Ответы и решения

View on GitHub

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 A1[1] (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 4$. Необходимо его восстановить. В качестве поля 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

Ответ: $v_3 = 38x^2 + 10x + 19$

Задание A2[1] (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.

Авторское решение: Переведём строку в байты по таблице ASCII: $[109, 97, 116, 104, 115]$.

Теперь разделим: $\begin{pmatrix} 53 & 242 & 238 & 140 & 27 \\ 24 & 219 & 218 & 14 & 218 \\ 2 & 196 & 65 & 3 & 21 \\ 30 & 208 & 107 & 203 & 105 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

Задание A3[1] (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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_4 = 20$
- Участник b знает: $s_1 = 2$, $s_6 = 32$, $s_7 = 25$
- Участник c знает: $s_5 = 17$, $s_8 = 34$
- Участник d знает: $s_3 = 29$, $s_1 = 2$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s_1 = s_5 + s_6$
- $s_2 = s_7 + s_8$

И тогда: $s_1 = 2$, $s_2 = 12$, $s_3 = 29$, $s_4 = 20$, $s_5 = 17$, $s_6 = 32$, $s_7 = 25$, $s_8 = 34$

Задание B1[1] (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.

Авторское решение:

Секрет поместим в точку $(17,\ 11,\ 23)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 46 & 37 & 12 \end{pmatrix} \vec{x} = 8$
2. $\begin{pmatrix} 25 & 10 & 16 \end{pmatrix} \vec{x} = 10$
3. $\begin{pmatrix} 39 & 2 & 31 \end{pmatrix} \vec{x} = 35$
4. $\begin{pmatrix} 43 & 29 & 40 \end{pmatrix} \vec{x} = 43$
5. $\begin{pmatrix} 12 & 31 & 28 \end{pmatrix} \vec{x} = 14$

Тогда каждый участник обладает следующим набором чисел:

1. $[46, 37, 12, 8]$
2. $[25, 10, 16, 10]$
3. $[39, 2, 31, 35]$
4. $[43, 29, 40, 43]$
5. $[12, 31, 28, 14]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты.

$$\begin{pmatrix} 12 & 31 & 28 \\ 46 & 37 & 12 \\ 25 & 10 & 16 \end{pmatrix} \vec{x} = \begin{pmatrix} 14 \\ 8 \\ 10 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 17 \\ 11 \\ 23 \end{pmatrix} \implies s = 17$$

Задание B2[1] (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 6 & 0 & 4 \\ 4 & 6 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 6 \\ 4 \\ 5 \end{pmatrix} \right]$

Задание B3[1] (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 определеить 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. $22x_1 + 5x_2 = 36$

Для вычислений использовалось поле $\mathbb{Z}_{43}$

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\begin{pmatrix} 30 & 3 \\ 38 & 16 \end{pmatrix} \vec{x} = \begin{pmatrix} 33 \\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 19 \\ 36 \end{pmatrix} \implies s = 19$
2. 1 и 3: $\begin{pmatrix} 30 & 3 \\ 33 & 41 \end{pmatrix} \vec{x} = \begin{pmatrix} 33 \\ 31 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \implies s = 1$
3. 1 и 4: $\begin{pmatrix} 30 & 3 \\ 38 & 25 \end{pmatrix} \vec{x} = \begin{pmatrix} 33 \\ 23 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 34 \end{pmatrix} \implies s = 2$
4. 1 и 5: $\begin{pmatrix} 30 & 3 \\ 22 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 33 \\ 36 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 36 \\ 38 \end{pmatrix} \implies s = 36$
5. 2 и 3: $\begin{pmatrix} 38 & 16 \\ 33 & 41 \end{pmatrix} \vec{x} = \begin{pmatrix} 8 \\ 31 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$
6. 2 и 4: $\begin{pmatrix} 38 & 16 \\ 38 & 25 \end{pmatrix} \vec{x} = \begin{pmatrix} 8 \\ 23 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$
7. 2 и 5: $\begin{pmatrix} 38 & 16 \\ 22 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 8 \\ 36 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$
8. 3 и 4: $\begin{pmatrix} 33 & 41 \\ 38 & 25 \end{pmatrix} \vec{x} = \begin{pmatrix} 31 \\ 23 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$
9. 3 и 5: $\begin{pmatrix} 33 & 41 \\ 22 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 31 \\ 36 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$
10. 4 и 5: $\begin{pmatrix} 38 & 25 \\ 22 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 23 \\ 36 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 41 \\ 16 \end{pmatrix} \implies s = 41$

