Cryptanalysis (COMPGA18/COMPM068)
Public Key Exercises - Session 1

Christophe Petit & Lucky Onwuzurike - University College London

1 Finite Field Arithmetic

(i) Compute $4 + 3 \bmod 5$

(ii) Compute $7 \cdot 8 \bmod 11$

(iii) What is the characteristic of $\mathbb{F}_{11}$? What is the size of $\mathbb{F}_{11}$?

(iv) What is the characteristic of $\mathbb{F}_{16}$? What is the size of $\mathbb{F}_{16}$?

(v) Is $\mathbb{Z}_{10}$ a field?

(vi) Suppose we represent $\mathbb{F}_{16}$ as $\mathbb{F}_2[x]/(x^4 + x + 1)$. Compute $x \cdot (x^3 + 1)$ in $\mathbb{F}_{16}$.

2 Get Acquainted with Sage

Find Sage commands to answer the following questions:

(i) What are the factors of 28?

(ii) What is the gcd of 77 and 11?

(iii) What is $11^{-1} \bmod 60$?

(iv) Is 25364772882647739926677265277281665356972 1 a prime number?

(v) What are the prime divisors of 2005?

(vi) What is the next prime number after 2011?

(vii) Create two (2 x 2) vectors, and two matrices with sizes (3 x 1) and (1 x 3). Multiply each pair together.

3 RSA 3-moduli attack when $e = 3$

For $i \in \{1, 2, 3\}$, let (p_i, q_i) be an RSA secret key and let $n_i = p_i q_i$ be the corresponding public key. To save time in the encryption process, the exponent $e = 3$ is used in the public key.

(i) Why is $e = 3$ advantageous from an efficiency point of view?

(ii) Suppose that Alice encrypts the same message m using all three public keys. Show that it is possible to recover the message from the three ciphertexts.

(iii) Propose a solution to protect against this attack.

4 Computing a modular inverse with Euclid

Let p and q be two distinct primes.

(i) Show how to use the extended Euclidean algorithm to simultaneously compute $p^{-1} \bmod q$ and $q^{-1} \bmod p$.

(ii) What is the complexity of this approach in terms of bit operations?

(iii) Compute $11^{-1} \bmod 17$ using this method

5 Rational Approximation using Euclid

For a real number r and integers a and b, we say a/b is a rational approximation of r up to ϵ if $\left|r - \frac{a}{b}\right| < \epsilon$.

For any real number r, its **continued fraction representation** is a (possibly infinite) sequence of integers $[r_0; r_1, r_2, \ldots]$ such that

$$r = r_0 + \cfrac{1}{r_1 + \cfrac{1}{r_2 + \cfrac{1}{r_3 + \cfrac{1}{r_4 + \cdots}}}}$$

(i) If $r = \frac{a}{b}$, show that the continued fraction representation of r can be computed with Euclid's Algorithm on (a, b)

When r is not rational, the continued fraction will be infinite. The truncation up to the element r_k gives an approximation $\frac{p_k}{q_k}$ of r: it is indeed possible to show that

$$\left| r - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k^2}$$

(ii) Compute an optimal rational approximation of $\pi = \frac{p_k}{q_k}$ which is precise up to 0.001.

6 Compare two matrix multiplication algorithms

(i) Construct a function *myScalarProduct* that takes as input two vectors of same lengths over a finite field $\mathbb{F}_p$, and return their scalar product.

(ii) Use this function to construct a function *easyMultiplication* taking two square matrices over a finite field $\mathbb{F}_p$ and returning their product.

(iii) Construct a function *StrassenMul* implementing Strassen's algorithm to multiply matrices of sizes 2^k, where k is integer.

(iv) Test both your algorithms on random matrices of increasing sizes over $\mathbb{F}_p$, and compare your experimental timings with the theoretical complexity predictions. What is the maximum matrix size for which you can solve the problem in a week? in a month? in a year?