ACTIVIDAD EVALUATIVA EJE 1

Laura Juliana Ramírez Barrera

Fundación Universitaria del Área Andina

Ingeniería De Sistemas – Virtual

[[CRIPTOGRAFIA I - 202560 - 6A - 61](https://areandina.instructure.com/courses/64205)](https://areandina.instructure.com/courses/51454)

Johnn Eduar Criollo Salamanca

18 de agosto de 2025

INTRODUCCIÓN

La criptografía es el conjunto de métodos utilizados para transformar un mensaje claro en otro ininteligible, denominado criptograma, con el fin de resguardar la confidencialidad de la información. En este trabajo se hablara sobre el método históricos de cifrado, la **Escítala**, un sistema de transposición utilizado por los espartanos en la antigua Grecia, y la maquina de cifrado, la **Máquina Bombe,** un dispositivo electromecánico fundamental durante la Segunda Guerra Mundial para el descifrado de los mensajes producidos por la máquina Enigma.

ANALISIS HISTORICO

La escítala

La escítala es el primer dispositivo criptográfico por transposición en la antigua Grecia, es atribuido a los espartanos en el siglo V a.C. para él envió de mensajes secretos, y fue utilizado especialmente durante la guerra entre Atenas y Esparta.

Figura 1

*Escítala espartana*

Un conjunto de letras negras en un fondo blanco

El contenido generado por IA puede ser incorrecto.

Nota. **Adaptado de *Figura sobre “¿Desde cuándo existe la criptografía?”*, por Criptored, s.f., en *MOOC Crypt4you*. Recuperado el 15 de agosto de 2025, de** <https://criptored.es/crypt4you/temas/criptografiaclasica/leccion2.html#apartado2-1>

García (2009) explica que la escítala es un sistema que consiste en una vara de madera sobre la cual enrollaban una cinta o papiro en forma de espiral una vez esta estuviera fijada se escribía el mensaje de arriba hacia abajo a lo largo de la vara. Cuando la cinta se desenrollaba las letras quedaban desordenadas, aparentando ser algo sin sentido. Para descifrar el mensaje el receptor debía tener una vara con las mismas dimensiones para que a la hora de enrollar la cinta las letras recuperaran la posición inicial. Este método, se le atribuye a Lisandro de Esparta, y aunque su diseño claramente era sencillo fue fundamental en la historia de la criptográfica ya que nos demuestra que la protección de la información es una preocupación que esta desde la antigüedad.

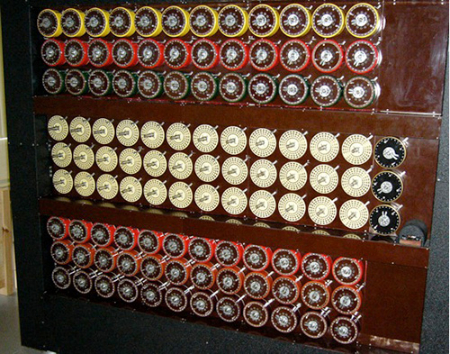
Durante las guerras del Peloponeso (431-404 c.C). La escítala desempeño un papel crucial, según Plutarco (citado en Antigone, 2021), líderes militares espartanos como Lisandro, Clearchus y Agesilao utilizaron la escítala para transmitir órdenes y estrategias sin que el enemigo pudiera interpretarlas en caso de ser interceptadas. Su uso estaba restringido para solo generales y mensajeros de confianza, garantizando así que la información permaneciera segura.

Maquina Bombe

Fue un dispositivo electromecánico que fue creado durante la Segunda Guerra Mundial para descifrar los mensajes que eran cifrados por la maquina Enigma que cifraba los mensajes mediante un cifrado de sustitución, esta máquina fue utilizada por los alemanes para para sus comunicaciones militares. Según García (2009), “Tanto los ingleses como los franceses habían asumido durante años que la maquina Enigma era inviolable. Pero según las investigaciones de los polacos la maquina podía descifrarse”.

