

Инструкция

1. В каждом варианте 9 заданий на любой вкус. Не выбирайте из одной секции больше одного задания.
2. Не надо решать все девять. Вес заданий в скобках, и больше 10 получить нельзя, увы.
3. Всегда указывайте номер варианта и номер задания.
4. Выбирайте вариант случайно, их всего шесть. Бросьте кубик, например. На [сайте](#) выбор происходит автоматически. Смешивать задания из разных вариантов нельзя.
5. Если вам требуется решить СЛАУ, то достаточно написать саму систему (или матрицу) и получившееся решение. Как вы его получили — не важно, но я рекомендую использовать <https://matrixcalc.org>. Аналогично с вычислениями по модулю m . Используйте любой калькулятор, например <https://planetcalc.com/8326/>. Главное напишите что вы считали и что получилось.
6. Не решайте задачи каким-то безумным перебором при помощи программ. Все они решаются вручную за вполне разумное время.

В случае каких-то вопросов свяжитесь со мной любым удобным способом: [tg](#), [vk](#), или даже почта: secret-sharing@sldr.xyz.

Темы заданий

- (n, n) -схема и булевы формулы
 - A1 (0.30): Восстановить секрет по простейшей (n, n) -схеме.
 - A2 (0.45): Разделить длинный секрет
 - A3 (0.70): Разделить секрет в соответствии с булевой формулой
- Схема Блэкли
 - B1 (0.30): Разделить секрет по схеме Блэкли.
 - B2 (0.45): Схема Блэкли реализована по википедии. Надо «взломать».
 - B3 (0.70): Один участник из пяти испортил свой секрет и называет не ту плоскость.
- Схема Шамира
 - C1 (0.30): Восстановить секрет по схеме Шамира
 - C2 (0.45): Выяснить четность секрета
 - C3 (0.70): Изменить своё значение так, чтобы повлиять на секрет определённым образом

Чтобы раскрыть вариант, кликните по заголовку.

▼ Вариант 1

Задание A1¹ (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 4$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 2 над кольцом \mathbb{Z}_{43}

Дано:

1. $s = 34x^2 + 19x + 4$
2. $v_1 = 37x^2 + 4x + 39$
3. $v_2 = 17x^2 + 35x + 3$
4. $v_4 = 28x^2 + 13x + 29$

Найти: v_3

Задание A2¹ (0.45)

Вам дана ASCII строка: `maths`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 4$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3¹ (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((d \vee a) \wedge b) \wedge ((c \vee b) \wedge d) \vee (b \vee c)$. Ваша задача — разделить секрет $s = 14$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание В1¹ (0.3)

1. Необходимо разделить секрет $s = 17, s \in \mathbb{Z}_{47}$ между 5 участниками так, чтобы любые 3 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 3 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание В2¹ (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $6x_1 + 0x_2 + 4x_3 = 0$
- $4x_1 + 6x_2 + 5x_3 = 3$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание В3¹ (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $30x_1 + 3x_2 = 33$
2. $38x_1 + 16x_2 = 8$
3. $33x_1 + 41x_2 = 31$
4. $38x_1 + 25x_2 = 23$
5. $22x_1 + 5x_2 = 36$

Задание C1¹ (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 6)$, $(2, 2)$, $(3, 0)$

Задание C2¹ (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{16} . Восстановить секрет могут 3 участников, но вам известны лишь 3 — 1 точка: $(2, 9)$, $(3, 9)$

Необходимо выяснить чётность секрета.

Задание C3¹ (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(1, 20)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{2, 3, 4\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 11. Какую точку вы должны назвать?

▼ Вариант 2

Задание A1² (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 4$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 4 над кольцом \mathbb{Z}_{37}

Дано:

1. $v_1 = 11x^4 + 26x^3 + x^2 + 4x + 26$
2. $v_2 = 8x^4 + 35x^3 + 15x^2 + 30x + 7$
3. $v_3 = 2x^4 + 20x^3 + 22x^2 + 26x + 36$
4. $v_4 = 5x^3 + 23x^2 + 17x + 28$

Найти: s

Задание A2² (0.45)

Вам дана ASCII строка: `ba/cs`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 5$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3² (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((d \vee a) \vee (b \wedge d)) \wedge ((c \vee b) \wedge d)$. Ваша задача — разделить секрет $s = 31$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание В1² (0.3)

1. Необходимо разделить секрет $s = 14, s \in \mathbb{Z}_{29}$ между 5 участниками так, чтобы любые 4 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 4 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание В2² (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $3x_1 + 4x_2 + 4x_3 = 6$
- $3x_1 + 4x_2 + 5x_3 = 2$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание В3² (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $3x_1 + 17x_2 = 21$
2. $8x_1 + 19x_2 = 0$
3. $18x_1 + 13x_2 = 20$
4. $16x_1 + 23x_2 = 8$
5. $8x_1 + 7x_2 = 25$

Задание C1² (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 10)$, $(2, 4)$, $(3, 3)$

Задание C2² (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{256} . Восстановить секрет могут 3 участников, но вам известны лишь 3 — 1 точка: $(2, 240)$, $(3, 189)$

Необходимо выяснить чётность секрета.

