****

**UNIVERSIDAD CATÓLICA SAN PABLO**

**FACULTAD DE INGENIERÍA Y TELECOMUNICACIONES**

**PROGRAMA PROFESIONAL DE CIENCIA DE LA COMPUTACIÓN**

# ALGORITMOS DE CRIPTOGRAFÍA TRADICIONALES

|  |  |
| --- | --- |
| |  | | --- | | - Dia de la Vega, Abel  - Estefanero Chávez, Renzo  - Guzmán Chiroque, Rubén Félix  - Salas Luna, Luis Enrrique  - Sicos Barrera, Rony Rodrigo  - Vilchez Gustavson, Diego Nicolás | |

AREQUIPA – PERÚ 2020

**CRIPTOGRAFÍA**

La **criptografía** (del [griego](https://es.wikipedia.org/wiki/Idioma_griego) κρύπτos (kryptós), «oculto», y γραφή (graphé), «grafo» o «escritura», literalmente «escritura oculta») se ha definido, tradicionalmente, como el ámbito de la [criptología](https://es.wikipedia.org/wiki/Criptolog%C3%ADa) que se ocupa de las técnicas de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) o [codificado](https://es.wikipedia.org/wiki/C%C3%B3digo_(criptograf%C3%ADa)) destinadas a alterar las [representaciones lingüísticas](https://es.wikipedia.org/wiki/C%C3%B3digo_(comunicaci%C3%B3n)) de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. El único objetivo de la criptografía era conseguir la [confidencialidad](https://es.wikipedia.org/wiki/Confidencialidad) de los mensajes, para lo cual se diseñaban [sistemas de cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) y [códigos](https://es.wikipedia.org/wiki/C%C3%B3digo_(criptograf%C3%ADa)), y la única criptografía existente era la llamada [criptografía clásica](https://es.wikipedia.org/wiki/Cifrado_cl%C3%A1sico).

Existen varias ramas de esta, pero nos centraremos en la criptografía tradicional.

**CRIPTOGRAFÍA TRADICIONAL**

En la criptografía tradicional, hay básicamente dos variantes: la simétrica y la asimétrica.

La simétrica es la más antigua de todas. Consta de una contraseña, frase de paso, o como le queramos llamar, que sirve tanto para codificar el mensaje, como para leerlo. Esto es muy útil, y eficaz. Pero el que lea el mensaje se puede hacer pasar por nosotros, pues tiene nuestra contraseña.

La asimétrica, algo más nueva, trata de dejar dos claves: una para cifrar y otra para descifrar. Esto es una seguridad añadida, pues no necesitamos que el receptor sea capaz de codificar mensajes, sólo descodificar.

Esto es una ventaja, porque si el receptor tiene un problema de seguridad, a tí no te compromete.

la criptografía tradicional se intentaba dificultar el criptoanálisis sobre todo mediante el empleo de claves muy grandes, en lugar de complicar los algoritmos.

**CRIPTOGRAFÍAS POR TRANSPOSICIÓN**

En [criptografía](https://es.wikipedia.org/wiki/Criptograf%C3%ADa), un **cifrado por transposición** es un tipo de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) en el que unidades de texto plano se cambian de posición siguiendo un esquema bien definido; las 'unidades de texto' pueden ser de una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior,... Es decir, hay una [permutación](https://es.wikipedia.org/wiki/Permutaci%C3%B3n) de 'unidades de texto'.

**Ejemplo:**

ESCITALA



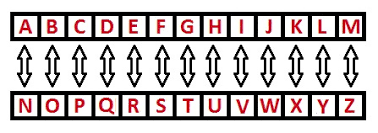
**CRIPTOGRAFÍAS POR SUSTITUCIÓN**

En [criptografía](https://es.wikipedia.org/wiki/Criptograf%C3%ADa), el **cifrado por sustitución** es un método de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular; las "unidades" pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros. El receptor descifra el texto realizando la sustitución inversa.

Entre los cuales encontramos cifrados:

