Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 3

Chinese Remainder Theorem and Rabin Encryption.

Problem 1. Suppose we are given two sets of positive integers: $\{n_1, \ldots, n_k\}$ and $\{a_1, \ldots, a_k\}$ such that the n_i are coprime: $gcd(n_i, n_j) = 1$ for all $i \neq j$. In this situation, the Chinese Remainder Theorem provides a solution to the simultaneous modular equations

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots, k.$$

The solutions x are found in three steps:

1. Compute $N = n_1 n_2 \cdots n_k$.
2. Compute the modular inverse $y_i = \dfrac{1}{N/n_i} \pmod{n_i}$.
3. One solution is $x = a_1 \dfrac{N}{n_1} y_1 + \ldots + a_k \dfrac{N}{n_k} y_k$. All other solutions are of the form $x + \lambda N$ for $\lambda \in \mathbb{Z}$, and the smallest is $x \pmod{N}$.

Answer the following questions:

i) Write a function to find x in Sage or Python. Use the code you used in the Lab List 1 to compute the modular inverse in step 2 above.

ii) Try your program for $\{n_1 = 19, n_2 = 18, n_3 = 17\}$ and $\{a_1 = 10, a_2 = 12, a_3 = 14\}$. Find the smallest positive x in this case.

Problem 2. Rabin encryption. The security of Rabin's cryptosystem is similar to RSA's and it relies on the hardness of factoring an integer which is the product of two primes.
Euler's criterion is needed to show the decryption function works. Euler's criterion says: an integer a not divisible by p is a square modulo the prime number p (so there is a solution to $a \equiv x^2 \pmod{p}$) if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Rabin's cryptosystem is basically the following set of algorithms:

key generation The private keys are two primes p, q satisfying

$$p \equiv 3 \pmod 4,\ q \equiv 3 \pmod 4.$$

The public key is

$$n = pq.$$

encryption To encrypt a message M one has to convert M into an integer $m < n$. Then the ciphertext is

$$c = m^2 \pmod n.$$

decryption To recover m from c one needs to know p and q. The idea is then to compute the square roots of c modulo p and also modulo q and then use the Chinese Remainder Theorem to find m. Specifically:

- Compute

$$m_p = c^{(p+1)/4} \pmod p,\ m_q = c^{(q+1)/4} \pmod q.$$

  These values are the square roots of c modulo p and modulo q by Euler's Criterion.

- Use the Extended Euclidean Algorithm to find y_p, y_q such that

$$y_p\, p + y_q\, q = 1.$$

- By the Chinese Remainder Theorem, the 4 roots of c modulo n are

$$\begin{aligned} m_1 &= y_p\, p\, m_q + y_q\, q\, m_p \pmod n, \\ m_2 &= n - m_1, \\ m_3 &= y_p\, p\, m_q - y_q\, q\, m_p \pmod n, \\ m_4 &= n - m_3. \end{aligned}$$

  The square root m we are looking for is one of m_1, m_2, m_3, m_4.

i) Write a function to encrypt and decrypt using this method.