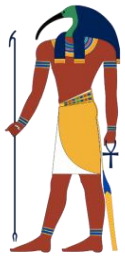
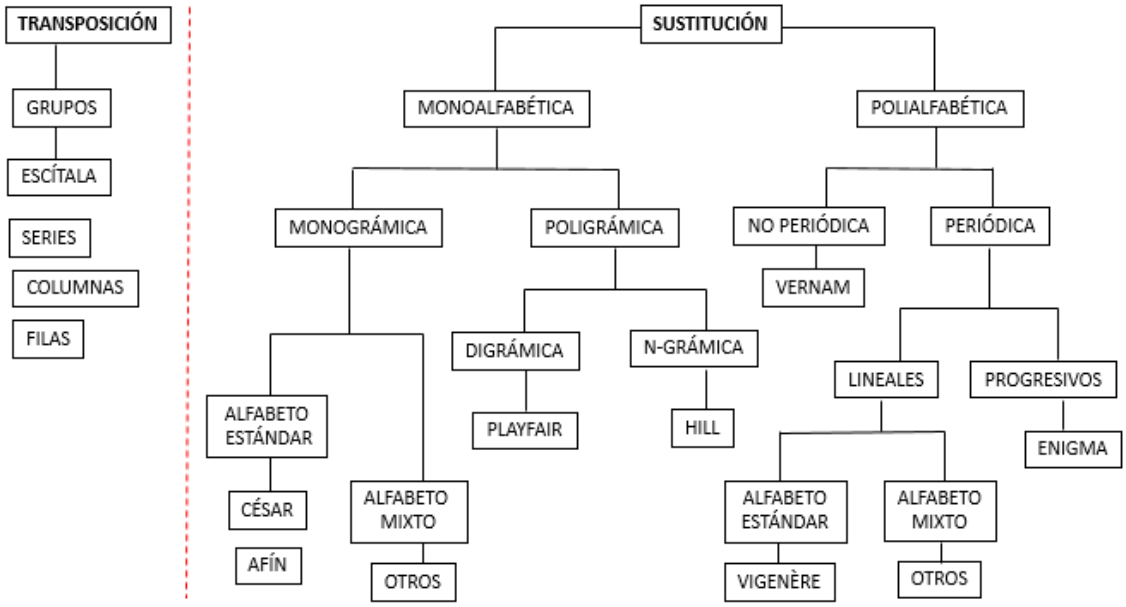


# Píldora nº 10: ¿Cómo se clasifican los sistemas de cifra clásica?

## Escena 1: Transposición y sustitución

La clasificación principal de los sistemas de cifra clásica atiende al tipo de operación que se realizará al texto en claro durante la cifra, bien sea la de transposición con el fin de lograr la difusión, o la de sustitución para lograr en este caso la confusión. La combinación de ambos métodos permitirá cifrados más resistentes al criptoanálisis. En la figura se muestran algunos sistemas de cifra representativos de las operaciones de transposición y sustitución y que se estudiarán en próximas píldoras.




## Escena 2: Algoritmos de cifra por transposición

En los algoritmos por transposición o permutación, las operaciones se realizan mediante grupos, series, columnas o filas. Estos sistemas no han experimentado un gran desarrollo y su importancia radica en que su uso en la cifra aumenta la seguridad de los algoritmos al difundir

las propiedades estadísticas del lenguaje. Un ejemplo clásico es la escítala ya vista en píldoras anteriores.

## Escena 3: Algoritmos de cifra por sustitución monoalfabética

La mayor diversidad la encontramos en los cifradores por sustitución, diferenciando entre la cifra monoalfabética, es decir sustitución mediante un único alfabeto de cifrado, y la cifra polialfabética, donde se usan dos o más alfabetos de cifrado. Hay que indicar que el alfabeto de cifra puede o no tener los mismos elementos que el alfabeto del texto en claro. En este segundo caso podrá incluir signos y diferentes objetos gráficos, como sucedía en el famoso libro El Escarabajo de Oro de Edgar Allan Poe.

En la cifra monoalfabética, como su nombre lo indica, se sustituye un elemento del texto en claro por un único elemento del alfabeto de cifrado. Podemos cifrar de manera monográmica, esto es letra a letra, o bien poligrámica usando un grupo de letras del mensaje. Así, en la sustitución monoalfabética monográmica, por ejemplo el texto en claro THOTH se podría cifrar como WKRWK. En cambio, en la sustitución monoalfabética poligrámica el mensaje THOTH podría cifrarse como tres digramas TH, OT y HX, añadiendo la letra X como relleno, dando lugar al criptograma QM QN KW. Algunos algoritmos muy conocidos de sustitución monoalfabética son el del César, la cifra afín, Playfair y las matrices de Hill.

## Escena 4: Algoritmos de cifra por sustitución polialfabética

Con respecto a los algoritmos de cifra polialfabética, estos se clasifican como no periódicos como el cifrador de Vernam, y periódicos, donde destacan la máquina Enigma y el cifrador de Vigenère. La periodicidad se refiere a la repetición o no de una clave durante el cifrado.

En la sustitución polialfabética monográmica, el mismo elemento del texto en claro puede sustituirse por varios elementos distintos del alfabeto de cifrado, en función de una clave. Así, el mensaje THOTH podría cifrarse como TISCH, NOULL o VLGWV si usamos como clave ABEJA, TIGRE o CERDO.

Madrid, septiembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*

creative commons
Attribution
Noncommercial
No derivative works