# Project 4: Cryptography

# Python Cryptography Toolkit (pycrypto) is a collection of both secure hash functions (such as SHA256 and RIPEMD160), and various encryption algorithms (AES, DES, RSA, ElGamal, etc.).

<https://pypi.python.org/pypi/pycrypto>

There are also other Python cryptographic libraries available. However, we are going to implement our own programs.

**Problem:** Implement (in Python) and test for very large numbers the following algorithms:

1. The Miller-Rabin primality test.
2. The Pollard-Rho integer factorization procedure.
3. Write a program to encrypt/decrypt an input number using the RSA public-key cryptosystem.
4. Write a program to break this code knowing only the RSA public key.
5. Encrypt a message and challenge your colleague to break the encryption code knowing only the RSA public key.