**Monoalfabéticos:** Cesar, Playfair

**Polialfabéticos:** Vernam, Polybius, Enigma



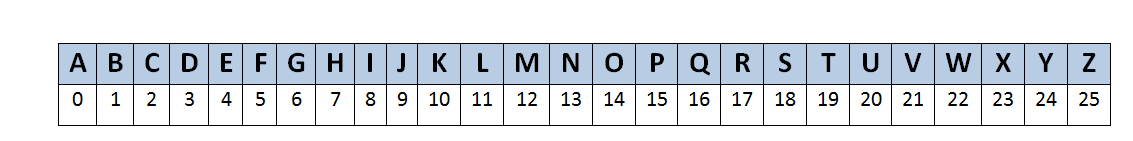
**VERNAM**

**Origen**

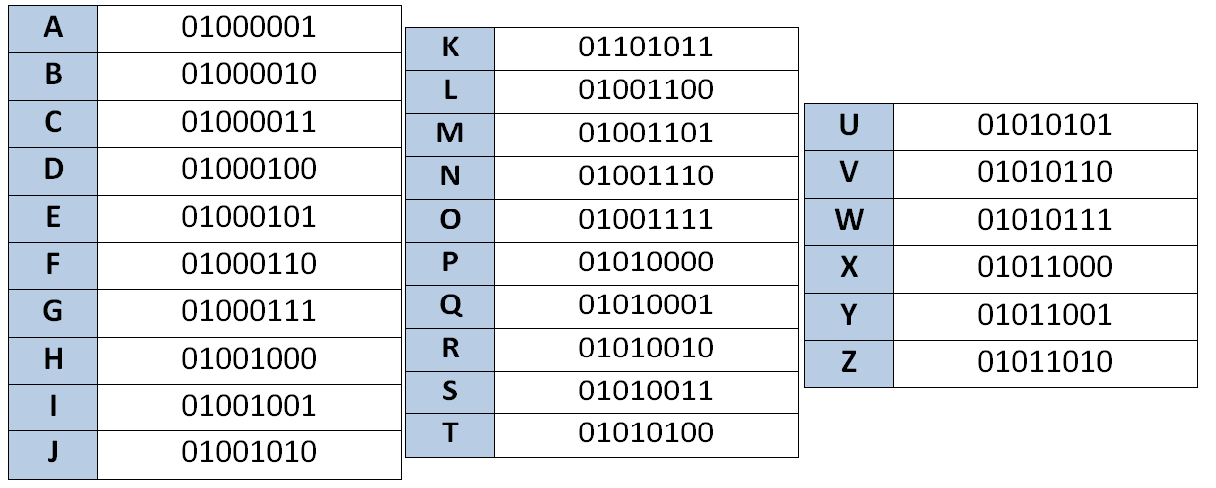
El cifrado Vernam es un algoritmo de criptografía inventado por Gilbert Vernam, ingeniero AT&T Bell Labs, en 1917.El cifrado de Vernam es un cifrado de flujo en el que el texto en claro, de tipo binario, se combina mediante la operación XOR con un flujo de datos aleatorio o pseudo aleatorio del mismo tamaño, para generar un texto cifrado.

**Cifrado**

Usamos este alfabeto

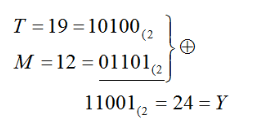


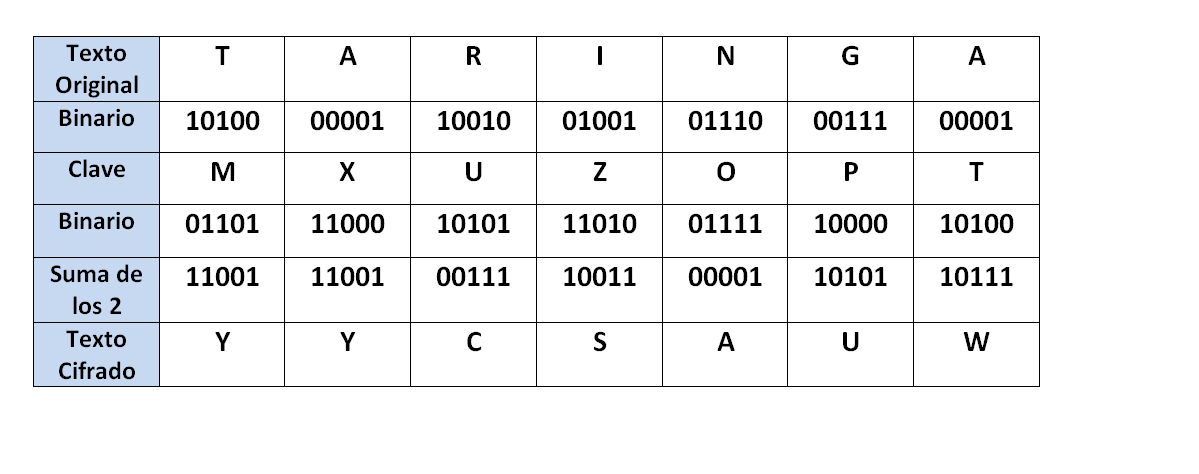
Se le proporciona un valor binario dependiendo de su posición en ASCII.



**Para encriptar cogemos el valor de la i letra tanto en el mensaje y en la clave y aplicamos la conversión a Binario y para finalizar usamos los 5 últimos dígitos de estos y aplicamos el XOR de estos. Para el descifrado se implementa el mismo método.**

**Ejemplo: TARINGA x MXUZOPT**



**ESCÍTALA**

**Origen**

La escítala era usada en el siglo V a.d. C. por el pueblo griego lacedemonios. Consistía en un bastón en el que se enrollaba una cinta y luego se escribe en ella el mensaje de forma longitudinal.

Al desenrollar la cinta, las letras aparecían sin orden alguno.

La única posibilidad de deshacer esta cifra pasaba por enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal.