Figura 2

*Maquina Bombe*



*Nota.* **De Frank Carter (s.f.), *The Turing Bombe*, en *The Rutherford Journal*. Recuperado el 16 de agosto de 2025, de** <https://rutherfordjournal.org/article030108.html>.

En Inglaterra se establece una sede secreta en **Bletchley Park**, donde personal especializado trabajaba de manera confidencial para descifrar los mensajes y enviar la información a los responsables de las operaciones aliadas.

Entre ellos estaba Alan Turing, quien fue un matemático brillante que tuvo ideas muy ingeniosas para acelerar este trabajo. Se dio cuenta de que algunos mensajes contenían palabras repetidas, como los reportes del clima con la palabra "wetter" (que en alemán significa tiempo). Turing, a través de estas repeticiones, creó un método para enlazar varios dispositivos Enigma por medio de un sistema eléctrico: al encontrar la combinación adecuada, se encendía una luz que indicaba que la clave había sido hallada.

La máquina que crearon, conocida como Bombe, permitió descifrar mensajes de una manera mucho más rápida y no solo eso sino también adaptarse a los cambios que los alemanes hacían para complicar el trabajo. Este invento fue clave para que los Aliados tuvieran ventaja en la guerra, y demostró lo importante que puede ser la unión entre las matemáticas y la tecnología en momentos decisivos (Hodges, 1983).

Me gustaría agregar que hay una película que habla sobre esta hazaña: *The Imitation Game* (titulada en español *El juego de la imitación*).

OPERACIÓN DEL MECANISMO DE CIFRADO ESCITALA

Recordando lo anterior mencionado el cifrado por escítala hace un cambio de ubicación en las letras más conocido como “transposición”. Esta transposición de letras convierte al método de la escítala en el primer cifrado por transposición que se ha conocido en la historia. Para entender cómo funciona este método de cifrado el proceso es el siguiente:

Para cifrar el mensaje se escribe el texto original en una tabla con un numero fijo de columnas, que se determina por el ancho de la vara). Y en lugar de leer el mensaje por filas como se escribió (de izquierda a derecha), se lee por columnas (de arriba hacia abajo). Para descifrar el proceso es inverso hay que leer por filas.

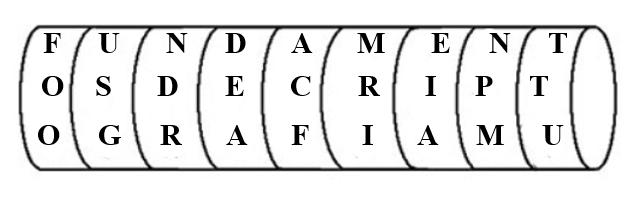
La escítala al ser un método de transposición no funciona con una fórmula matemática como si lo hacen el cifrado Cesar y Vigenere. Sin embargo, si es posible encontrar la clave con facilidad encontrando los divisores del total de letras del mensaje cifrado. Esto se explicara más a fondo en el ejemplo.

EJEMPLO PRACTICO

Acá podemos observar como un mensaje sencillo como “FUNDAMENTOS DE CRIPTOGRAFIA”, puede convertirse en una secuencia de letras confusas, lo que hace que su significado quede oculto a cualquier persona que intercepte la tira:

Figura 3

*Ejemplo Escítala*

**

Nota. **Elaboración propia**.

Al desenrollar la tira, se leería:

**FOOUSGNDRDEAACFMRIEIANPMTTU**

Ahora lo haremos mediante una cuadricula, según Carrión Lostal (2021), Para cifrar un determinado texto hay que seguir los siguientes pasos:

1. Contar el numero de letras que tiene el texto.
2. Obtener los divisores de dicho número.
3. Se pueden utilizar diferentes columnas de acuerdo con los divisores obtenidos anteriormente.
4. Dibujar la cuadricula (fila x columna)
5. Se escribe el texto en horizontal, empezando por la primera casilla a la izquierda.
6. El texto cifrado se obtiene al leer en vertical de arriba hacia abajo.

