Домашнее задание №3

Математические основы криптографии группа 1.2

14 Декабря 2022

Преподаватель: Дакуо Жан-Мишель Никодэмович @jeandakuo

Дедлайн: Среда, 28 Декабря, 18:40 по МСК

Правила

- За домашнее задание вы должны набрать:
  - 20 баллов, если отправляете домашнее задание вовремя;
  - 25 баллов, если отправляете домашнее задание после дедлайна.
- Ответы без решения не принимаются (код - тоже решение).
- Если вы не можете решить, но думаете, что на правильном пути, отправьте свои мысли, они могут помочь получить некоторое количество баллов.
- Плагиат - это плохо :c
- Высылайте в любом удобном для прочтения формате (PDF файл). Если отправить домашнее до дедлайна, то можно получить фидбэк и возможность исправить выявленные недочеты, что позволит набрать дополнительные баллы. **Домашнее задание высылайте на почту:**

  jeandakuo@mail.ru

Задания

Задание 1 Квадратичные вычеты по модулю p (3 балла).

Пусть p - это нечетное простое целое число. Докажите следующие теоремы:

1.a (2 балла) В группе $\mathbb{Z}_p^*$ существует ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов:

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

1.b (1 балл) Каждый квадратичный вычет $a \in \mathbb{Z}_p^*$ имеет ровно 2 корня по модулю p.

Задание 2 Символ Лежандра — Якоби — Кронекера (3 балла).

2.a (1 балл) Найдите символ Лежандра — Якоби — Кронекера:

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 балла) Символ Лежандра — Якоби — Кронекера $\left(\frac{a}{n}\right) = 1$ не гарантирует того что a будет квадратичным вычетом по модулю n.

- Для каждого элеента a in $\mathbb{Z}_n^*$, где $n = 5 \cdot 7 = 35$, найдите является ли он квадратичным вычетом или невычетом.
- Для каждого элемента a in $\mathbb{Z}_{35}^*$, Найдите символы Лежандра $\left(\frac{a}{5}\right)$ and $\left(\frac{a}{7}\right)$

- Для каждого элемента a in $\mathbb{Z}_{35}^*$, Найдите Символ Лежандра — Якоби — Кронекера $\left(\frac{a}{35}\right)$
- Найдите элементы которые не являются квадратичными вычетами, но имеют символ Лежандра — Якоби — Кронекера равный 1.

Задание 3 Криптосистема Гольдвассер — Микали (4 балла).

Задана криптосистема Гольдвассера — Микали

Сообщение M, которое было преобразовано в его двоичное представление в ASCII m. Длина сообщения M - 48 бит. Сообщение m зашифровали в c, используя криптосистема Гольдвассера — Микали. Расшифруйте M.

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

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

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

Задание 4 Тесты простоты: Ферма и Соловея-Штрассена (6 баллов).

Реализуйте тесты:

- **(2 балла)** Тест простоты Ферма.
- **(4 балла)** Тест Соловея-Штрассена (Вычисления символа Лежандра реализуйте сами, не используя библиотеки)

Предоставьте код и проверьте следующте числа:

1. 2455921
2. 134899510405807901072383429627628720821425287778688627092802 7
3. 322080889572919065053331882946267215349260779989681431623909060542697713321951535785434 17
4. 187352183548821691011603483206335175445058818164858663319391738204968363448068360508281259424187715890886535953552784918363483411492065298146682089072399770417002736809905920110596285867969468281189253753266702516831877840048790039143707155242781379638905777628244577304347346516648816743000444690876693475549
5. 411482053694408436626203894097575331763736396159120829209725307798091953819317408863704725757666061847735945600515243416861922837875630632076871634802128134649341322136729331485528591019303696377030321052209634833543165256926439895530466038788119594948068096484605588168550739535208662918659184588341879856 77

какой тест лучше?

Задание 5 Операции над полиномами. (4 балла, $\frac{1}{2}$ за каждое)

Решите упражнения. Все полиномы лежат в $\mathbb{Z}_2[x]$, что означает, что все коэффициенты из $\mathbb{Z}_2$.

1. **Сложение**. Для полиномов

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

найти $f(x) + g(x)$.

2. **Вычитание**. Для полиномов

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

найти $f(x) - g(x)$.

3. **Умножение**. Для полиномов

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

найти $f(x)g(x)$.

4. **Деление с остатком**. Для полиномов

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

найти частное $q(x)$ и остаток $r(x)$ для $f(x)/g(x)$.