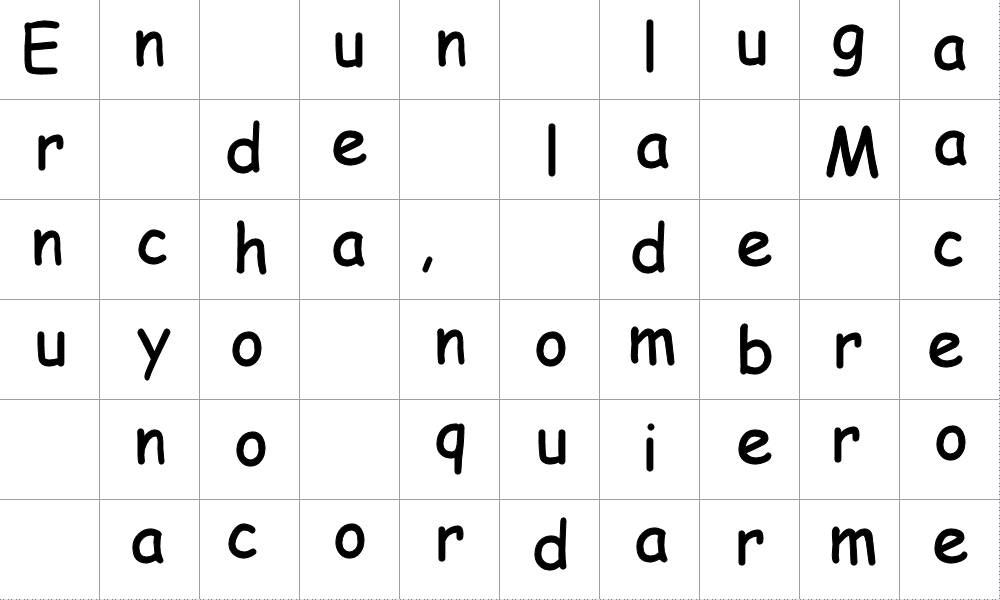
**Cifrado y descifrado**

Usa el método de transposición que consiste en alterar el orden de los elemento de un mensaje.

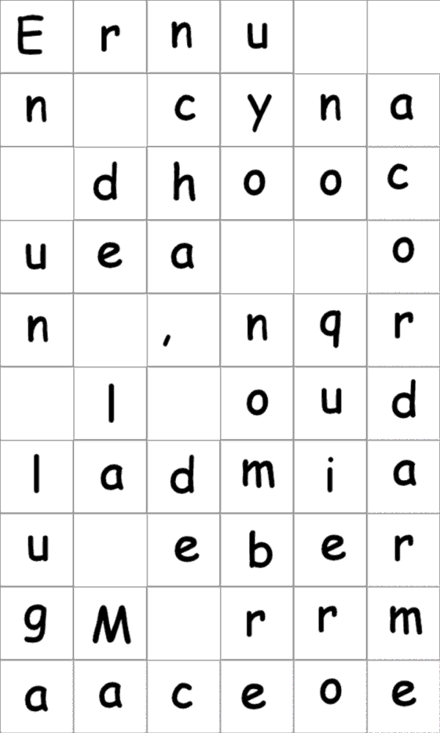
El método que se usa para escítala, es la transposición seriada continua (no tiene saltos). Este método también es conocido como transposición de matrices.

Prácticamente es como disponer en una tabla cada elementos de la palabra en filas y luego recibir las columnas como la palabra cifrada.

**Ejemplo:**



El mensaje a cifrar es: “En el lugar de la Marche, de cuyo nombre no quiero acordarme” con clave 10, se construye una tabla, en el que empezamos a disponer cada elemento del mensaje(teniendo en cuenta los “espacios”) en las casillas de izquierda a derecha, de arriba hacia abajo.



El texto cifrado resulta de tomar verticalmente cada elemento y recorriendo una columna al terminar la fila. Siendo el mensaje cifrado resultante: “Ernu n cyna dhoocuea on ,nqr l oudladmiau ebergM rrmaaceoe”.

Descifrar el texto es volver a disponer cada elemento en la tabla y volver a hacer el proceso que se hizo al cifrar, tomar verticalmente cada elemento y recorriendo una columna al terminar la fila.

**Código de ruptura**

Se puede romper fácilmente, porque el proceso de cifrado consiste en transponer las letras del mensaje y no sustituirlas.

Tomemos, por ejemplo, una vez desenrollado, la cinta en la que se encuentra el siguiente mensaje:

MSE\_YEEEARM\_QÑNJOUPUO

Con esta visión de cifrado, podemos atacar con los siguientes pasos:

1. Cuente el número de letras en la tira (aquí 21)
2. Crea cuadrículas de varios tamaños para que puedas colocar todas las letras. Con 21, tenemos 2 × 11, 3 × 7, 4 × 6, 5 × 5, 6 × 4, etc.
3. Para cada cuadrícula, los cuadros se llenan línea por línea con el texto cifrado. Hacemos lo mismo con una copia de esta cuadrícula pero esta vez rellenando columna por columna. Esto equivale a tener, por ejemplo, una cuadrícula de 4 × 6 y 6 × 4.
4. Compruebe si aparece un texto plano perpendicular al relleno de la cuadrícula (si se ha llenado línea por línea, leemos columna por columna).

En nuestro caso, con una cuadrícula de 3 × 7:



El mensaje no aparece en las columnas, intentamos con la cuadrícula inversa, es decir, 7 × 3:



mensaje: MENSAJERO MUY PEQUEÑO

**PLAYFAIR**

Primer algoritmo de cifrado por pares, desarrollado por Wheatstone y difundido por Playfair.

Hace uso de una clave de matriz 5x5, la cual usa la clave original para la primera fila(si el tamaño de la clave supera los 5, se procede con la siguiente fila), y las demás s con las primeras letras del abecedario omitiendo las de la clave original.(el abecedario no hace uso de la J ni de la Ñ)

El mensaje tiene que ser procesado:

* Si el mensaje es impar, agregar una X, en cualquier posición.
* De haber un par igual, agregar una letra insignificable.

Para codificar el mensaje se hace uso de 5 reglas:

1. Si **m1** y **m2** se encuentran en la misma fila, escoger **c1** y **c2** situados a su derecha (circularmente).
2. Si **m1** y **m2** se encuentran en la misma columna, escoger **c1** y **c2** situados debajo (circularmente).
3. Si **m1** y **m2** se encuentran en distintas filas y columnas, escoger **c1** y **c2** situados en la diagonal opuesta.
4. Si **m1** = **m2**, insertar carácter sin significado entre **m1** y **m2** para evitar su repetición, y después aplicar las reglas 1-3.
5. Si el número de letras es impar, añadir una sin significado al final del texto.

