PISTA Nº 57

Centro: CC Santísima Trinidad. Zamora.
Lugar de Libro: "EL MINISTERIO DEL TIEMPO"

Nivel: Educación Secundaria Obligatoria

Enigma: "Criptografía: El disco cifrado de Alberti".

Uno de los agentes de campo del Ministerio del Tiempo ha quedado atrapado en la España del Siglo de Oro. Investigando las posibles relaciones entre las obras de Lope de Vega y Cervantes con la pintura de Pablo Ruiz Picasso ha perdido su enlace y está a punto de ser descubierto.

El subsecretario del Ministerio del Tiempo, junto con el jefe de operaciones y la jefa de logística, muy preocupados por el agente de campo, te eligen como oficial de la organización de inteligencia del Ministerio, encargado de descodificar el mensaje encriptado que hará regresar a nuestra época al compañero atrapado en una de las épocas más significativas de la Historia de España.

Como oficial de inteligencia debes averiguar el mensaje cifrado que el agente de campo ha transmitido desde Madrid unos días antes del fallecimiento de Miguel de Cervantes allá por el mes de abril de 1616.

Utiliza el disco de cifrado de Alberti y encontrarás la palabra que buscamos.

EHM9K

Gracias a una lista secreta superior se confirma que la **clave** para este mensaje es **9**.

Instrucciones:
Sigue los siguientes pasos para descifrar el mensaje.

1. Copia la clave en el lugar que le corresponde en el formulario (ver más abajo).
2. Copia igualmente el texto cifrado en el lugar que le corresponde del formulario.
3. Utiliza el disco de cifrado de Alberti para desencriptar el mensaje de texto sin formato.
4. Puedes utilizar la versión imprimible o el juego online (descárgalo AQUÍ)

Ingresa tanto el texto cifrado como la clave repetitiva en los cuadros apropiados en el formulario.

Gira el rotor hasta que el primer carácter de tecla ('L') esté alineado debajo de 'A' en la placa de base exterior. Encuentra el primer carácter de texto cifrado ('V') en el rotor.

Encima de 'V' en el rotor encuentras 'L' en la placa base. Este es el primer caracter en el mensaje de texto plano. Escribe 'L' en el primer recuadro en la línea de texto plano.

Para encontrar la segunda letra de texto plano, gira el rotor hasta que el segundo carácter de tecla ('I') esté alineado debajo de 'A' en la placa de base.

El segundo carácter de texto cifrado (también 'I') ahora está alineado debajo de 'A' en la placa de base. Por lo tanto, 'A' es el segundo carácter en el mensaje de texto sin formato, por lo que escribe 'A' en el segundo recuadro en la línea de texto sin formato.

Completa este ejemplo para leer el mensaje secreto.

Se insertan algunas letras adicionales de texto sin formato como ayuda en este ejercicio.

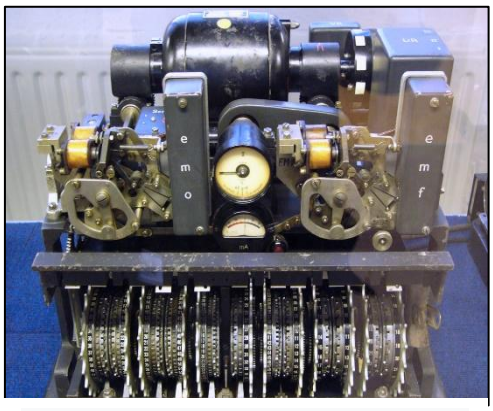
Formulario:

PLAINTEXT					
KEY	9	9	9	9	9
CIPHERTEXT	E	H	M	9	K

INFORMACIÓN PREVIA:

1. ¿Qué es la Criptografía?

Del griego κρύπτος (criptos), «oculto», y γραφη (grafé), «grafo» o «escritura», literalmente ***«escritura oculta»***.



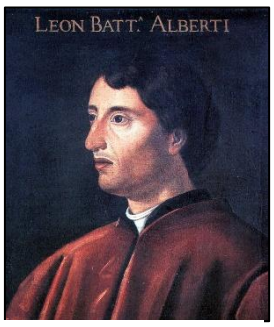
Máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes destinados a generales de muy alto rango.

