Cifrado Playfair

Mejoras en el diseño de los criptosistemas

Las mejoras que se proponen tienen como objetivo evitar el ataque por análisis de frecuencias

Dos principales mejoras:

- Aumento del tamaño de los alfabetos utilizados
- Permitir que cifrar una misma letra de texto plano produzca como resultado diferentes letras de texto cifrado

Cifrado Playfair

Fue inventado en 1854 por Charles Wheatstone, pero lleva el nombre de Lyon Playfair por promover su uso

Opera en pares de letras (bigramas)

Características del cifrado Playfair:

- Simétrico
- Polialfabético
- Sustitución
- Confidencialidad

Cifrado Playfair | Funcionamiento

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