Ejemplo: Cifraremos el mensaje “Fundamentos de Criptografía”

1. 25 letras.
2. Divisores: 1, 5, 25.
3. Cuadricula: 1x25 o 5x5.
4. Si la cuadricula 5x5 es decir, 5 filas y 5 columnas.
5. La cuadricula quedaría así

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| F | U | N | D | A |
| M | E | N | T | O |
| S | D | E | C | R |
| I | P | T | O | G |
| R | A | F | I | A |

1. El texto cifrado seria:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F | M | S | I | R | U | E | D | P | A | N | N | E | T | F | D | T | C | O | I | A | O | R | G | A |

Al ver los posibles divisores podemos darnos cuenta de que el único razonable seria 5x5 si se intentara con 1x25 el mensaje no se cifraría. En estos casos lo recomendable es añadir una letra para obtener un numero compuesto y así muchos más divisores.

FORTALEZAS Y DEBILIDADES

Escítala

Fortalezas:

* Si los participantes disponían de las mismas varas de madera, era muy fácil y rápido de utilizar.
* No necesita tecnología avanzada, solo una cinta y madera
* Era útil para mensajes cortos y secretos dentro de un grupo pequeño (como los ejércitos de Esparta).

Debilidades:

* Si alguien interceptaba tanto la vara como la cinta, podría descifrar el mensaje muy fácilmente.
* Solo se podía usar solamente para mensajes cortos, ya que con textos más extensos era más difícil de manejar.
* Es necesario que tanto el emisor y receptor tengan varas exactamente iguales; cualquier diferencia hacía ilegible el mensaje.

Máquina Bombe

Fortalezas:

* Era capaz de procesar miles de combinaciones en un tiempo más corto que cualquier ser humano.
* Permitía descifrar los mensajes diarios de la Enigma y la adaptación a las modificaciones continuas que hacían los alemanes.
* Durante la Segunda Guerra Mundial, daba a los Aliados un beneficio táctico esencial.

Debilidades:

* Era demasiado grande y costoso de construir, requería un enorme espacio y una cantidad considerable de personas capacitadas para su buen funcionamiento.
* No podía descifrar mensajes de forma independiente; para hacerlo requería si o si pistas o información del mensaje para funcionar.
* Su complejidad técnica hacía que fuera vulnerable frente a errores humanos o fallas mecánicas.

CRIPTOANALISIS

El criptoanálisis es el conjunto de métodos que se emplean para descifrar mensajes encriptados sin saber cuál es la clave original. En el caso de la **escítala espartana**, algunos de los mecanismos de criptoanálisis que lo hacen inseguro en la actualidad son:

Fuerza Bruta

Uno de los métodos de criptoanálisis consiste en la búsqueda del número de columnas, donde se prueban diferentes diámetros de vara o longitudes de cinta hasta que las letras se conviertan en un mensaje coherente.

Análisis de frecuencia

En cuanto al análisis de frecuencias no es muy útil para este método ya que se trata de una transposición mas no de una sustitución, pero puede ser utilizado para identificar las alineaciones adecuadas a través de la comparación con patrones del idioma original.

Ataque de texto plano conocido

Si el atacante conoce parte del contenido, lograra alinear esas palabras con el criptograma, ya que puede colocar las letras que conoce en una tabla y deducir con facilidad cuantas columnas hay y a su vez cuantos saltos se forman en la frase, ya con la estructura determina puede acceder al mensaje rápidamente.

Al ver estos métodos de criptoanálisis podemos decir que el mecanismo de cifrado escítala es muy inseguro en la actualidad, ya que la clave que tiene es el numero de columnas y cualquier computadora o persona puede probar rápidamente todas las opciones hasta descifrar el mensaje.