Теперь заметим, что $s = 41$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №1

Задание C1[1] (0.3)

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

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

Ответ: $s = 12$, причём $f(x) = x^2 + 6x + 12$

Задание C2[1] (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.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 9 \\ 9 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} 9 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$

Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет нечётен

P.S. Секрет был $s = 5$

Задание C3[1] (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?

Решение:

Проведём многочлен через точки $[(2, 0), (3, 0), (4, 0), (0, 11)]$: в нуле равен 11, в точках остальных участников равен нулю. Получим многочлен $12x^3 + 7x^2 + 13x + 11$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 1$; там он равен 20.

Теперь прибавим это к известному выданному y и получим $y' = 20 + 20 = 17$.

Значит нужно назвать точку $(1, 17)$

P.S. **Процесс восстановления**:

Через точки $[(1, 20), (2, 19), (3, 0), (4, 21)]$ проходит $f(x) = 2x^3 + 2x^2 + 2x + 14$

Но в результате атаки через $[(1, 17), (2, 19), (3, 0), (4, 21)]$ был проведён $f'(x) = 14x^3 + 9x^2 + 15x + 2$.

Получили: $s = f(0) = 14$ и $s = f'(0) = 2$, что и требовалось

Вариант 2

Задание A1² (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 4$. Необходимо его восстановить. В качестве поля 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

Ответ: $s = 21x^4 + 12x^3 + 24x^2 + 3x + 23$

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.

Авторское решение: Переведём строку в байты по таблице ASCII: $[98, 97, 47, 99, 115]$.

Теперь разделим: $\begin{pmatrix} 12 & 32 & 126 & 140 & 141 \\ 77 & 56 & 151 & 250 & 95 \\ 41 & 206 & 41 & 123 & 214 \\ 230 & 212 & 129 & 165 & 73 \\ 250 & 103 & 112 & 189 & 104 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_4 = 17$
- Участник b знает: $s_2 = 3$, $s_6 = 16$
- Участник c знает: $s_5 = 15$
- Участник d знает: $s_3 = 11$, $s_2 = 3$, $s = 31$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s = s_5 + s_6$

И тогда: $s_1 = 28$, $s_2 = 3$, $s_3 = 11$, $s_4 = 17$, $s_5 = 15$, $s_6 = 16$

Задание B1[2] (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.

Авторское решение:

Секрет поместим в точку $(14,\ 15,\ 14,\ 20)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 27 & 18 & 11 & 11 \end{pmatrix} \vec{x} = 7$
2. $\begin{pmatrix} 22 & 5 & 13 & 11 \end{pmatrix} \vec{x} = 2$
3. $\begin{pmatrix} 21 & 0 & 22 & 16 \end{pmatrix} \vec{x} = 23$
4. $\begin{pmatrix} 18 & 10 & 2 & 18 \end{pmatrix} \vec{x} = 7$
5. $\begin{pmatrix} 4 & 9 & 26 & 11 \end{pmatrix} \vec{x} = 21$

Тогда каждый участник обладает следующим набором чисел:

1. $[27, 18, 11, 11, 7]$
2. $[22, 5, 13, 11, 2]$
3. $[21, 0, 22, 16, 23]$
4. $[18, 10, 2, 18, 7]$
5. $[4, 9, 26, 11, 21]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты. $\begin{pmatrix} 22 & 5 & 13 & 11 \\ 18 & 10 & 2 & 18 \\ 21 & 0 & 22 & 16 \\ 27 & 18 & 11 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 2 \\ 7 \\ 23 \\ 7 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 14 \\ 15 \\ 14 \\ 20 \end{pmatrix} \implies s = 14$

