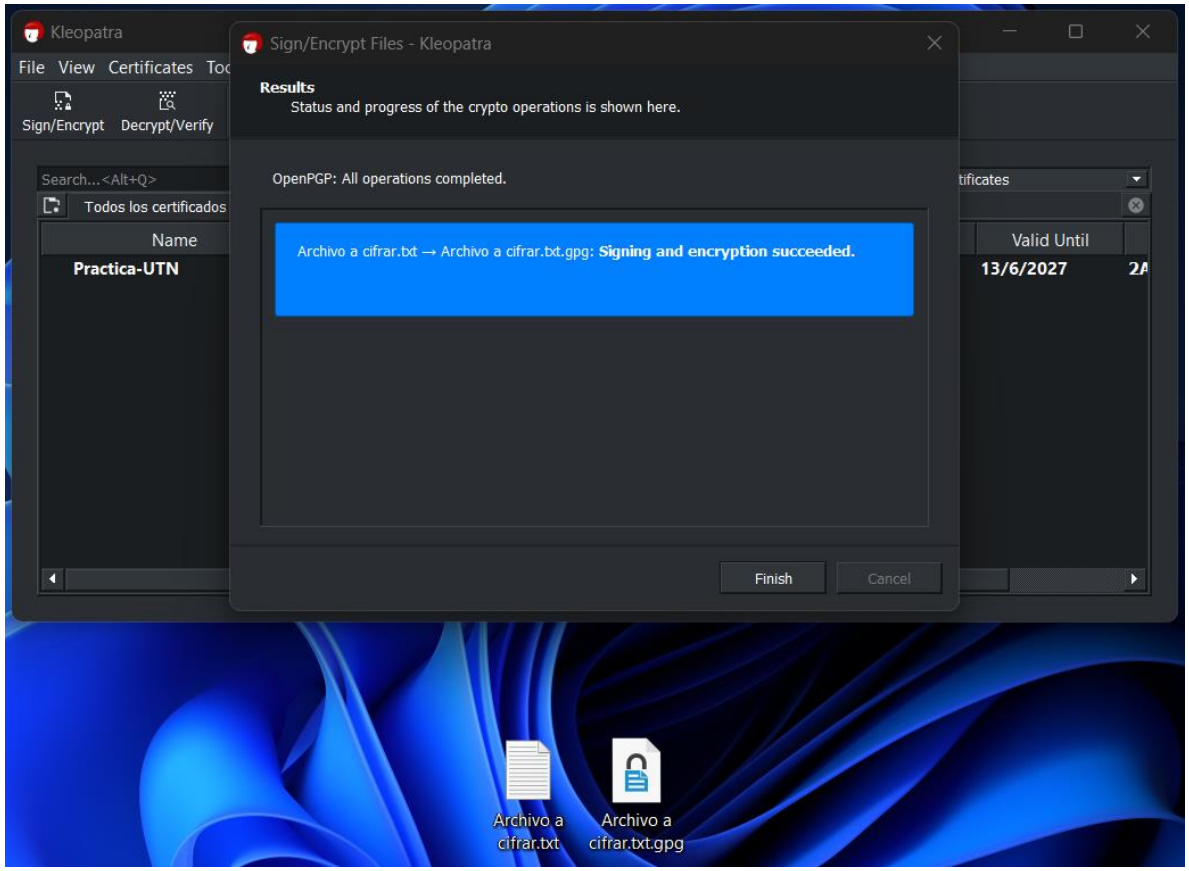



Creando clave:

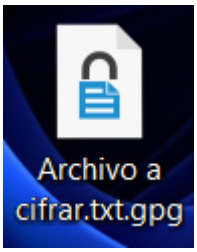




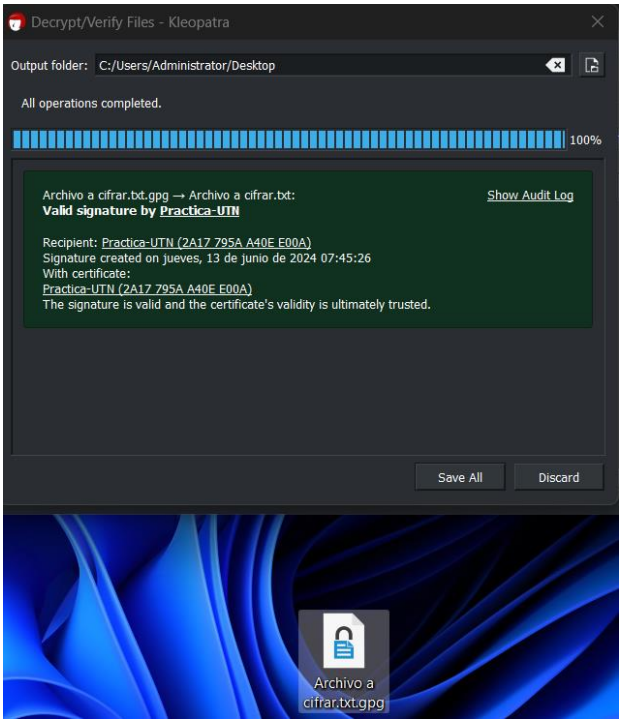

Archivo cifrado:



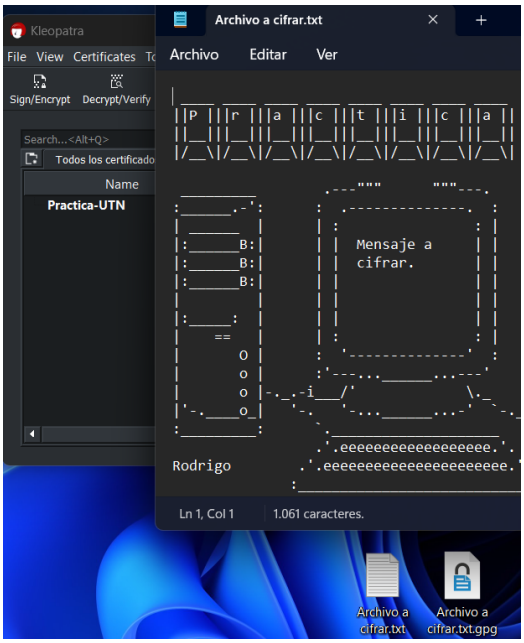
Podemos eliminar el archivo original y quedarnos solo con el cifrado:




Luego le damos doble click al archivo para desencriptarlo o lo seleccionamos desde Kleopatra para desencriptarlo.




Listo, ya tenemos nuestro archivo desencriptado:




***Rodrigo Vila.-***