SIMULACIONES COMPUTACIONALES

Es una técnica que se utiliza en la actualidad para que programas de computadora puedan imitar o modelar el comportamiento de un sistema real, utilizando algoritmos y cálculos matemáticos. Encontré un simulador (<https://scratch.mit.edu/projects/167849719/>), realizado por un estudiante de la universidad politécnica de valencia. Que, aunque cifra muy bien el texto falla al momento de descifrar.

Así que genere uno utilizando Visual Studio y como lenguaje de programación Python. Es muy sencillo ya que con el puedes cifrar y descifrar un mensaje siempre y cuando sepas la clave o bien puedes intentar con varias combinaciones hasta que el mensaje tenga sentido.

Primero definimos los métodos que utilizaremos, en este caso serán dos, cifrar y descifrar. Para cifrar la longitud del mensaje se divide entre el numero de columnas, si llegan a sobrar se suma una fila extra. Se organiza el mensaje en una tabla con n columnas y se lee columna por columna para cifrar el mensaje.

def escitala\_cifrar(mensaje, columnas):

    filas = len(mensaje) // columnas + (len(mensaje) % columnas > 0)

    cifrado = ""

    for i in range(columnas):

        for j in range(filas):

            indice = j \* columnas + i

            if indice < len(mensaje):

                cifrado += mensaje[indice]

    return cifrado

Ahora para el descifrado, calcula las filas que tuvo el mensaje original, recordemos que para cifrar se lee columna por columna mientras que para descifrar es fila por fila.

def escitala\_descifrar(mensaje\_cifrado, columnas):

    filas = (len(mensaje\_cifrado) + columnas - 1) // columnas

    descifrado = ""

    for i in range(filas):

        for j in range(columnas):

            indice = j \* filas + i

            if indice < len(mensaje\_cifrado):

                descifrado += mensaje\_cifrado[indice]

    return descifrado

Para que sea interactivo primero se crea un bucle infinito que mantiene el programa corriendo hasta que el usuario decida salir. Dentro de este bucle se crea el menú de opciones

while True:

    print("\n=== Escítala ===")

    print("1. Cifrar mensaje")

    print("2. Descifrar mensaje")

    print("3. Salir")

    opcion = input("Elige una opción: ")

Y de acuerdo con la opción escogida el programa llama a los métodos que fueron definidos al principio del código

 if opcion == "1":

        mensaje = input("Escribe el mensaje a cifrar: ")

        columnas = int(input("Escribe el tamaño de la vara (número de columnas): "))

*# Normalización del texto*

        mensaje = mensaje.replace(" ", "").upper()

        mensaje\_cifrado = escitala\_cifrar(mensaje, columnas)

        print("\nMensaje cifrado:", mensaje\_cifrado)

    elif opcion == "2":

        mensaje\_cifrado = input("Escribe el mensaje a descifrar: ")

        columnas = int(input("Escribe el tamaño de la vara (número de columnas): "))

*# Normalización del texto cifrado*

        mensaje\_cifrado = mensaje\_cifrado.replace(" ", "").upper()

        mensaje\_descifrado = escitala\_descifrar(mensaje\_cifrado, columnas)

        print("\nMensaje descifrado:", mensaje\_descifrado)

Pero si se elige la opción 3, el ciclo se rompe por medio de un break. O por el contrario si la opción no estaba dentro del menú sale un mensaje de alerta.

elif opcion == "3":

        print("Saliendo del programa...Adios!")