La criptografía se ha definido, tradicionalmente, como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

El único objetivo de la criptografía era conseguir la confidencialidad de los mensajes, para lo cual se diseñaban sistemas de cifrado y códigos.

2. ¿Quién era Leon Battista Alberti?

Génova, Italia, 18 de febrero de 1404 - Roma, 25 de abril de 1472.



Retrato de Albeti

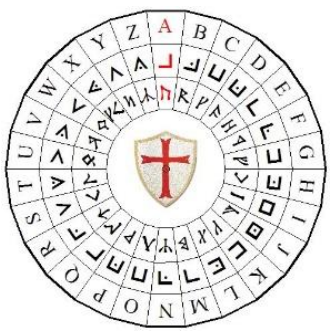
Fue un arquitecto, secretario personal (abreviador apostólico) de tres papas - Eugenio IV, Nicolás V y Pío II - , humanista, tratadista, matemático y poeta italiano.

Además de estas actividades principales, también fue criptógrafo, lingüista, filósofo, músico y arqueólogo.

Fue, sin duda, uno de los humanistas más polifacéticos e importantes del Renacimiento.

Como criptógrafo publicó el primer libro sobre criptoanálisis en Europa Occidental y creó el primer cifrado polialfabético (conocido como ***"Cifrado de Alberti"***) e inventó la primera máquina de cifrado (Alberti Cipher Disk - "El disco cifrado de Alberti").

Su cifrado polialfabético fue el avance más significativo en la criptografía desde la época de Julio César. Por ello, el historiador de la criptografía David Kahn, bautizó a Alberti como el "Padre de la Criptografía Occidental".



Alberti estaba activo en la masonería italiana. Esto le condujo a una relación con los Caballeros Templarios que

aunque aún no está clara, los historiadores especulan que él diseñó el Disco de Cifrado Templario y enseñó a los Caballeros cómo usarlo para asegurar sus comunicaciones clandestinas. Ambos dispositivos funcionan con los mismos principios.

Disco de cifrado Templario

Notas históricas:

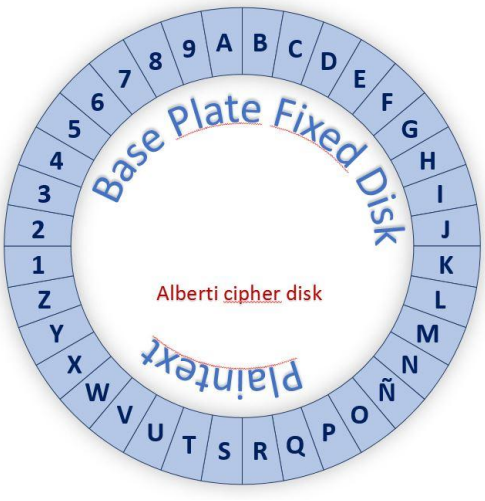
- La Royal Navy usó el cifrado de Alberti (British Naval Cypher No. 2) hasta principios de 1942, cuando descubrieron que los alemanes habían roto el código y estaban leyendo sus mensajes secretos.
- En la Segunda Guerra Mundial, por ejemplo, el Kriegsmarine (Armada alemana) usó el cifrado supuestamente irrompible de la máquina Enigma para proteger sus comunicaciones de radio. Cada barco en su flota llevaba un folleto que enumeraba la configuración diaria del rotor (un tipo de clave) y se actualizaba trimestralmente.
- El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.

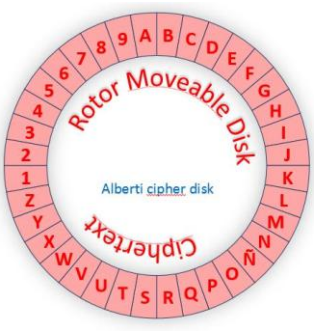
3. ¿Qué es el disco de cifrado Alberti?

El disco de cifrado Alberti es un dispositivo simple.