1.(Wikipedia, Cifrado de Playfair, <https://es.wikipedia.org/wiki/Cifrado_de_Playfair> ,21/04/2020)

Algunas reglas comunes para el cifrado son:

1.-'J' se reemplaza con 'I' para ajustarse al cuadrado de 5x5

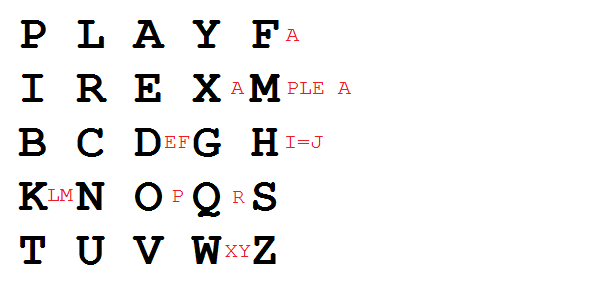
2.-'X' se usa como sustitución en caso de que necesite completar una segunda letra en el diagrama, o dividir dos letras idénticas.

2.(Planetcalc, Cifrado de Playfair, <https://es.planetcalc.com/7751/>, 21/04/2020)

**Ejemplo:**

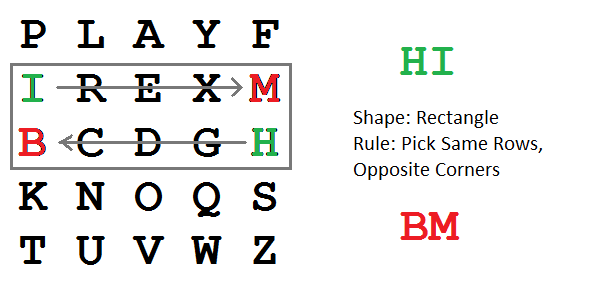
Usando "playfair example" como la clave (suponiendo que I y J son intercambiables), la tabla se convierte (letras omitidas en rojo):

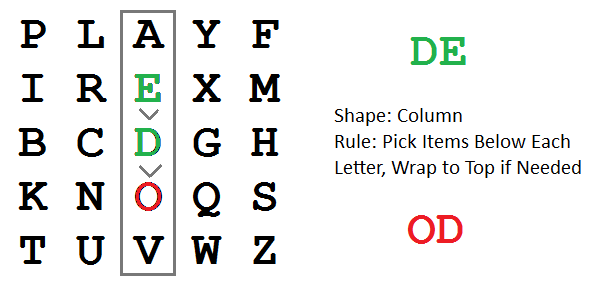
**Matriz:**



Cifrando el mensaje "Hide the gold in the tree stump" (tenga en cuenta la "X" nula utilizada para separar las "E" repetidas):

HI DE TH EG OL DI NT HE TR EX ES TU MP

1. El par HI forma un rectángulo, reemplácelo con BM [](https://translate.googleusercontent.com/translate_c?depth=1&hl=es&pto=aue&rurl=translate.google.com&sl=auto&sp=nmt4&tl=es&u=https://en.m.wikipedia.org/wiki/File:Playfair_Cipher_01_HI_to_BM.png&usg=ALkJrhgXX2VGz3VkZtiNMelNo0TYJgQQGA)

2. El par DE está en una columna, reemplácelo con OD [](https://translate.googleusercontent.com/translate_c?depth=1&hl=es&pto=aue&rurl=translate.google.com&sl=auto&sp=nmt4&tl=es&u=https://en.m.wikipedia.org/wiki/File:Playfair_Cipher_02_DE_to_OD.png&usg=ALkJrhjSrmqWrGlkLcOKLnmJhVknhyXGhw)

3. El par TH forma un rectángulo, reemplácelo con ZB

4. El par EG forma un rectángulo, reemplácelo con XD

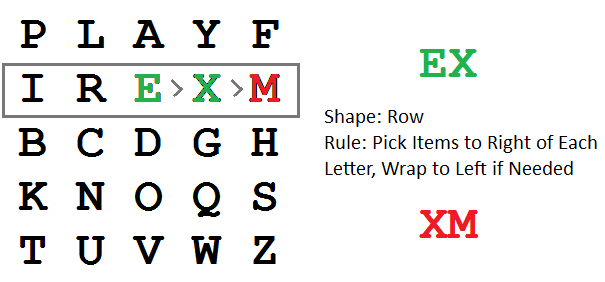
5. El par OL forma un rectángulo, reemplácelo con NA

6. El par DI forma un rectángulo, reemplácelo con BE

7. El par NT forma un rectángulo, reemplácelo con KU

8. El par HE forma un rectángulo, reemplácelo con DM

9. El par TR forma un rectángulo, reemplácelo con UI

10. El par EX (X insertado para dividir EE) está en una fila, reemplácelo con XM [](https://translate.googleusercontent.com/translate_c?depth=1&hl=es&pto=aue&rurl=translate.google.com&sl=auto&sp=nmt4&tl=es&u=https://en.m.wikipedia.org/wiki/File:Playfair_Cipher_10_EX_to_XD.png&usg=ALkJrhhhsQE6uRJqm__bANWZyjhzls6lgw)

