Projecto Prático 4

I — Implemente a cifra RSA.

- Preenchimento não âmbiguo; Modo de operação ECB.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação do algoritmo de Geração das chaves em *C++*.
- Implementação (cifrar/decifrar) em *C++*.

II — Implemente os ataques à cifra RSA: método das divisões, Fórmula Geradora, Método de Fermat.

- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação em *C++*.

Projecto Prático 4 — Ficheiros

Ficheiros

Makefile	Automatização dos procedimentos de compilação
msg.txt	*Mar Português*, Fernado Pessoa
cifraRSA.hpp	Especificação da classe Cifra RSA
cifraRSA.cpp	Implementação da classe Cifra RSA
gerarChavesRSA.cpp	Gerar as chaves RSA
encriptarRSA.cpp	Encriptar com cifra RSA
desencriptarRSA.cpp	Desencriptar com cifra RSA
quebrarRSA.cpp	Criptoanálise da cifra RSA com os métodos: divisões; fórmula $6k \pm 1$; Fermat.