El disco está formado por dos discos concéntricos que giran independientemente. En el disco exterior, aparecen ordenadas de la "A" a la "Z" las letras del alfabeto así como los números del 1 al 9 también ordenados. En el disco interior, más pequeño, aparecen las mismas letras y números.

Así, el disco cifrado de Alberti consta de dos piezas: la placa base (disco exterior en azul) y el rotor (disco interior en rojo). El rotor se sitúa siempre en la parte superior de la placa base.





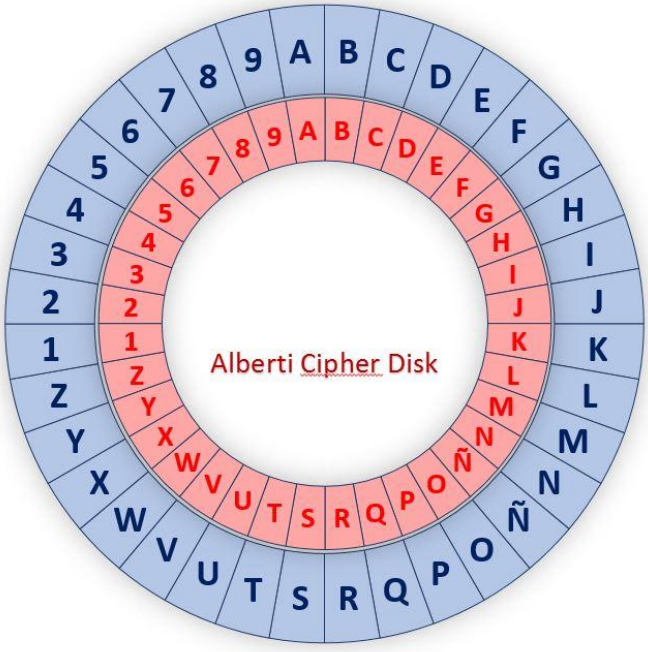
Disco interior: Rotor (en rojo)

Disco exterior: Placa base (en azul)

4. ¿Cómo se utiliza el disco de cifrado Alberti?

Para poder utilizarlo, hay que ponerlos juntos en su eje de rotación haciendo coincidir, en su primera colocación, todas sus letras y números:

'A' azul con 'A' roja, 'B' azul con 'B' roja y así sucesivamente.



Disco cifrado de Alberti

Inicialmente, el Rotor (rojo) está alineado con la Placa base (azul) para que todas las letras y números coincidan y estén alineadas: rojo 'A' frente al azul 'A', etc.

Si el Rotor se gira un espacio en el sentido de las agujas del reloj, esto pone el rojo '9' opuesto al azul 'A', el rojo 'A' opuesto al azul 'B'…

En el Ejemplo 1, la CLAVE es '9' porque colocamos '9' en el rotor debajo de 'A' en la placa de base y dejamos esta configuración para todo el mensaje.

Ejemplo 1:

PLAINTEXT / TEXTO PLANO	A	T	T	A	C	K
KEY / CLAVE	9	9	9	9	9	9
CIPHERTEXT / TEXTO CIFRADO	9	S	S	9	B	J

Clave: **9**

Texto plano: **Attack**

Texto cifrado: **9SS9BJ**

Esto es idéntico al método simple y antiguo de sustitución **monoalfabética** llamado cifrado por desplazamiento de Caesar.

Agregando otra tecla, alternamos el primer turno en el sentido de las agujas del reloj con un segundo turno en sentido contrario a las agujas del reloj a 'B'. Ahora la tecla es '9B', que refleja estos cambios alternativos a la derecha / izquierda.