11. El par ES forma un rectángulo, reemplácelo con MO.

12. El par TU está en una fila, reemplácelo con UV.

13. El par MP forma un rectángulo, reemplácelo con IF.

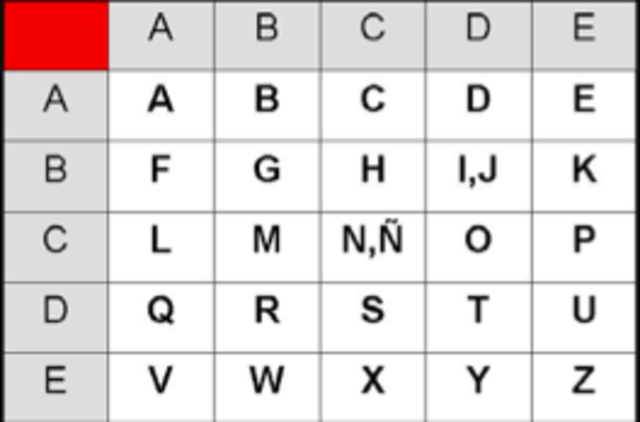
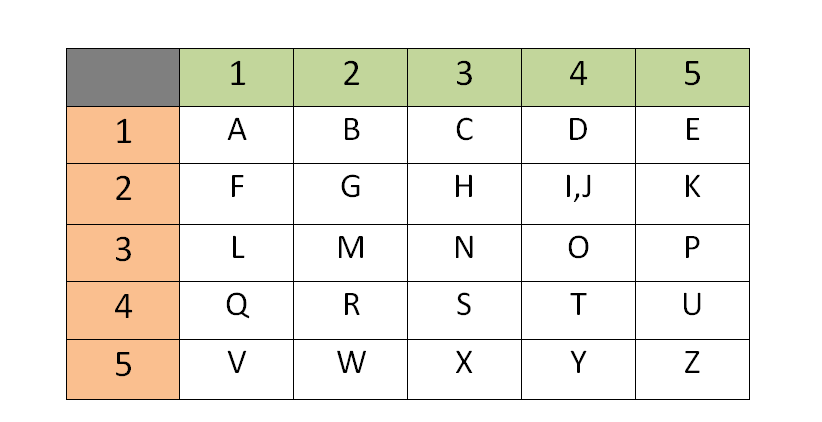
mensaje cifrado:

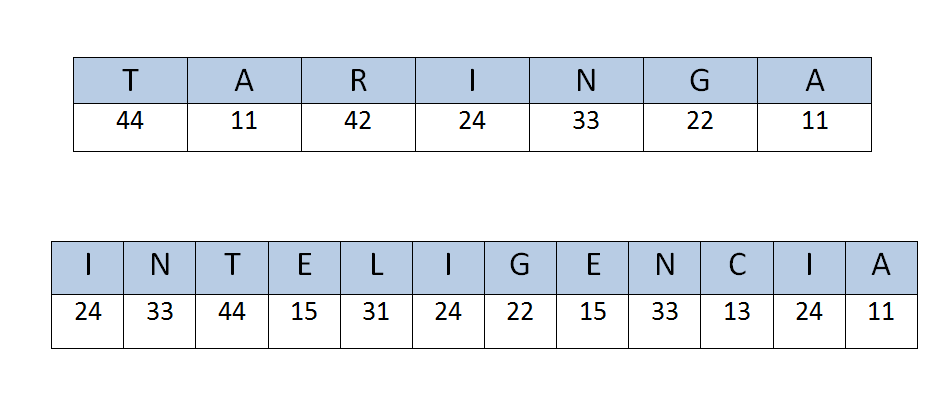
BM OD ZB XD NA BE KU DM UI XM MO UV SI

**POLYBIUS**

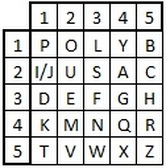
Inventado hacia 150 a.C por el historiador Polibio, el **cuadrado de Polibio** fue utilizado principalmente por nihilistas rusos encerrados en las prisiones zaristas.

Se trata de un algoritmo trivial, donde cada letra del alfabeto es reemplazada por las coordenadas de su posición en un cuadrado. Es un caso particular de transposición mono-alfabética. Este tipo de código no resiste a un análisis de frecuencias.



De esta manera, la codificación consiste en indicar la fila y columna que ocupa cada letra, de forma sucesiva, en el cuadrado. Por ejemplo, la *T* está en la línea 4 y en la columna 4, y por lo tanto, le corresponde el 44.

Esta encriptación es estándar, y hasta ahora no tiene clave, por lo que se rompe fácilmente. Necesitamos introducir la idea de una clave en el cuadrado de Polybius para hacerlo más seguro (Principio de Karckhoffs).



Se reordena el alfabeto usando primero las letras de la palabra clave, ignorando cualquier repetición.

Entonces, usando una palabra clave de polybius obtenemos el cuadro mixto.

El proceso de encriptado es el mismo al explicado anteriormente

**HILL**

Es un cifrado de sustitución poligráfica que se basa en el álgebra lineal. Fue inventado por Lester S. Hill en 1929, y fue el primer cifrado poligráfico que era práctico para operar inmediatamente sobre más de tres símbolos. Para poder operar con este cifrado, hay que tener un conocimiento básico de matrices.

En este cifrado, comúnmente se utiliza el alfabeto numérico sin considerar la ñ (A = 0, B = 1, … , Z = 25), pero esta característica no es esencial para el cifrado. Para la encriptación de un mensaje, cada bloque de N letras (consideradas como un vector) se multiplica por una matriz invertible de tamaño NxN mod 26. El cifrado puede ser adaptado a cualquier otro alfabeto con diferentes órdenes numéricos, donde el modular 26 sea reemplazado por la longitud del alfabeto. La única condición especial es que la matriz NxN siempre debe ser invertible.

Dicha matriz NxN es la clave del cifrado, donde cada uno de los elementos representa el número equivalente a las letras de dicha clave.