        break

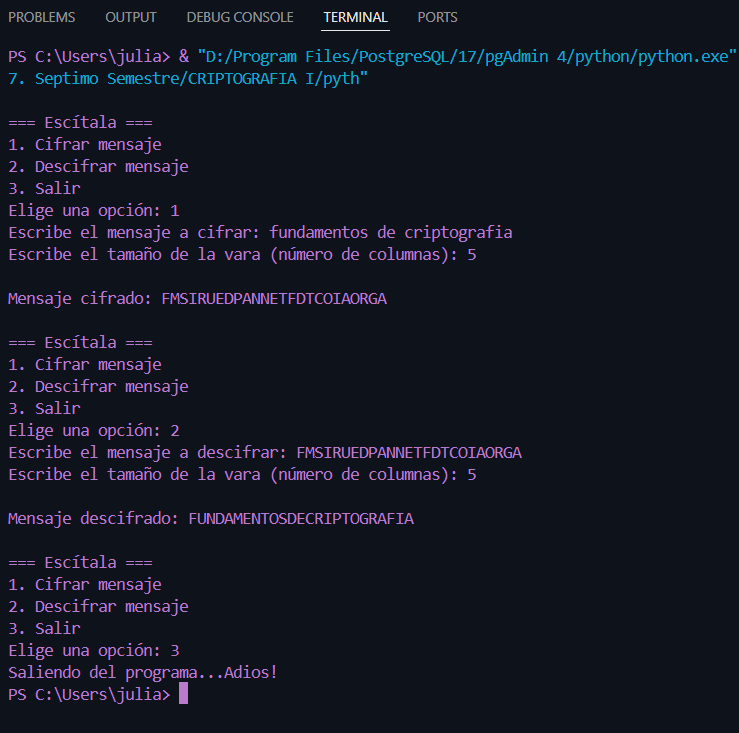
    else:

        print("Opción no válida. Intenta de nuevo.")

Al correr la terminal y hacer intentos el resultado es el siguiente

Texto

El contenido generado por IA puede ser incorrecto.



Texto

El contenido generado por IA puede ser incorrecto.

A continuación, dejo el enlace para ir al repositorio de GitHub, donde encontrara el código completo.

REFERENCIAS

Hernández Encinas, L. (2016). *La criptografía:*(ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas.

<https://elibro-net.proxy.bidig.areandina.edu.co/es/lc/areandina/titulos/41843>   
Criptored. (s.f.). *Figura sobre “¿Desde cuándo existe la criptografía?”* [Figura 1]. MOOC Crypt4you.

<https://criptored.es/crypt4you/temas/criptografiaclasica/leccion2.html#apartado2-1>

García, R. D. M. (2009). *Criptografía clásica y moderna* (ed.). Septem Ediciones. <https://elibro-net.proxy.bidig.areandina.edu.co/es/ereader/areandina/102985?page=8>

Antigone. (2021). *Ancient Cybersecurity? Deciphering the Spartan Scytale*. <https://antigonejournal.com/2021/06/deciphering-spartan-scytale/>

iAgua Grupo-Inclam. (2018, 14 de junio)*. Descifrando Enigma.* [*https://www.iagua.es/noticias/grupo-inclam/descifrando-enigma*](https://www.iagua.es/noticias/grupo-inclam/descifrando-enigma)

*Tyldum, M. (Director). (2014). The imitation game [El juego de la imitación] [Película]. Black Bear Pictures.*

CertSuperior. *(s.f.). Descifrando códigos: Un viaje por el criptoanálisis. CertSuperior.* [*https://www.certsuperior.com/criptoanalisis*](https://www.certsuperior.com/criptoanalisis)

*Carrión Lostal, Ó. (2021). Criptografía para principiantes: método de la escítala. Entorno Abierto, 38, 18–21. Funes.* [*https://funes.uniandes.edu.co/funes-documentos/criptografia-para-principiantes-metodo-de-la-escitala*](https://funes.uniandes.edu.co/funes-documentos/criptografia-para-principiantes-metodo-de-la-escitala)

*Scratch Team. (n.d.). Simulador de cifrado y descifrado [Proyecto en línea]. Scratch.* [*https://scratch.mit.edu/projects/167849719/*](https://scratch.mit.edu/projects/167849719/)