Ejemplo 2:

PLAINTEXT / TEXTO PLANO	A	T	T	A	C	K
KEY / CLAVE	9	B	9	B	9	B
CIPHERTEXT / TEXTO CIFRADO	9	U	S	B	B	L

Clave: **9B**

Texto plano: **Attack**

Texto cifrado: **9USBBL**

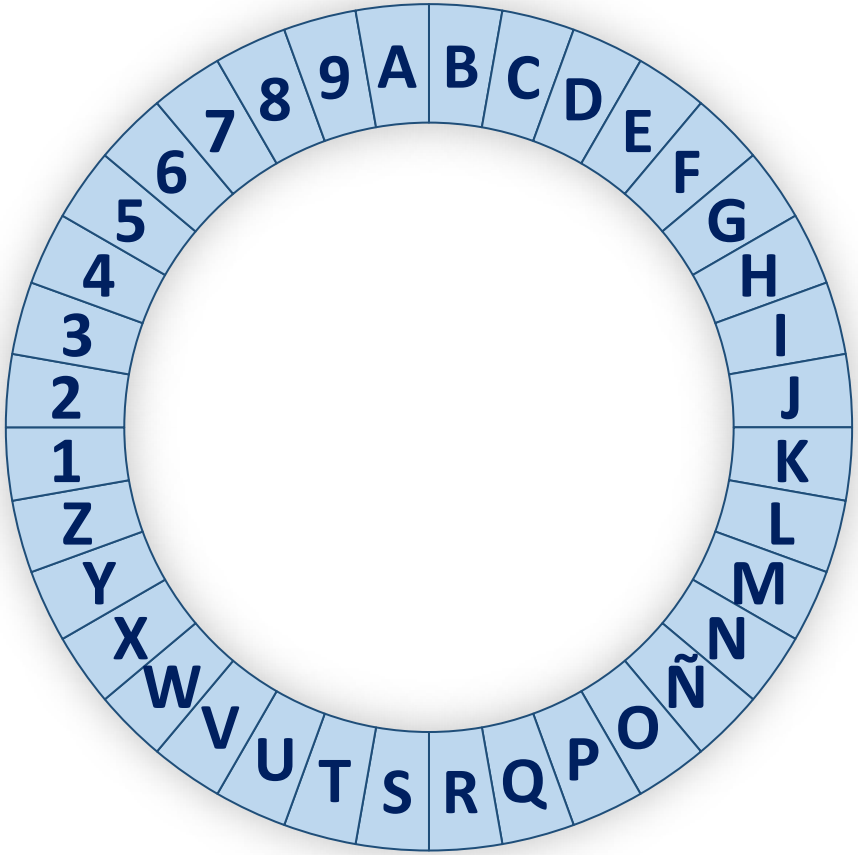
El cambio adicional produce un texto cifrado mejorado.

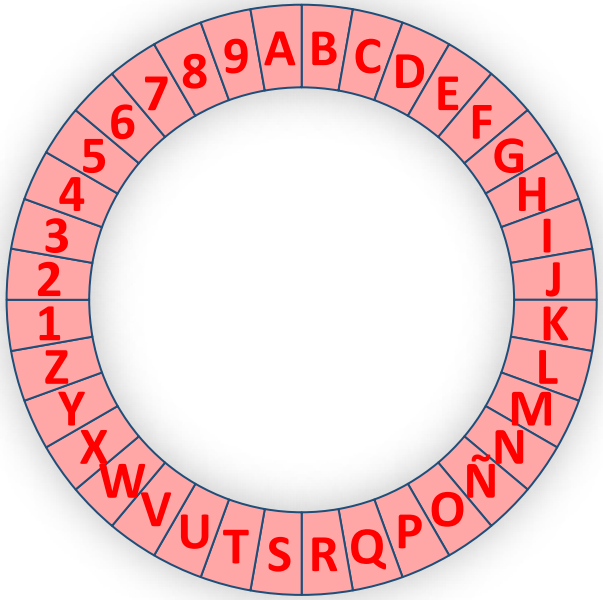
El texto plano 'A' ahora puede aparecer como '9' o como 'B' en el texto cifrado. El texto plano 'T' puede aparecer en el texto cifrado como 'U' o como 'S'.

Si bien, este cifrado no disuadiría a un experto criptoanalista por mucho tiempo, la diferencia más significativa es que ahora es un cifrado **polialfabético** (aunque la versión más simple de este tipo).

El sistema polialfabético tiene posibilidades de sustitución ilimitadas, en función de la longitud de la llave/clave que se usa.

Disco Cifrado para imprimir:
(Cortar y montar)


9 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 1 2 3 4 5 6 7 8


9 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 1 2 3 4 5 6 7 8