**Ejemplo:**

Consideremos el mensaje ‘ACT’ y la clave ‘GYBNQKURP’:

**6 24 1**

**13 16 10**

**20 17 15**

‘A’ equivale a 0, ‘C’ equivale a 2 y ‘T’ equivale a 19, por lo que el mensaje sería el vector:

**0**

**2**

**19**

Por lo tanto, el vector cifrado da como resultado:

**6 24 1 0 67**

**13 16 10 x 2 = 222**

**20 17 25 19 319**

Luego, se saca el módulo 26 de los elementos resultantes:

**67mod26 15**

**222mod26 = 14**

**319mod26 7**

En este nuevo vector, el texto resultante corresponde a ‘POH’. Ahora supongamos que el mensaje es ‘CAT’:

**6 24 1 2 31mod26 5**

**13 16 10 x 0 = 216mod26 = 8**

**20 17 15 19 325mod26 13**

Vemos que el texto resultante corresponde al mensaje ‘FIN’, por lo que alterar el orden del mensaje original cambia por completo el mensaje cifrado.

**Descifrado:**

Para descifrar, se transforma al texto cifrado en un vector, tal como en el cifrado, pero la clave debe convertirse en su matriz inversa (considerando la misma clave del cifrado, esta inversa vendría a ser ‘IFKVIVVMI’), por lo que el descifrado para ‘POH’ sería:

