# Criptosistema Playfair

Este sistema criptográfico fue inventado en 1854 por Charles Wheatstone, pero debe su nombre al Baron Playfair de St Andrews quien promovió el uso de este criptosistema.

El algoritmo utiliza una tabla o matriz de 5x5.

La tabla se llena con una palabra o frase secreta descartando las letras repetidas. Se rellenan los espacios de la tabla con las letras del alfabeto en orden. Usualmente se omite la "W" y se utiliza la "V" en su lugar o se reemplazan las "J" por "I". Esto se hace debido a que la tabla tiene 25 espacios y el alfabeto tiene 26 símbolos. La frase secreta usualmente se ingresa a la tabla de izquierda a derecha y arriba hacia abajo o en forma de espiral, pero puede utilizarse algún otro patrón. La frase secreta junto con las convenciones para llenar la tabla de 5x5 constituyen la clave de encriptación.

Por ejemplo:

Si la frase secreta es "CRIPTOSISTEMA PLAYFAIR"

Llenaremos de izquierda a derecha y arriba hacia abajo y omitiremos la W

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C | R | I | P | T |
| O | S | E | M | A |
| L | Y | F | B | D |
| G | H | J | K | N |
| Q | U | V | X | Z |

La encriptación se realiza de la siguiente forma:

El mensaje original que se desea encriptar es dividido en bloques de dos caracteres cada uno y se le aplican las siguientes cuatro reglas en orden:

1. Si en el bloque las dos letras son la misma, se reemplaza la segunda generalmente por una X (o alguna letra poco frecuente) y se encripta el nuevo par.

2. Si las dos letras del bloque aparecen en la misma fila de la tabla, cada una se reemplaza por la

letra adyacente que se encuentra a su derecha (si es la letra que se encuentra en la última posición a la derecha de la fila se la reemplaza con la primera de la izquierda de esa fila). Ej. SM se reemplazará por EA y AE por OM.

3. Si las dos letras del bloque aparecen en la misma columna de la tabla, cada una se reemplaza por la letra adyacente que se encuentra por debajo (si es la letra que se encuentra en la última posición inferior de la columna, se la reemplaza con la primera de arriba de esa columna). Ej. LC se reemplazará por GO y GQ por QC.

4. Si las letras no se encuentran en la misma fila ni columna, se determina el rectángulo formado por los dos caracteres y se encripta tomando los caracteres que están en las esquinas del rectángulo y en la misma fila que el carácter a encriptar. Ej. SB se reemplazará por MY y KR por HP.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C | R | I | P | T |
| O | S | E | M | A |
| L | Y | F | B | D |
| G | H | J | K | N |
| Q | U | V | X | Z |

Para desencriptar se aplican estas cuatro reglas en forma inversa, descartando las "X" que no tengan sentido en el mensaje final.

#### Ejemplo

Si queremos codificar "LENGUAJE"

1. Tomamos "LE" como no están ni en la misma fila ni columna se utiliza la regla 4, "LE" se

reemplaza por "FO".

2. Tomamos "NG" como están en la misma fila utilizamos la regla 2, "NG" se reemplaza por "GH".

3. Luego, tomamos "UA" como no están ni en la misma fila ni columna se utiliza la regla 4, "UA" se reemplaza por "ZS" .

4. Finalmente tomamos "JE" como están en la misma columna utilizamos la regla 3, "JE" se reemplaza por "VF".

Por lo tanto "LENGUAJE" se encriptará como "FOGHZSVF".

De este esquema podemos deducir que el sistema es polialfabético (por ejemplo "LE"="FO" implica que "E"="O" y "JE"="VF" implica que "E"="F"). En el sistema Playfair, si bien no es cierto que todo carácter siempre es encriptado en un mismo carácter, sí es cierto que todo par de caracteres es encriptado en el mismo par de caracteres (por lo que en lugar de decir que el sistema es polialfabético podemos decir que es monoalfabético de orden 2).

#### Criptoanálisis:

El sistema Playfair es un sistema de encriptación bastante bueno, la cantidad de posibles claves es enorme ya que son las permutaciones de 25 elementos tomados de entre 26 lo cual da un número muy grande como para derrotar al algoritmo por fuerza bruta. Además es un sistema polialfabético por lo que un análisis de la frecuencia de aparición de cada carácter en el código cifrado no nos aporta nada.

La técnica que se debe utilizar con el esquema Playfair consiste en analizar la frecuencia de aparición de los pares de letras (diagramas) y compararlas con los diagramas mas frecuentes del idioma en el cual se supone que se escribió el mensaje original. En castellano, los diagramas más probables son (ordenados por frecuencia):

ES,EN,EL,DE,LA,OS,AR,UE,RA,RE,ER,AS,ON,ST,AD,AL,OR,TA,CO

El criptoanalista deberá analizar cual es el diagrama mas ocurrente en el código cifrado y ver qué ocurre si se lo reemplaza por 'ES'. De esta forma se van probando distintas combinaciones entre los diagramas mas frecuentes en el mensaje cifrado y los diagramas más frecuentes del idioma hasta que se consigue descifrar el texto. Esta es una técnica muy habitual del criptoanálisis y suele funcionar muy bien.

Los sistemas monoalfabéticos de orden 'N' son vulnerables a este tipo de ataque. En general, todo criptoanalista esta preparado con programas específicos para analizar las frecuencias de aparición de caracteres individuales, diagramas, tetragramas, y compararlas con las frecuencias estadísticas de un determinado idioma. Los programas se encargan también de generar las pruebas necesarias y todo lo que tiene que hacer el criptoanalista es analizar si el texto que resulta de las pruebas tiene sentido.