# Projecto Prático 3

Implemente a seguinte cifra produto.

## Cifra Produto

Sejam $\mathcal{M} = \mathcal{C} = \mathcal{K}$ o conjunto de todas as sequências binárias de elementos com 16 bits de comprimento (dois "bytes").

$$\begin{aligned} E_k^{(1)}(m) &= m \oplus k, \text{ aonde } k \in \mathcal{K}, \\ E^{(2)}(m) &= (m_{13}\, m_{14}\, m_{15}\, m_{16}\, m_9\, m_{10}\, m_{11}\, m_{12}\, m_5\, m_6\, m_7\, m_8\, m_1\, m_2\, m_3\, m_4). \end{aligned}$$

A cifra produto é dada por $E_k^{(1)}(E^{(2)}(m))$.

- Preenchimento não âmbiguo.
- Modo de operação ECB.
- Introdução de uma chave pelo utilizador.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação (cifrar/decifrar) em C++.

# Projecto Prático 3 — Ficheiros

## Ficheiros

| | |
|---|---|
| Makefile | Automatização dos procedimentos de compilação |
| msg.txt | *Mar Português*, Fernado Pessoa |
| cifrasProduto.hpp | Especificação da classe Cifras Produto |
| cifrasProduto.cpp | Implementação da classe Cifras Produto |
| encriptarProduto.cpp | Encriptar com cifra produto |
| desencriptarProduto.cpp | Desencriptar com cifra produto |