Задание C3² (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(3, 40)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{1, 2, 4\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 34. Какую точку вы должны назвать?

▼ Вариант 3

Задание A1³ (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 4$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 2 над кольцом \mathbb{Z}_{37}

Дано:

1. $s = 6x^2 + 10x + 20$
2. $v_1 = 14x^2 + 32x + 6$
3. $v_2 = 27x^2 + 22x + 34$
4. $v_4 = 10x^2 + 5x + 6$

Найти: v_3

Задание A2³ (0.45)

Вам дана ASCII строка: `C#>Java`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 3$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3³ (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((a \vee c) \vee ((b \wedge d) \vee c)) \wedge (b \wedge a)$. Ваша задача — разделить секрет $s = 12$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание В1³ (0.3)

1. Необходимо разделить секрет $s = 11$, $s \in \mathbb{Z}_{13}$ между 5 участниками так, чтобы любые 4 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 4 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание В2³ (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $0x_1 + 3x_2 + 3x_3 = 5$
- $3x_1 + 6x_2 + 2x_3 = 4$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание В3³ (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $6x_1 + 19x_2 = 25$
2. $26x_1 + 20x_2 = 10$
3. $6x_1 + 11x_2 = 21$
4. $6x_1 + 1x_2 = 16$
5. $9x_1 + 9x_2 = 19$

Задание C1³ (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 12)$, $(2, 7)$, $(3, 12)$

Задание C2³ (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{16} . Восстановить секрет могут 3 участника, но вам известны лишь 3 — 1 точка: $(2, 11)$, $(3, 14)$

Необходимо выяснить чётность секрета.

Задание C3³ (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(1, 10)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{2, 3, 4\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 2. Какую точку вы должны назвать?

▼ Вариант 4

Задание A1⁴ (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 3$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 2 над кольцом \mathbb{Z}_{19}

Дано:

1. $s = 3x^2 + 18x + 15$
2. $v_2 = 16x^2 + 5x$
3. $v_3 = 9x^2 + 12x + 11$

Найти: v_1

Задание A2⁴ (0.45)

Вам дана ASCII строка: `CS HSE`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 4$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3⁴ (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((c \vee a) \vee (b \wedge d)) \wedge ((a \vee d) \wedge b)$. Ваша задача — разделить секрет $s = 4$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание B1⁴ (0.3)

1. Необходимо разделить секрет $s = 24$, $s \in \mathbb{Z}_{47}$ между 4 участниками так, чтобы любые 4 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 4 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание B2⁴ (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $0x_1 + 0x_2 + 4x_3 = 5$
- $5x_1 + 3x_2 + 0x_3 = 2$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание B3⁴ (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $8x_1 + 19x_2 = 10$
2. $31x_1 + 22x_2 = 17$
3. $11x_1 + 15x_2 = 16$
4. $22x_1 + 8x_2 = 14$
5. $4x_1 + 6x_2 = 24$

Задание C1⁴ (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 11)$, $(2, 5)$, $(3, 7)$

Задание C2⁴ (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{256} . Восстановить секрет могут 3 участников, но вам известны лишь 3 — 1 точка: $(2, 64)$, $(3, 253)$

Необходимо выяснить чётность секрета.

Задание C3⁴ (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(4, 6)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{1, 2, 3\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 40. Какую точку вы должны назвать?

▼ Вариант 5

Задание A1⁵ (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 3$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 3 над кольцом \mathbb{Z}_{11}

Дано:

1. $s = 9x^3 + 3x^2 + 6x + 9$
2. $v_2 = 9x^3 + x^2 + 5x + 7$
3. $v_3 = 5x^3 + 2x^2 + 4x + 8$

Найти: v_1

Задание A2⁵ (0.45)

Вам дана ASCII строка: `crypto`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 4$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3⁵ (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((d \vee c) \vee ((d \wedge a) \vee b)) \wedge (d \wedge c)$. Ваша задача — разделить секрет $s = 29$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание B1⁵ (0.3)

