Fundamentals of Cryptography

Homework 3

Dr. Mohammad Dakhilalian

Fall 2023

Theory Part

Question 1

With the Euclidean algorithm, we finally have an efficient algorithm for finding the multiplicative inverse in Z_m that is much better than an exhaustive search. Find the inverses in Z_m of the following elements a modulo m:

1. $a = 7$, $m = 26$
2. $a = 19$, $m = 999$

Note that the inverses must again be elements in Z_m and that you can easily verify your answers.

Question 2

Verify that Euler's Theorem holds in Z_m, $m = 6, 9$, for all elements a for which $gcd(a, m) = 1$. Also verify that the theorem does not hold for elements a for which $gcd(a, m) \neq 1$.

Question 3

Using the basic form of Euclid's algorithm, compute the greatest common divisor of

1. 7469 and 2464
2. 2689 and 4001

For this problem use only a pocket calculator. Show every iteration step of Euclid's algorithm, i.e., don't write just the answer, which is only a number. Also, for every gcd, provide the chain of gcd computations, i.e.,

$$gcd(r_0, r_1) = gcd(r_1, r_2) = ...$$

Question 4

An RSA encryption scheme has the set-up parameters $p = 31$ and $q = 37$. The public key is $e = 17$. Decrypt the ciphertext $y = 2$ using the CRT(Chinese Remainder Theorem).

Question 5

In practice, the short exponents $e = 3, 17$ and $2^{16} + 1$ are widely used.

1. Why can't we use these three short exponents as values for the exponent d in applications where we want to accelerate decryption?
2. Suggest a minimum bit length for the exponent d and explain your answer.

Question 6

Assume p is a prime number and a is a positive integer, then prove the following expression:

$$\phi(p^a) = p^a - p^{a-1}$$

Question 7

Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA.

1. Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent? Justify your choice.
2. Compute the corresponding private key $K_{pr} = (p, q, d)$. Use the extended Euclidean algorithm for the inversion and point out every calculation step.

Programming Part

Question 8

Implement the Miller-Rabin Primality Test in your favorite programming language, then test 38200901201 for primality with $a = 2$ and $a = 3$.