Домашнее задание №1

Математические основы криптографии

16 Ноября 2022

Преподаватель: Дакуо Жан-Мишель Никодэмович @jeandakuo

Дедлайн: Понедельник, 28 Ноября, 23:59 по МСК

Правила

- За каждое домашнее задание вы должны набрать:
  - 10 очков, если отправляете домашнее задание вовремя;
  - 13 очков, 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 очки. **Задание высылайте на почту jeandakuo@mail.ru или в телеграм**

Задания

Задание 1 Модульная арифметика. (3 балла, $\frac{1}{12}$ за каждое задание).

Можете повторить следующие темы:

- деление с остатком

- арифметическое операции по модулю n
- НОД (Наибольший общий делитель)
- функция Эйлера и ее свойства
- мультипликативное обратное (приложил алгоритм поиска к сообщению (Расширенный алгоритм Евклида))

Пусть n целое число. Посчитайте:

1. $x \equiv 12 \bmod 5$
2. $x \equiv 12 \bmod 6$
3. $x \equiv -1 \bmod 13$
4. $x \equiv 119 \bmod 5$
5. $x \equiv -144 \bmod 7$
6. $x \equiv -656 \bmod 13$
7. $x \equiv 1000 \bmod 11$
8. $x \equiv 1234 \bmod 1$
9. $x \equiv 3n \bmod 3$
10. $x \equiv 2n + 1 \bmod 2$
11. $x \equiv 15n^4 + 9n^2 + 2 \bmod 3$
12. $x \equiv 9 + 4 \pmod{12}$
13. $x \equiv 3 + 9 \pmod{12}$
14. $x \equiv 7 + 8 \pmod{21}$
15. $x \equiv 7 - 8 \pmod{21}$
16. $x \equiv 3 - 10 \pmod{15}$
17. $x \equiv 10 - 3 \pmod{15}$
18. $x \equiv 7 \cdot 8 \pmod{15}$
19. $x \equiv 6 \cdot 10 \pmod{15}$
20. $x \equiv 14 \cdot 14 \pmod{15}$
21. $x \equiv 3^2 \pmod{15}$
22. $x \equiv 3^4 \pmod{15}$
23. $x \equiv 3^6 \pmod{7}$
24. $\gcd(56, 76)$
25. $\gcd(124, 0)$
26. $\gcd(999\,999, 1\,000\,000)$
27. $\gcd(35\,764, 30\,952)$
28. $\varphi(10)$
29. $\varphi(37)$
30. $\varphi(38)$

31. $\varphi(2^3 \cdot 7^1)$
32. $\varphi(2^{11})$
33. $\varphi(2^8 \cdot 3^4 \cdot 5^1 \cdot 7^2)$
34. $3^{-1} \pmod 5$
35. $8^{-1} \pmod 9$
36. $6^{-1} \pmod{12}$

где $n \in \mathbb{Z}$

Задание 2 Фундаментальная теорема номера ИСУ. (1 балл).

Найдите каноническую форму своего номера ИСУ.

Подсказка: Фундаментальная теорема арифметики.

Задание 3 Наименьшее общее кратное (1 балл).

Найдите НОК от вашего номера ИСУ и следующего по спику + 4 по модую {количество человек в группе + 1} :D

Задание 4 Алгоритм быстрого возведения в степень (1 балл).

Посчитайте:

$$17^{189} \bmod 200$$

Задание 5 Очумелые ручки (1 балл).

$$(1! + 2! + 3! + ... + 2022!) \bmod 8$$

Получите в 4 раза больше если решите ручками в тетради

Задание 6 Взлом RSA??? (5 баллов).

1. Необходимо прочитать и понять, как работает алгоритм шифрования RSA.

2. Далее Боб шифрует некоторое сообщение m и отправляет его Алисе. Помогите Еве узнать, какое сообщение было отправлено.

Открытый ключ Алисы(e, N):

$$e = 17$$

$$N = 29329$$

Секретное сообщение Боба c:

$$c = 16469$$

Ответ

Задание 7 Функция Кармайкла (4 points).

Как вы уже узнали, что иногда В RSA используют функцию Эйлера, а иногда функцию Кармайкла. Объясните почему тогда в стандарте алгоримта используется функция Камайкла?

Задание 8 Можно я покожу? (4 балла).

Реализуйте Расширенный алгоритм Евклида (PAE), используя любой язык программирования, например, Python.

Используя PAE, создайте программу, которая решает уравнение вида:

$$ax \equiv b \pmod{n},$$

где $a, b, n \in \mathbb{Z}$

Задание 9 Эль-Гамаль (4 балла).

Вам необходимо прочитать про схему шифрования Эль-Гамаля.

"Злые языки" говорят, что она произошла от идеи Диффи и Хелмана. Покажите, что у этих авторов общего.