

Контрольная работа  
по дисциплине  
**КРИПТОГРАФИЯ НА РЕШЕТКАХ**  
2021–2022

Время: 200 минут + 10 минут на скан и отправку  
24.05.2021

Имя :

Фамилия :

**Требования:**

- Решения можно записывать, либо используя этот темплейт, либо отдельные листы с четким указанием, к какому заданию относится решение. Первую страницу заполнять необязательно.
- Пишите **разборчиво**.
- Присыпать решения (желательно в файлах формата .pdf или .jreg **адекватного** размера) на почту [elenakirshanova@gmail.com](mailto:elenakirshanova@gmail.com)  
Решение задания №4 присыпать в формате **.sage**
- Время начала экзамена: **8:30**, ответы на почту принимаются строго до **12:00**.

---

Задание	1	2	3	4
Баллы	/ 6	/ 5	/ 5	/ 5

**Задание 1. Тривиальные задачки** ( $3 \times 2$  баллов)

1 Пусть решетка  $L \subset \mathbb{Z}^2$  задана как

$$L = \{v \in \mathbb{Z}^2 : v_1 + v_2 = 0 \bmod 2\}$$

Найдите кратчайший ненулевой вектор решетки  $L$  (в евклидовой норме).

2 Положим, для целого  $n \geq 1$  евклидова решетка  $L$  задана базисом  $5\text{Id}_n$ . Опишите ранг решетки, все её последовательные минимумы, а также базис  $\hat{L}$  – решетки, дуальнойной к  $L$ .

3 Положим, даны две матрицы  $B_1, B_2 \in \mathbb{Z}^{n \times n}$  ранга  $n$ . Как определить, порождают ли они одну и ту же решетку?

**Задание 2. Подрешетка в любой целой решетке** (5 баллов)

Докажите, что для любой целочисленной решетки  $L$  полного ранга справедливо  $\det(L) \cdot \mathbb{Z}^n \subseteq L$ .

**Задание 3. Легкая версия LWE** (5 баллов)

Пусть  $q = 2^\ell$ . Рассмотрим вариацию задачи LWE, в которой, вместо  $\vec{a} \leftarrow \mathbb{Z}_q^n$ , мы будем умножать фиксированное секретное значение (скаляр)  $s \in \mathbb{Z}_q$  на вектор-гаджет  $\vec{g} = [1, 2, 4, \dots, 2^{\ell-1}]$ . Иными словами, нам дано

$$(\vec{g}, \vec{b} = s \cdot \vec{g} + \vec{e} \bmod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n,$$

где  $e \in [-\frac{q}{4}, \frac{q}{4}]^n$  – вектор-ошибка. Покажите, как по данным значениям  $(\vec{g}, \vec{b})$ , можно эффективно найти  $s$ . Обобщите результат для гаджета-матрицы  $G = \text{Id}_n \otimes \vec{g} = \text{diag}(\vec{g}, \dots, \vec{g}) \in \mathbb{Z}_q^{n\ell \times n}$  и LWE выборки  $(G, \vec{b} = G\vec{s} + \vec{e} \bmod q)$ .

#### **Задание 4. На программирование. Взлом криптосистемы Меркля-Хэллмана (5 баллов)**

Криптосистема Меркля-Хэллмана [1] была благополучно взломана Ади Шамиром с помощью решеток в работе [2]. Из-за этого долгие годы решетки считались лишь методами взлома, а не основой для конструкций безопасных криптоалгоритмов. Ваша задача состоит в реализации атаки Шамира.

Начнем с описания криптосистемы. Для формирования секретного ключа нам понадобится определение сверхвозрастающей последовательности.

