Exercício Prático 9

Implementação da Cifra de Chave Pública "Goldwasser-Micalli" [1].

1. A. Meneses, P. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

Notas:

- A implementação deve ser feita na linguagem C, recorrendo à biblioteca GMP para lidar com os números inteiros de grande dimensão.
- Podem (devem) usar as funções disponíveis na biblioteca GMP, nomeadamente as da secção "5.9 Number Theoretic Functions".