1. Необходимо разделить секрет $s = 10, s \in \mathbb{Z}_{11}$ между 5 участниками так, чтобы любые 4 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 4 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание B2⁵ (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $3x_1 + 6x_2 + 2x_3 = 0$
- $1x_1 + 0x_2 + 6x_3 = 1$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание B3⁵ (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $36x_1 + 2x_2 = 26$
2. $20x_1 + 34x_2 = 35$
3. $24x_1 + 1x_2 = 0$
4. $8x_1 + 28x_2 = 8$
5. $18x_1 + 11x_2 = 6$

Задание C1⁵ (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 12)$, $(2, 0)$, $(3, 8)$

Задание C2⁵ (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{256} . Восстановить секрет могут 3 участников, но вам известны лишь 3 — 1 точка: $(2, 177)$, $(3, 40)$

Необходимо выяснить чётность секрета.

Задание C3⁵ (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(4, 21)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{1, 2, 3\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 10. Какую точку вы должны назвать?

▼ Вариант 6

Задание A1⁶ (0.3)

Секрет разделён при помощи простейшей (n, n) -схемы, $n = 3$. Необходимо восстановить недостающую информацию. В качестве группы используется кольцо многочленов степени не выше 2 над кольцом \mathbb{Z}_{29}

Дано:

1. $v_1 = 3x^2 + 6x + 10$
2. $v_2 = 3x^2 + 20x + 1$
3. $v_3 = 4x^2 + 25x + 27$

Найти: s

Задание A2⁶ (0.45)

Вам дана ASCII строка: `Botay`. Необходимо её при помощи простейшей (n, n) схемы разделить между $n = 5$ участниками.

Использовать для вычислений модуль более 10000 не допускается.

Выпишите какой набор чисел получит каждый из участников.

Задание A3⁶ (0.7)

Есть четыре участника: a, b, c, d . Вам дана булева формула $((d \vee c) \wedge (a \wedge c)) \vee (a \vee b)$. Ваша задача — разделить секрет $s = 31$ при помощи простейшей (n, n) -схемы над полем \mathbb{Z}_{47} таким образом, чтобы его могли восстановить тогда и только тогда, когда эта функция, будучи применена к присутствующим участникам, принимает значение истины.

Необходимо описать какие числа получит каждый из участников и описать как происходит восстановление секрета.

Задание B1⁶ (0.3)

1. Необходимо разделить секрет $s = 12$, $s \in \mathbb{Z}_{13}$ между 5 участниками так, чтобы любые 3 могли его восстановить. Выпишите, что каждый участник знает.
2. Затем выбрать любых 3 участников и восстановить секрет обратно.

Нужно использовать схему Блэкли.

Задание B2⁶ (0.45)

Человек по неосторожности реализовал схему Блэкли, описанную на [криптовики](#). От схемы из презентации она отличается тем, что секрет распределяется между всеми координатами секретной точки. Засчёт этого, говорится, схема идеальна.

Для вычислений использовалось поле \mathbb{Z}_7 .

В схеме секрет разделяется так, что лишь трое могут его восстановить. Вам даны две плоскости:

- $5x_1 + 6x_2 + 2x_3 = 4$
- $2x_1 + 4x_2 + 2x_3 = 6$

Необходимо перечислить все 7 точек, в которых может находиться секрет.

Задание B3⁶ (0.7)

Секрет при помощи схемы Блэкли разделили между пятью участниками таким образом, что любые двое его могут восстановить. Однако **ровно один** из участников испортил свою долю, причём неизвестно кто. Необходимо восстановить секрет и определить участника с некорректной долей.

Участники назвали следующие гиперплоскости:

1. $13x_1 + 17x_2 = 3$
2. $5x_1 + 13x_2 = 1$
3. $26x_1 + 12x_2 = 17$
4. $13x_1 + 20x_2 = 16$
5. $23x_1 + 8x_2 = 13$

Задание C1⁶ (0.3)

Секрет разделили при помощи схемы Шамира над полем \mathbb{Z}_{13} . Нужно его восстановить.

Даны следующие точки: $(1, 7)$, $(2, 8)$, $(3, 3)$

Задание C2⁶ (0.45)

Для реализации схемы Шамира в качестве поля взяли \mathbb{Z}_{32} . Восстановить секрет могут 3 участников, но вам известны лишь 3 — 1 точка: $(1, 13)$, $(2, 2)$, $(3, 23)$

Необходимо выяснить чётность секрета.

Задание C3⁶ (0.7)

При помощи схемы Шамира был разделён секрет. Вам, как участнику схемы, досталась точка $(1, 16)$. Точки других участников вы точно не знаете, но уверены, что они имеют $x \in \{2, 3, 4\}$.

Необходимо, чтобы в результате восстановления значение секрета изменилось на 30. Какую точку вы должны назвать?