Exercício Prático 6

Implemente a Cifra de Vernam.

$$E_K(c_i) = m_i \oplus k_i, \qquad 1 \leq i \leq t$$

- Alfabeto Português incompleto $\mathcal{A} = \{\text{a-z}\}$.
- Cifração carácter a carácter.
- Chaves:
  - introdução de uma chave pelo utilizador.
  - Geração aleatória de uma chave única.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Algoritmo (cifrar/decifrar) em C (ou C++).
- Qual a forma de introdução de chaves é a mais segura? Porquê?