

Projecto Prático 3

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 (ou C++).
- Implementação (cifrar/decifrar) em C (ou C++).
- Utilização da biblioteca de funções GMP como forma de implementar números inteiros de grande dimensão.

Apresente um relatório em que documente a sua implementação indicando os algoritmos que usou nas diferentes fases do programa e a forma como utilizou a biblioteca GMP para implementar os números inteiros de grande dimensão.