Задание B2² (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 3 & 4 & 4 \\ 3 & 4 & 5 \end{pmatrix} \vec{x} = \begin{pmatrix} 6 \\ 2 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 5 \\ 0 \\ 3 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 5 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 6 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 6 \\ 3 \end{pmatrix} \right]$

Задание B3² (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 определеить 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. $8x_1 + 7x_2 = 25$

Для вычислений использовалось поле $\mathbb{Z}_{31}$

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\begin{pmatrix} 3 & 17 \\ 8 & 19 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 0 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 13 \\ 19 \end{pmatrix} \implies s = 13$
2. 1 и 3: $\begin{pmatrix} 3 & 17 \\ 18 & 13 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 20 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 28 \\ 20 \end{pmatrix} \implies s = 28$
3. 1 и 4: $\begin{pmatrix} 3 & 17 \\ 16 & 23 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 27 \\ 22 \end{pmatrix} \implies s = 27$
4. 1 и 5: $\begin{pmatrix} 3 & 17 \\ 8 & 7 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 25 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 7 \\ 0 \end{pmatrix} \implies s = 7$
5. 2 и 3: $\begin{pmatrix} 8 & 19 \\ 18 & 13 \end{pmatrix} \vec{x} = \begin{pmatrix} 0 \\ 20 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$
6. 2 и 4: $\begin{pmatrix} 8 & 19 \\ 16 & 23 \end{pmatrix} \vec{x} = \begin{pmatrix} 0 \\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$
7. 2 и 5: $\begin{pmatrix} 8 & 19 \\ 8 & 7 \end{pmatrix} \vec{x} = \begin{pmatrix} 0 \\ 25 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$
8. 3 и 4: $\begin{pmatrix} 18 & 13 \\ 16 & 23 \end{pmatrix} \vec{x} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$
9. 3 и 5: $\begin{pmatrix} 18 & 13 \\ 8 & 7 \end{pmatrix} \vec{x} = \begin{pmatrix} 20 \\ 25 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$
10. 4 и 5: $\begin{pmatrix} 16 & 23 \\ 8 & 7 \end{pmatrix} \vec{x} = \begin{pmatrix} 8 \\ 25 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \implies s = 24$

Теперь заметим, что $s = 24$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №1

Задание C1[2] (0.3)

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

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

Ответ: $s = 8$, причём $f(x) = 9x^2 + 6x + 8$

Задание C2[2] (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.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 240 \\ 189 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} 342 \\ -51 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$ Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет чётен

P.S. Секрет был $s = 140$

Задание C3[2] (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?

Решение:

Проведём многочлен через точки $[(1, 0), (2, 0), (4, 0), (0, 34)]$: в нуле равен 34, в точках остальных участников равен нулю. Получим многочлен $31x^3 + 18x^2 + 11x + 34$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 3$; там он равен 32.

Теперь прибавим это к известному выданному y и получим $y' = 40 + 32 = 25$.

Значит нужно назвать точку $(3, 25)$

P.S. **Процесс восстановления**:

Через точки $[(1, 2), (2, 30), (3, 40), (4, 28)]$ проходит $f(x) = 15x^3 + 42x^2 + 32x + 7$

Но в результате атаки через $[(1, 2), (2, 30), (3, 25), (4, 28)]$ был проведён $f'(x) = 46x^3 + 13x^2 + 43x + 41$.

Получили: $s = f(0) = 7$ и $s = f'(0) = 41$, что и требовалось

Вариант 3

Задание A1[3] (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 4$. Необходимо его восстановить. В качестве поля 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

Ответ: $v_3 = 29x^2 + 25x + 11$

Задание A2[3] (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.

Авторское решение: Переведём строку в байты по таблице ASCII:
$[67, 35, 62, 74, 97, 118, 97]$.

Теперь разделим: $\begin{pmatrix} 141 & 197 & 49 & 88 & 132 & 229 & 50 \\ 36 & 155 & 7 & 237 & 193 & 164 & 230 \\ 146 & 195 & 6 & 5 & 28 & 237 & 73 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

Задание A3[3] (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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_3 = 12$, $s = 12$
- Участник b знает: $s_5 = 31$, $s = 12$
- Участник c знает: $s_4 = 35$, $s_6 = 28$
- Участник d знает: $s_5 = 31$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s_2 = s_5 + s_6$

И тогда:$s_1 = 0$, $s_2 = 12$, $s_3 = 12$, $s_4 = 35$, $s_5 = 31$, $s_6 = 28$

Задание B1[3] (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.

