

Cifra de Vigenère

Talles Marcelo - 200060295



O que é?

- Cifra de substituição polialfabética
- Uso de uma palavra-chave, que é usada para determinar o deslocamento das letras no texto original.
- Cada letra da chave corresponde a um valor numérico que é usado para deslocar a letra correspondente no texto original.
- Para decifrar o texto cifrado de Vigenère, é necessário conhecer a chave correta, que permite reverter os deslocamentos aplicados às letras do texto original





Será que preciso da
chave?

- Ataque de frequência é uma técnica de criptoanálise usada para tentar quebrar cifras de substituição simples e cifras de substituição polialfabéticas
- Padrões de frequência de letras ou símbolos em um texto cifrado



Como funciona?

- Padrões de repetição de letras e símbolos na língua
- Busca por padrões recorrentes(grupos de letras)
- Para chaves muito grandes ou complexas o ataque de frequência pode não ser muito eficaz(devido aos diferentes deslocamentos usados para cada letra da chave)