**8 5 10 15 260mod26 0**

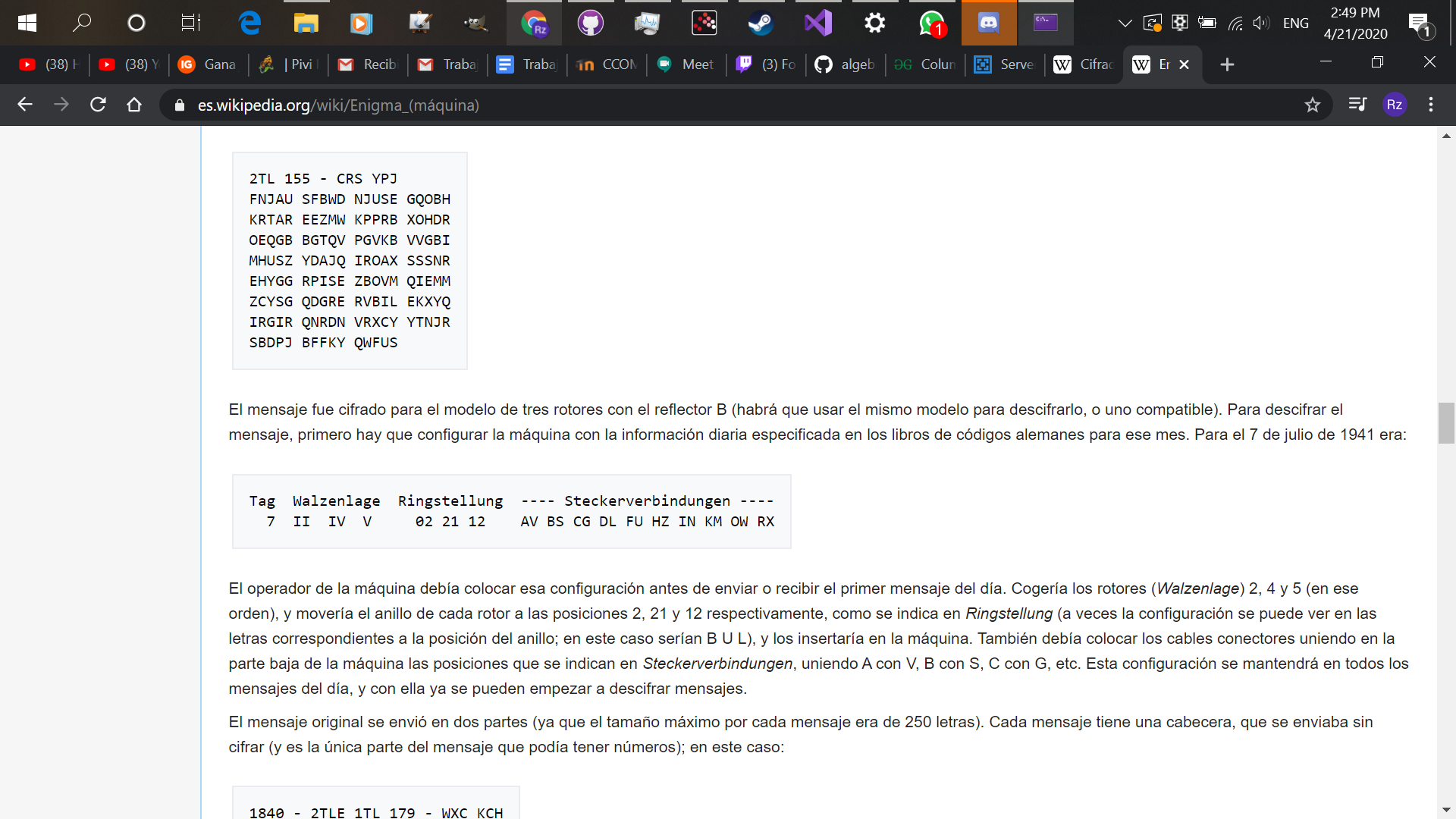
**21 8 21 x 14 = 574mod26 = 2**

**21 12 8 7 539mod26 19**

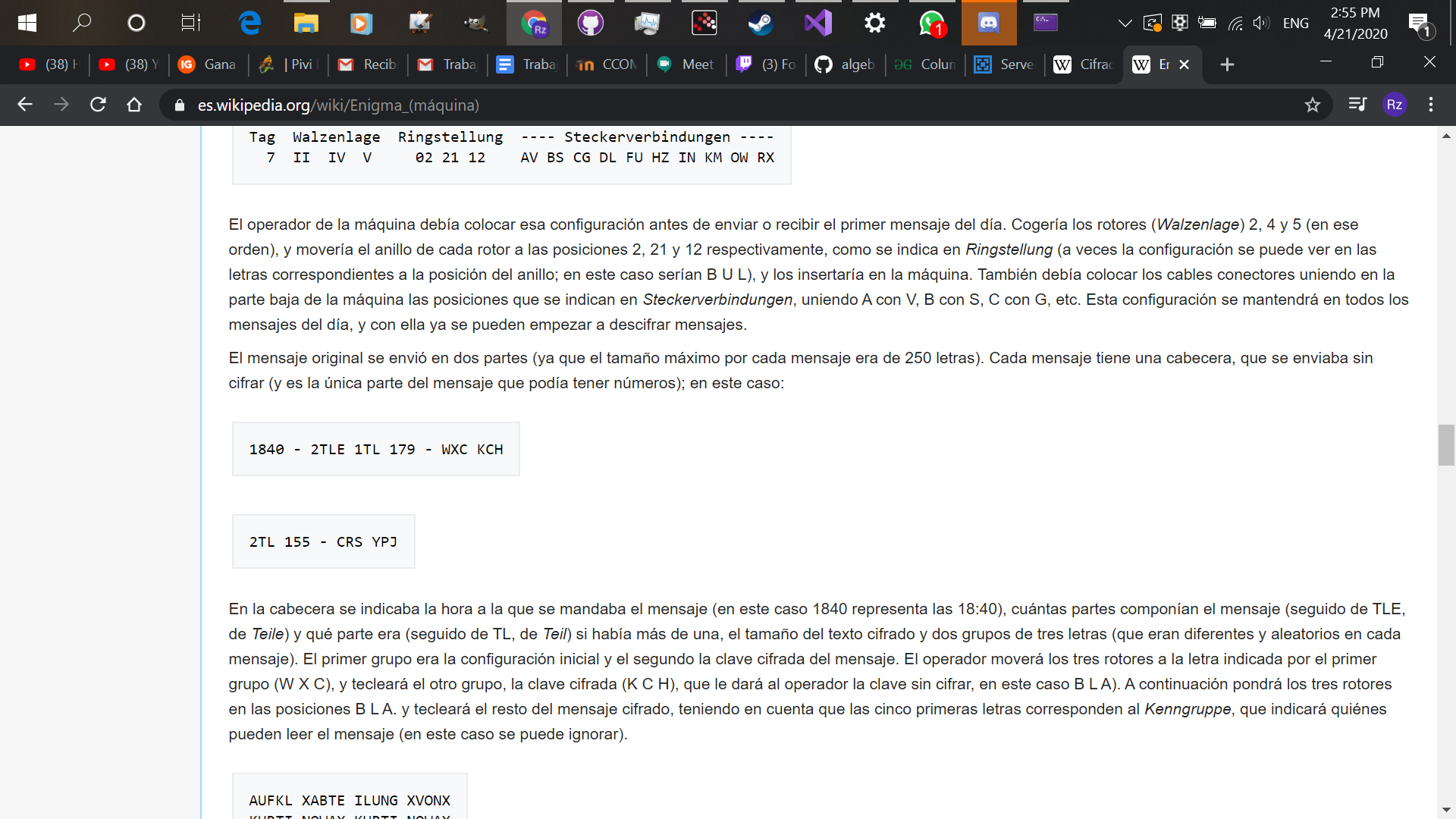
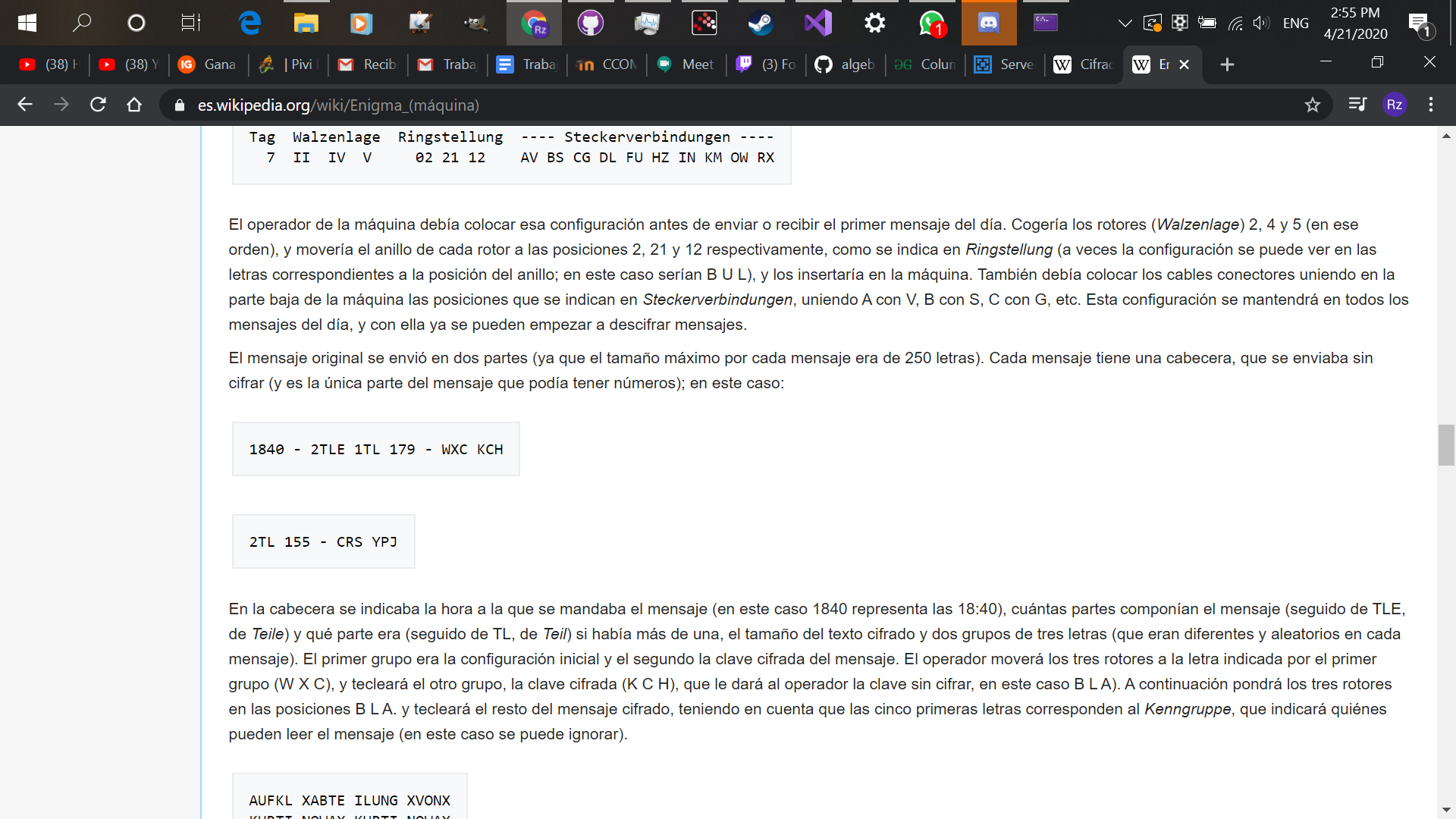
Este descifrado nos da como resultado el vector equivalente al mensaje ‘ACT’, tal y como se esperaba.