Авторское решение:

Секрет поместим в точку $(11,\ 2,\ 3,\ 0)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 2 & 0 & 12 & 6 \end{pmatrix} \vec{x} = 6$
2. $\begin{pmatrix} 12 & 5 & 4 & 9 \end{pmatrix} \vec{x} = 11$
3. $\begin{pmatrix} 9 & 2 & 6 & 2 \end{pmatrix} \vec{x} = 4$
4. $\begin{pmatrix} 10 & 7 & 7 & 8 \end{pmatrix} \vec{x} = 2$
5. $\begin{pmatrix} 8 & 6 & 10 & 2 \end{pmatrix} \vec{x} = 0$

Тогда каждый участник обладает следующим набором чисел:

1. $[2, 0, 12, 6, 6]$

2. $[12, 5, 4, 9, 11]$
3. $[9, 2, 6, 2, 4]$
4. $[10, 7, 7, 8, 2]$
5. $[8, 6, 10, 2, 0]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты. $\begin{pmatrix} 9 & 2 & 6 & 2 \\ 10 & 7 & 7 & 8 \\ 8 & 6 & 10 & 2 \\ 2 & 0 & 12 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 4 \\ 2 \\ 0 \\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 11 \\ 2 \\ 3 \\ 0 \end{pmatrix} \implies s = 11$

Задание B2[3] (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 0 & 3 & 3 \\ 3 & 6 & 2 \end{pmatrix} \vec{x} = \begin{pmatrix} 5 \\ 4 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 5 \\ 4 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 6 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 5 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix} \right]$

Задание B3[3] (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 определеить 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. $9x_1 + 9x_2 = 19$

Для вычислений использовалось поле $\mathbb{Z}_{31}$

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\begin{pmatrix} 6 & 19 \\ 26 & 20 \end{pmatrix} \vec{x} = \begin{pmatrix} 25 \\ 10 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
2. 1 и 3: $\begin{pmatrix} 6 & 19 \\ 6 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 25 \\ 21 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
3. 1 и 4: $\begin{pmatrix} 6 & 19 \\ 6 & 1 \end{pmatrix} \vec{x} = \begin{pmatrix} 25 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
4. 1 и 5: $\begin{pmatrix} 6 & 19 \\ 9 & 9 \end{pmatrix} \vec{x} = \begin{pmatrix} 25 \\ 19 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 16 \\ 24 \end{pmatrix} \implies s = 16$
5. 2 и 3: $\begin{pmatrix} 26 & 20 \\ 6 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 21 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
6. 2 и 4: $\begin{pmatrix} 26 & 20 \\ 6 & 1 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
7. 2 и 5: $\begin{pmatrix} 26 & 20 \\ 9 & 9 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 19 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 13 \\ 27 \end{pmatrix} \implies s = 13$
8. 3 и 4: $\begin{pmatrix} 6 & 11 \\ 6 & 1 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \implies s = 0$
9. 3 и 5: $\begin{pmatrix} 6 & 11 \\ 9 & 9 \end{pmatrix} \vec{x} = \begin{pmatrix} 21 \\ 19 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 28 \\ 12 \end{pmatrix} \implies s = 28$
10. 4 и 5: $\begin{pmatrix} 6 & 1 \\ 9 & 9 \end{pmatrix} \vec{x} = \begin{pmatrix} 16 \\ 19 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 20 \\ 20 \end{pmatrix} \implies s = 20$

Теперь заметим, что $s = 0$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №5

Задание C1³ (0.3)

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

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

Ответ: $s = 1$, причём $f(x) = 5x^2 + 6x + 1$

Задание C2[3] (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: $(2, 11), (3, 14)$

Необходимо выяснить чётность секрета.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 11 \\ 14 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} 5 \\ 3 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$

Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет нечётен

P.S. Секрет был $s = 3$

Задание C3[3] (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?