5. **Факторизация**. Разложите на множители: $f(x) = x^3 + 1$

6. **Умножение по модулю полинома**.Для полиномов

$$f(x) = x^2 + x + 1$$

$$g(x) = x^3 + 1$$

$$h(x) = x^4 + x + 1$$

найти $f(x)g(x) \bmod h(x)$.

7. **GCD**. Для полиномов

$$f(x) = x^5 + x^4 + 1$$

$$g(x) = x^5 + x^2 + x + 1$$

найти $\gcd(f(x), g(x))$ (используя алгоритм Евклида для полиномов).

8. **Обратное**. Для полиномов

$$f(x) = x^7 + x^4 + x + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

найти $f^{-1}(x) \bmod g(x)$ (используя расширенный алгоритм Евклида для полиномов).

Задание 6 Кольцо или поле?. (5 баллов за все)

В этом задании вам необходимо понять является ли данное множество с 2мя определенными на нем операциями полем, или кольцом, или ни тем, ни другим. Для каждого кольца или поля покажите:

- какая из операций является сложением, а какая умножением
- нейтральные элементы по сложению и умножению
- порядок и характеристику
- если это кольцо, то коммутативно ли оно
- если это поле, то какова его группа по умножению

Задания:

(a) **($\frac{1}{2}$ балла)** Множество $\mathbb{Z}_n$ вычетов по модулю n, где n - целое > 1, по операциям:

- сложение по модулю n
- умножение по модулю n

(b) **($\frac{1}{2}$ балла)** Множество $\mathbb{Z}_p$ вычетов по модулю p, где p - простое, по операциям:

- сложение по модулю p
- умножение по модулю p

(c) **($\frac{1}{2}$ балла)** Множество $B = \{0, 1\}$ по операциям:

- $\oplus$ (логический XOR)
- $\vee$ (логическое ИЛИ)

(d) **($\frac{1}{2}$ балла)** Множество $B = \{0, 1\}$ по операциям:

- $\oplus$ (логический XOR)
- $\wedge$ (логическое И)

(e) **($\frac{1}{2}$ балла)** Множество $B_n = \{0, 1\}^n$ всех n-битных бинарных строк по операциям:

- $\oplus$ (побитовый XOR)
- $\wedge$ (побитовое И)

(f) **($\frac{1}{2}$ балла)** Множество $\mathbb{Z}[x]$ всех полиномов $a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$ (для любого целого k) с целыми коэффициентами $a_i \in \mathbb{Z}$ по операциям сложения и умножения.

(g) **($\frac{1}{2}$ балла)** Множество $\mathbb{Q}[x]$ всех полиномов с рациональными коэффициентами (по аналогии с предыдущим) по операциям сложения и умножения.

(h) **($\frac{3}{2}$ балла)** Это задание про 2 множества:

(1) Множество $\mathbb{C}$ комплексных чисел по операциям сложения и умножения.

(2) Множество $\mathbb{C} \setminus \{0\}$ ненулевых комплексных чисел по операциям:

- умножения
- возведение в степень

Задание 7 Построение $GF(p^m)$. (3 балла)

Найдите все элементы поля Галуа $GF(2^4)$ с примитивным полиномом $p(x) = x^4 + x^3 + 1$. Привидите каждый элемент в следующих формах:

- полиномиальное представление
- степень примитивного элемента x.

Задание 8 Разделение секрета. (5 балла)

В данном задании вам предстоит познакомится со схемой разделения секрета Шамира. Можете посмотреть видео на эту тему, или почитать главу 12.7 в книге "Handbook of Applied Cryptography"за авторством A. Menezes. Видео вдохновит вас, но книга скорее всего окажется более полезной.

Дана (4,2)-схема разделения секрета Шамира в поле $\mathbb{Z}_{13}$. Это означает, что всего есть 4 пользователя и только 2 из них должны собраться вместе, чтобы восстановить секрет.

Пользователи предъявили следующие тени:

$$(x_1, y_1) = (1, 10)$$
$$(x_2, y_2) = (2, 12)$$
$$(x_3, y_3) = (3, 8)$$
$$(x_4, y_4) = (4, 4)$$

Один из них пытается обмануть всех остальных, и для этого он изменил свое значение y_i, чтобы нарушить процесс восстановления секрета.

Ваша задача найти лжеца и правильно восстановить секрет.

(Но помните, мы работаем в поле $\mathbb{Z}_{13}$, а не $\mathbb{R}$)