**ENIGMA**

Al principio de cada mes, se daba a los operadores de la Enigma un nuevo libro que contenía las configuraciones iniciales para la máquina. Por ejemplo, Para el 7 de julio de 1941 era:



El operador de la máquina debía colocar esa configuración antes de enviar o recibir el primer mensaje del día. Cogería los rotores (*Walzenlage*) 2, 4 y 5 (en ese orden), y movería el anillo de cada rotor a las posiciones 2, 21 y 12 respectivamente, como se indica en *Ringstellung* y los insertaría en la máquina. También debía colocar los cables conectores uniendo en la parte baja de la máquina las posiciones que se indican en *Steckerverbindungen*, uniendo A con V, B con S, C con G, etc. Esta configuración se mantendrá en todos los mensajes del día, y con ella ya se pueden empezar a descifrar mensajes.



En la cabecera se indicaba la hora a la que se mandaba el mensaje (en este caso 1840 representa las 18:40), cuántas partes componían el mensaje (seguido de TLE, de *Teile*) y qué parte era (seguido de TL, de *Teil*) si había más de una, el tamaño del texto cifrado y dos grupos de tres letras (que eran diferentes y aleatorios en cada mensaje). El primer grupo era la configuración inicial y el segundo la clave cifrada del mensaje. El operador moverá los tres rotores a la letra indicada por el primer grupo (W X C), y tecleará el otro grupo, la clave cifrada (K C H), que le dará al operador la clave sin cifrar, en este caso B L A). A continuación, pondrá los tres rotores en las posiciones B L A. y tecleara el resto del mensaje cifrado, teniendo en cuenta que las cinco primeras letras corresponden al *Kenngruppe*, que indicará quiénes pueden leer el mensaje (en este caso se puede ignorar).

**REFERENCIAS**

**Vernam**

<https://es.wikipedia.org/wiki/Cifrado_Vernam>

<https://www.taringa.net/+crypto/aprende-criptografia-cifrado-de-verman-con-este-post_hrjd2>

<http://www.ugr.es/~esantos/flujo.html>

**Escítala**

<https://es.wikipedia.org/wiki/Esc%C3%ADtala>

<https://riunet.upv.es/bitstream/handle/10251/86454/YANG%20-%20Arqueolog%C3%ADa%20inform%C3%A1tica%3A%20la%20criptograf%C3%ADa%20cl%C3%A1sica%20con%20Scracth.pdf?sequence=1>

<https://es.slideshare.net/prof.2007/ejemplos-criptografia>

<https://fr.wikipedia.org/wiki/Scytale> <https://es.wikipedia.org/wiki/Esc%C3%ADtala#Transposici%C3%B3n_en_Criptograf%C3%ADa>

**Polybios**

<https://es.slideshare.net/prof.2007/ejemplos-criptografia>

**Enigma**

<https://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina)>

**Playfair**

<https://es.planetcalc.com/7751/>

<https://es.wikipedia.org/wiki/Cifrado_de_Playfair>

<https://en.wikipedia.org/wiki/Playfair_cipher>

**Hill**

<https://web.archive.org/web/20110719235517/http://w08.middlebury.edu/INTD1065A/Lectures/Hill%20Cipher%20Folder/Hill1.pdf>

<https://es.wikipedia.org/wiki/Cifrado_Hill>