Решение:

Проведём многочлен через точки $[(2, 0), (3, 0), (4, 0), (0, 2)]$: в нуле равен 2, в точках остальных участников равен нулю. Получим многочлен $21x^3 + 18x^2 + 17x + 2$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 1$; там он равен 12.

Теперь прибавим это к известному выданному y и получим $y' = 10 + 12 = 22$.

Значит нужно назвать точку $(1, 22)$

P.S. **Процесс восстановления**:

Через точки $[(1, 10), (2, 15), (3, 17), (4, 4)]$ проходит $f(x) = 21x^3 + 22x^2 + 22x + 14$

Но в результате атаки через $[(1, 22), (2, 15), (3, 17), (4, 4)]$ был проведён $f'(x) = 19x^3 + 17x^2 + 16x + 16$.

Получили: $s = f(0) = 14$ и $s = f'(0) = 16$, что и требовалось

Вариант 4

Задание A1[4] (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 3$. Необходимо его восстановить. В качестве поля 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

Ответ: $v_1 = 16x^2 + x + 4$

Задание A2[4] (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.

Авторское решение: Переведём строку в байты по таблице ASCII:
$[99, 114, 121, 112, 116, 111]$.

Теперь разделим: $\begin{pmatrix} 232 & 239 & 255 & 27 & 92 & 112 \\ 3 & 50 & 197 & 104 & 51 & 0 \\ 4 & 96 & 41 & 220 & 56 & 121 \\ 116 & 241 & 140 & 17 & 173 & 134 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

Задание A3[4] (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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_4 = 27$, $s_5 = 25$
- Участник b знает: $s_2 = 20$, $s = 4$
- Участник c знает: $s_3 = 4$
- Участник d знает: $s_2 = 20$, $s_6 = 26$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s = s_5 + s_6$

И тогда:$s_1 = 31$, $s_2 = 20$, $s_3 = 4$, $s_4 = 27$, $s_5 = 25$, $s_6 = 26$

Задание B1[4] (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.

Авторское решение:

Секрет поместим в точку $(24,\ 29,\ 4,\ 16)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 11 & 7 & 11 & 40 \end{pmatrix} \vec{x} = 23$
2. $\begin{pmatrix} 5 & 20 & 44 & 30 \end{pmatrix} \vec{x} = 40$
3. $\begin{pmatrix} 20 & 15 & 6 & 12 \end{pmatrix} \vec{x} = 3$
4. $\begin{pmatrix} 31 & 28 & 17 & 27 \end{pmatrix} \vec{x} = 35$

Тогда каждый участник обладает следующим набором чисел:

1. $[11, 7, 11, 40, 23]$
2. $[5, 20, 44, 30, 40]$

3. $[20, 15, 6, 12, 3]$
4. $[31, 28, 17, 27, 35]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты. $\begin{pmatrix} 11 & 7 & 11 & 40 \\ 20 & 15 & 6 & 12 \\ 5 & 20 & 44 & 30 \\ 31 & 28 & 17 & 27 \end{pmatrix} \vec{x} = \begin{pmatrix} 23 \\ 3 \\ 40 \\ 35 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 24 \\ 29 \\ 4 \\ 16 \end{pmatrix} \implies s = 24$

Задание B2[4] (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 0 & 0 & 4 \\ 5 & 3 & 0 \end{pmatrix} \vec{x} = \begin{pmatrix} 5 \\ 2 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 6 \\ 0 \\ 3 \end{pmatrix} + t \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 6 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \\ 3 \end{pmatrix} \right]$

Задание B3[4] (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 определеить 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. $4x_1 + 6x_2 = 24$

