Homework #3

Mathematical Foundations of Modern Cryptography

2 November 2022

Teacher: Andrei Golovanov pnqke

Deadline: Monday, 14th of November, 23:59 MSK (for MF MC 1.1)

Rules

- For each homework, you must get:
  - 5 points if you send your solution before deadline
  - 8 points if you send your solution after deadline.
- Notice that the tasks in a homework sum up to more than 10–13 points, so you are free to choose which tasks to solve.
- Instead of giving just the final answer, give an explanation of your solution. If you make a program for your solution, give your code.
- If you cannot solve it to the end but you are sure you are on a right way, write your thoughts down, it may give you some points.
- Plagiarism is not allowed!
- Send your solutions to your teacher in any of user-friendly formats. The teacher will give you feedback, and you will probably have to correct your errors or answer some questions in text messages.

Materials

Books

1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone *Handbook of Applied Cryptography*
    - ch. 2.4.3 Integers modulo n (Def. 2.134–Ex. 2.141)
    - ch. 2.4.5 The Legendre and Jacobi symbols
    - ch. 4.2 Probabilistic primality tests
    - ch. 8.7.1 Goldwasser-Micali probabilistic encryption
    - ch. 10.4.1 Overview of zero-knowledge concepts

Tasks

Task 1 Quadratic residues modulo p (3 points)

Let p be a prime number. Prove these theorems:

1.a (2 points) In $\mathbb{Z}_p^*$ there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p. In notation:

$$|Q_p| = |\overline{Q_p}| = \frac{p-1}{2}$$

1.b (1 point) Each quadratic residue $a \in \mathbb{Z}_p^*$ has exactly 2 square roots modulo p.

Task 2 Legendre and Jacobi Symbols (3 points)

Legendre symbol is a function which defined as follows. Let p be a prime number > 2. Then Legendre symbol is:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{when } a \vdots p \\ 1, & \text{when } a \text{ is a quadratic residue modulo } p \\ -1, & \text{when } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Don't mix up Legendre symbol $\left(\frac{a}{p}\right)$ with division of a over p in brackets! It is not!

There is also a Jacobi symbol, which is also a function. Let n be an odd integer. If n's canonical representation is:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

then Jacobi symbol is:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}$$

where $\left(\frac{a}{p_i}\right)$ is a Legendre symbol.

Note that Legendre symbol is a special case of Jacobi symbol.

There are some properties of These symbols, which you can find in the Handbook of Applied Cryptography (check materials for the homework). Also, you can find an algorithm for calculating Jacobi symbol.

2.a (1 point) Find Jacobi symbol:

1. $\left(\frac{8}{13}\right)$
2. $\left(\frac{9}{13}\right)$
3. $\left(\frac{14}{21}\right)$
4. $\left(\frac{15}{21}\right)$
5. $\left(\frac{100}{100}\right)$
6. $\left(\frac{290}{431}\right)$

2.b (2 points) The objective of this problem is to observe that $\left(\frac{a}{n}\right) = 1$ does not imply that a is a quadratic residue modulo n.

- For each element a in $\mathbb{Z}_n^*$, where $n = 5 \cdot 7 = 35$, find if it is a quadratic residue or quadratic non-residue.
- For each element a in $\mathbb{Z}_{35}^*$, find its Legendre symbols $\left(\frac{a}{5}\right)$ and $\left(\frac{a}{7}\right)$
- For each element a in $\mathbb{Z}_{35}^*$, find its Jacobi symbol $\left(\frac{a}{35}\right)$
- Find the elements which are not quadratic residues but have Jacobi symbol equal to 1.

Task 3 Goldwasser-Micali (4 points)

As you can see from task 2, when n is a composite integer and $\left(\frac{a}{n}\right) = 1$, then we don't know if a is a quadratic residue modulo n or not. Indeed, deciding if such a is a quadratic residue modulo n is considered a hard problem (quadratic reciprocity problem, QRP). When there is a hard problem, we can make a cryptosystem based on it!

Learn about Goldwasser-Micali probabilistic encryption scheme. I advise reading Handbook of Applied Cryptography (check materials for the homework).

There was a message M, which was transformed into its ASCII binary representation m. It turned out, the message M is 48-bit long. Then, m was encrypted into ciphertext c using Goldwasser-Micali encryption scheme. Decrypt M.

$$
\begin{aligned}
c = [\ & 218, \ 34, \ 194, \ 164, \ 220, \ 50, \ 237, \ 77, \\
& 68, \ 151, \ 135, \ 21, \ 101, \ 167, \ 196, \ 98, \\
& 196, \ 219, \ 89, \ 241, \ 16, \ 134, \ 240, \ 43, \\
& 36, \ 193, \ 37, \ 17, \ 184, \ 61, \ 81, \ 41, \\
& 81, \ 148, \ 18, \ 172, \ 193, \ 37, \ 203, \ 233, \\
& 244, \ 145, \ 18, \ 1, \ 121, \ 46, \ 18, \ 193 \ ]
\end{aligned}
$$

Public key: $(y, n) = (109, 247)$

Secret key: $(p, q) = (13, 19)$

Task 4 Primality tests: Fermat and Solovay-Strassen (6 points)

Implement these two primality tests in your favourite programming language:

- **(2 points)** Fermat's primality test
- **(4 points)** Solovay-Strassen primality test (Calculation of Legendre symbol must be written by yourself. Don't use libraries!)

Provide your code. Provide some examples of calculation.

Which primality test is more powerful?