# Cifrado Plafair

El cifrado de Playfair es un método manual de [criptografía simétrica](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica) por medio de [sustitución](https://es.wikipedia.org/wiki/Cifrado_por_sustituci%C3%B3n) (unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular).

El sistema de [cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) toma pares de letras, o [diagramas](https://es.wikipedia.org/wiki/Bigrama), y las cambia mediante una tabla generada por una [clave](https://es.wikipedia.org/wiki/Clave_(criptograf%C3%ADa)).

### Creación de la matriz de cifrado

En esta sustitución, la clave viene dada por una tabla de 5x5 caracteres (sin las letras J ni Ñ). Para empezar, colocamos en la primera fila de la matriz la palabra clave sin letras repetidas.

Ejemplo:

Clave: NORIA

Matriz de cifrado resultante:

N O R I A

B C D E F

G H K L M

P Q S T U

V W X Y Z

### Cifrado de un texto

Reglas para cifrar dos caracteres **m1** y **m2**:

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.

Por ejemplo, en este texto en claro: AT AQ UE CE RO HO RA SX pondremos X al final, porque al tener el texto un número de letras impar, se requiere una letra sin significado, de relleno, para volver a la paridad. También podrían ponerse letras sin significado al final de cada palabra para evitar confusiones o hacer más claro el texto resultante.

[**Criptograma**](https://es.wikipedia.org/wiki/Criptograma)**resultante**: IU OU TF DF IR QC IN XR