Для вычислений использовалось поле $\mathbb{Z}_{37}$

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\left(\begin{array}{rr} 8 & 19 \\ 31 & 22 \end{array}\right) \vec{x} = \left(\begin{array}{r} 10 \\ 17 \end{array}\right) \implies \vec{x} = (\begin{array}{r} 11 \\ 29 \end{array}\right) \implies s = 11$
2. 1 и 3: $\begin{pmatrix} 8 & 19 \\ 11 & 15 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$
3. 1 и 4: $\begin{pmatrix} 8 & 19 \\ 22 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 14 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$
4. 1 и 5: $\begin{pmatrix} 8 & 19 \\ 4 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 10 \\ 24 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$
5. 2 и 3: $\begin{pmatrix} 31 & 22 \\ 11 & 15 \end{pmatrix} \vec{x} = \begin{pmatrix} 17 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 14 \\ 13 \end{pmatrix} \implies s = 14$
6. 2 и 4: $\begin{pmatrix} 31 & 22 \\ 22 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 17 \\ 14 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 7 \\ 1 \end{pmatrix} \implies s = 7$
7. 2 и 5: $\begin{pmatrix} 31 & 22 \\ 4 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 17 \\ 24 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 10 \\ 22 \end{pmatrix} \implies s = 10$
8. 3 и 4: $\begin{pmatrix} 11 & 15 \\ 22 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 16 \\ 14 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$
9. 3 и 5: $\begin{pmatrix} 11 & 15 \\ 4 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 16 \\ 24 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$
10. 4 и 5: $\begin{pmatrix} 22 & 8 \\ 4 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 14 \\ 24 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 30 \\ 21 \end{pmatrix} \implies s = 30$

Теперь заметим, что $s = 30$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №2

Задание C1[4] (0.3)

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

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

Ответ: $s = 12$, причём $f(x) = 4x^2 + 8x + 12$

Задание C2[4] (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.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 64 \\ 253 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} -314 \\ 189 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$ Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет чётен

P.S. Секрет был $s = 50$

Задание C3[4] (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?

Решение:

Проведём многочлен через точки $[(1, 0), (2, 0), (3, 0), (0, 40)]$: в нуле равен 40, в точках остальных участников равен нулю. Получим многочлен $22x^3 + 40x^2 + 27x + 40$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 4$; там он равен 3.

Теперь прибавим это к известному выданному y и получим $y' = 6 + 3 = 9$.

Значит нужно назвать точку $(4, 9)$

P.S. **Процесс восстановления**:

Через точки $[(1, 21), (2, 37), (3, 10), (4, 6)]$ проходит $f(x) = 11x^3 + 20x^2 + 8x + 25$

Но в результате атаки через $[(1, 21), (2, 37), (3, 10), (4, 9)]$ был проведён $f'(x) = 33x^3 + 17x^2 + 35x + 22$.

Получили: $s = f(0) = 25$ и $s = f'(0) = 22$, что и требовалось

Вариант 5

Задание A1[5] (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 3$. Необходимо его восстановить. В качестве поля 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

Ответ: $v_1 = 6x^3 + 8x + 5$

Задание A2[5] (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.

Авторское решение: Переведём строку в байты по таблице ASCII:
$[99, 114, 121, 112, 116, 111]$.

Теперь разделим: $\begin{pmatrix} 244 & 143 & 145 & 206 & 81 & 201 \\ 130 & 37 & 132 & 69 & 214 & 113 \\ 68 & 4 & 92 & 214 & 169 & 150 \\ 169 & 186 & 8 & 135 & 164 & 159 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

Задание A3[5] (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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_5 = 28$
- Участник b знает: $s_6 = 23$
- Участник c знает: $s_4 = 0$, $s = 29$
- Участник d знает: $s_3 = 25$, $s_5 = 28$, $s = 29$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s_2 = s_5 + s_6$

И тогда:$s_1 = 25$, $s_2 = 4$, $s_3 = 25$, $s_4 = 0$, $s_5 = 28$, $s_6 = 23$

Задание B1[5] (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.

Авторское решение:

Секрет поместим в точку $(10,\ 6,\ 0,\ 0)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 0 & 6 & 0 & 2 \end{pmatrix} \vec{x} = 3$
2. $\begin{pmatrix} 9 & 9 & 9 & 1 \end{pmatrix} \vec{x} = 1$
3. $\begin{pmatrix} 4 & 9 & 2 & 7 \end{pmatrix} \vec{x} = 6$
4. $\begin{pmatrix} 7 & 4 & 7 & 2 \end{pmatrix} \vec{x} = 6$
5. $\begin{pmatrix} 7 & 5 & 7 & 0 \end{pmatrix} \vec{x} = 1$

Тогда каждый участник обладает следующим набором чисел:

