

VE475

Introduction to Cryptography

Homework 2

Manuel — UM-JI (Summer 2021)

Non-programming exercises:

- Write in a neat and legible handwriting, or use \LaTeX
- Clearly explain the reasoning process
- Write in a complete style (subject, verb and object)

Programming exercises:

- Write a README file for each program
- Upload an archive with all the programs onto Canvas

Ex. 1 — Simple questions

1. Find the inverse of 17 modulo 101
2. Find all the solutions to $12x \equiv 28 \pmod{236}$.
3. Given a plaintext m modulo 31, its corresponding ciphertext is $c = m^7 \pmod{31}$. Explain how to decrypt the message.
4. Factor 4883 and 4369 into a product of primes.
5. Find all the primes p such that $\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{p}$ is not invertible.
6. Let p be a prime and a and b be two integers such that $ab \equiv 0 \pmod{p}$. Show that at least one of a and b is congruent to 0 mod p .
7. Compute 2^{2017} modulo 5, 13, and 31. What is $2^{2017} \pmod{2015}$?

Ex. 2 — Rabin cryptosystem

1. Research and explain how the Rabin cryptosystem works.
2. To implement decryption for the Rabin cryptosystem one decides to build a machine that does the following. When the device is given a number x , it computes the square root of $x \pmod{n}$. Since there usually are more than one, it chooses one at random. If one gets a meaningful message he assumes this is the correct result and otherwise input x again.
 - a) Explain why a meaningful message can be expected fairly soon
 - b) If Eve intercepts x , can she easily determine the original message?
 - c) Eve has stolen the device and plans to run some attacks on it. What type of attack should she run to recover the factorization of n . Explain the process.

Note: the computation of square roots mod n will be covered later, so there is no need to detail this part.

Ex. 3 — CRT

A group prepares for a parade. If they arrange in rows of three, one person is left over. If they line up four to a row, two are left over and if they try rows of five, three are left over. What are the two smallest possible number of people in the group?