Relatório

Lógica do programa

Fazendo uso da repetição de chave criptográfica para cifrar uma mensagem usando o OTP podemos quebrar a cifra e obter os textos originais.

Sejam T_1, T_2, C_1, C_2 e K textos claros, cifrados e chave (nessa ordem).

$$C_1 \oplus C_2 = (T_1 \oplus K) \oplus (T_2 \oplus K) = T_1 \oplus T_2 \oplus K \oplus K = T_1 \oplus T_2$$

Mesmo assim o texto obtido não está claro e para acessá-lo precisamos de uma sequência de palpites para que possamos obter as duas mensagens, é possível usar um ataque de força bruta, mas dependendo do tamanho das mensagens isso pode levar muito tempo, tornando a análise humana uma melhor opção.

O programa itera os palpites pela *string* e retorna os resultados, alguns valores são descartados pelo programa por possuírem algum carácter que não seja letra, número, diacrítico ou ponto.