1. $[0, 6, 0, 2, 3]$

2. $[9, 9, 9, 1, 1]$
3. $[4, 9, 2, 7, 6]$
4. $[7, 4, 7, 2, 6]$
5. $[7, 5, 7, 0, 1]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты. $\begin{pmatrix} 7 & 5 & 7 & 0 \\ 4 & 9 & 2 & 7 \\ 9 & 9 & 9 & 1 \\ 7 & 4 & 7 & 2 \end{pmatrix} \vec{x} = \begin{pmatrix} 1 \\ 6 \\ 1 \\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 10 \\ 6 \\ 0 \\ 0 \end{pmatrix} \implies s = 10$

Задание B2[5] (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 3 & 6 & 2 \\ 1 & 0 & 6 \end{pmatrix} \vec{x} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 5 \\ 1 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 0 \\ 5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 6 \end{pmatrix} \right]$

Задание B3[5] (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 определеить 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. $18x_1 + 11x_2 = 6$

Для вычислений использовалось поле $\mathbb{Z}_{37}$

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\begin{pmatrix} 36 & 2 \\ 20 & 34 \end{pmatrix} \vec{x} = \begin{pmatrix} 26 \\ 35 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 11 \\ 0 \end{pmatrix} \implies s = 11$
2. 1 и 3: $\begin{pmatrix} 36 & 2 \\ 24 & 1 \end{pmatrix} \vec{x} = \begin{pmatrix} 26 \\ 0 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 4 \\ 15 \end{pmatrix} \implies s = 4$
3. 1 и 4: $\begin{pmatrix} 36 & 2 \\ 8 & 28 \end{pmatrix} \vec{x} = \begin{pmatrix} 26 \\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 4 \\ 15 \end{pmatrix} \implies s = 4$
4. 1 и 5: $\begin{pmatrix} 36 & 2 \\ 18 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 26 \\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 17 \\ 3 \end{pmatrix} \implies s = 17$
5. 2 и 3: $\begin{pmatrix} 20 & 34 \\ 24 & 1 \end{pmatrix} \vec{x} = \begin{pmatrix} 35\ 0 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 4\ 15 \end{pmatrix} \implies s = 4$
6. 2 и 4: $\begin{pmatrix} 20 & 34\ 8 & 28 \end{pmatrix} \vec{x} = \begin{pmatrix} 35\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 4\ 15 \end{pmatrix} \implies s = 4$
7. 2 и 5: $\begin{pmatrix} 20 & 34\ 18 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 35\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 17\ 3 \end{pmatrix} \implies s = 17$
8. 3 и 4: $\begin{pmatrix} 24 & 1\ 8 & 28 \end{pmatrix} \vec{x} = \begin{pmatrix} 0\ 8 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 4\ 15 \end{pmatrix} \implies s = 4$
9. 3 и 5: $\begin{pmatrix} 24 & 1\ 18 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 0\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 9\ 6 \end{pmatrix} \implies s = 9$
10. 4 и 5: $\begin{pmatrix} 8 & 28\ 18 & 11 \end{pmatrix} \vec{x} = \begin{pmatrix} 8\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 13\ 23 \end{pmatrix} \implies s = 13$

Теперь заметим, что $s = 4$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №5

Задание C1[5] (0.3)

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

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

Ответ: $s = 5$, причём $f(x) = 10x^2 + 10x + 5$

Задание C2[5] (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.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 177 \\ 40 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} 451 \\ -137 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$ Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет нечётен

P.S. Секрет был $s = 123$

Задание C3[5] (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?

Решение:

Проведём многочлен через точки $[(1, 0), (2, 0), (3, 0), (0, 10)]$: в нуле равен 10, в точках остальных участников равен нулю. Получим многочлен $19x^3 + 10x^2 + 23x + 10$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 4$; там он равен 21.

Теперь прибавим это к известному выданному y и получим $y' = 21 + 21 = 11$.

Значит нужно назвать точку $(4, 11)$

P.S. **Процесс восстановления**:

Через точки $[(1, 27), (2, 17), (3, 18), (4, 21)]$ проходит $f(x) = 14x^3 + 30x^2 + 19x + 26$

Но в результате атаки через $[(1, 27), (2, 17), (3, 18), (4, 11)]$ был проведён $f'(x) = 2x^3 + 9x^2 + 11x + 5$.