**Определение.** Сверхвозрастающая последовательность – список целых положительных чисел  $\mathbf{r} = (r_1, \dots, r_n)$ , таких, что

$$r_i > 2r_{i-1}, \quad 2 \leq i < n.$$

Из определения следует  $r_k > r_{k_1} + \dots + r_1$  для всех  $2 \leq k \leq n$ . Для сверхвозрастающей последовательности задача рюкзака решается тривиально: пусть дано  $S \in \mathbb{Z}$ , такое, что существует  $\mathbf{b} \in \{0, 1\}^n$ , для которого выполняется

$$S = \sum_{i=1}^n b_i r_i.$$

Эффективный алгоритм решения задачи о рюкзаке:

---

INPUT:

OUTPUT:

- 1:  $\mathbf{b} = \mathbf{0}$
  - 2: **for**  $i$  **do** from  $n$  down to 1
  - 3:     **if**  $S \geq r_i$  **then**
  - 4:          $b_i = 1$
  - 5:          $S = S - r_i$
- 

Функции генерации ключа KEYGEN, шифрования ENC и дешифрования DEC работают следующим образом. Публичный параметр системы – целое положительное  $n$ .

KEYGEN( $n$ ).

1. Сгенерировать сверхвозрастающую последовательность  $\mathbf{r}$
2. Выбрать  $A, q$ , такие, что  $q > r_n$  и  $\gcd(A, q) = 1$ .
3. Вычислить последовательность  $M_i = Ar_i \bmod q$
4.  $pk = \mathbf{M}$ ,  $sk = (A^{-1} \bmod q, q, \mathbf{r})$ .

ENC( $pk, \mathbf{m} \in \{0, 1\}^n$ ).

1.  $c = \sum_{i=1}^n M_i \mathbf{m}_i \in \mathbb{Z}$

DEC( $sk, c$ ).

1. Вычислить  $c' = c \cdot A^{-1} \bmod q$
2. С помощью эффективного алгоритма для задачи о рюкзаке, найти  $\mathbf{m}' \in \{0, 1\}^n$  для  $c' \in \mathbb{Z}, \mathbf{r}$ .

В корректности схемы вы можете убедиться самостоятельно. В безопасности убеждаться не смысла, так как сейчас мы увидим эффективный алгоритм дешифрования шифр-текста  $c$  без знания секретного ключа.

**Атака Шамира.** Шамир в [2] заметил, что из открытого ключа  $\mathbf{M}$  и шифр-текста  $c$  можно сформировать решетку, порожденную **строками** следующей матрицы размера  $(n + 1) \times (n + 1)$ :

$$B = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & M_1 \\ 0 & 2 & 0 & \dots & 0 & M_2 \\ 0 & 0 & 2 & \dots & 0 & M_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & 1 & c \end{pmatrix}$$

Заметьте, что если  $\mathbf{m}$  – открытый текст для шифр-текста  $c$  (то есть  $c = \sum_{i=1}^n M_i m_i$ ), то в решетке  $L(B)$  (порожденной строками  $B$ ), лежит вектор  $\mathbf{t} = (2m_1 - 1, 2m_2 - 1, 2m_1 - 1, 2m_n - 1, 0) \in \mathbb{Z}^{n+1}$ . Для бинарного  $\mathbf{m}$ , это короткий вектор в  $L(B)$ , который может быть (для большинства интересных параметров) найден с помощью алгоритма LLL.

**Задание:** реализовать атаку Шамира.

1. Со страницы курса скачать скрипт `merkle_hellman.sage`. В нем реализованы процедуры `KEYGEN`, `ENC`, `DEC`. Они даны для ознакомления того, как были сгенерированы тесты. Изменять и вызывать их не понадобится.
2. Изменять нужно функцию `attack()`. А именно, в ней должна быть реализована атака Шамира. Входные и выходные данные описаны в начале тела функции.
3. Проверить корректность реализации можно с помощью команды

```
sage -t merkle_hellman.sage
```

Так будут проверены три теста, представленные в теле программы. Задание считается выполненным, если программа проходит все тесты.

4. При отправке выполненного задания, нужно переименовать файл в свою фамилию, оставив при этом расширение, например `alisova.sage`.

## Список литературы

- [1] Ralph Merkle and Martin Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks*. IEEE Trans. Information Theory. 1978
- [2] Adi Shamir, *A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem*. CRYPTO. 1982