Получили: $s = f(0) = 26$ и $s = f'(0) = 5$, что и требовалось

Вариант 6

Задание A1[6] (0.3)

Секрет разделён при помощи простейшей (n, n)-схемы, $n = 3$. Необходимо его восстановить. В качестве поля 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

Ответ: $s = 10x^2 + 22x + 9$

Задание A2[6] (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.

Авторское решение: Переведём строку в байты по таблице ASCII: $[66, 111, 116, 97, 121]$.

Теперь разделим: $\begin{pmatrix} 3 & 198 & 181 & 183 & 222 \\ 224 & 89 & 65 & 0 & 83 \\ 60 & 224 & 54 & 78 & 55 \\ 89 & 47 & 104 & 187 & 25 \\ 202 & 65 & 224 & 161 & 248 \end{pmatrix}$

Каждый участник получает одну из строк таблицы, и сумма элементов в каждом столбце даёт соответсвующий символ строки.

Задание A3[6] (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.

Возможный ответ:

Секретная информация:

- Участник a знает: $s_1 = 1$, $s_5 = 44$
- Участник b знает: $s_6 = 33$
- Участник c знает: $s_4 = 33$, $s_1 = 1$
- Участник d знает: $s_3 = 15$

Переменные объявлены так, что:

- $s = s_1 + s_2$
- $s_1 = s_3 + s_4$
- $s_2 = s_5 + s_6$

И тогда:$s_1 = 1$, $s_2 = 30$, $s_3 = 15$, $s_4 = 33$, $s_5 = 44$, $s_6 = 33$

Задание B1[6] (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.

Авторское решение:

Секрет поместим в точку $(12,\ 6,\ 3)$. Он находится в первой её координате.

Проведём через эту точку плоскости. Здесь и далее $\vec{x}$ - вектор-столбец

1. $\begin{pmatrix} 12 & 0 & 4 \end{pmatrix} \vec{x} = 0$
2. $\begin{pmatrix} 3 & 11 & 3 \end{pmatrix} \vec{x} = 7$
3. $\begin{pmatrix} 4 & 7 & 5 \end{pmatrix} \vec{x} = 1$
4. $\begin{pmatrix} 12 & 12 & 4 \end{pmatrix} \vec{x} = 7$
5. $\begin{pmatrix} 11 & 11 & 3 \end{pmatrix} \vec{x} = 12$

Тогда каждый участник обладает следующим набором чисел:

1. $[12, 0, 4, 0]$

2. $[3, 11, 3, 7]$
3. $[4, 7, 5, 1]$
4. $[12, 12, 4, 7]$
5. $[11, 11, 3, 12]$

Чтобы восстановить секрет достаточно решить СЛАУ, после чего извлечь секрет из первой координаты. $\begin{pmatrix} 4 & 7 & 5 \\ 3 & 11 & 3 \\ 11 & 11 & 3 \end{pmatrix} \vec{x} = \begin{pmatrix} 1 \\ 7 \\ 12 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 12 \\ 6 \\ 3 \end{pmatrix} \implies s = 12$

Задание B2[6] (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.

Авторское решение

Составим и решим СЛАУ на координаты точек пересечения:

$$\begin{pmatrix} 5 & 6 & 2 \\ 2 & 4 & 2 \end{pmatrix} \vec{x} = \begin{pmatrix} 4 \\ 6 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, t \in \mathbb{Z}_7$$

Остаётся перебрать все значения t и получить следующие варианты: $\vec{x} \in \left[\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 5 \end{pmatrix} \right]$

Задание B3[6] (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 определеить 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. $23x_1 + 8x_2 = 13$

Для вычислений использовалось поле Z_{29}

Авторское решение:

Переберём все пары участников, для каждой вычислим секрет:

1. 1 и 2: $\begin{pmatrix} 13 & 17 \\ 5 & 13 \end{pmatrix} \vec{x} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 12 \\ 20 \end{pmatrix} \implies s = 12$
2. 1 и 3: $\begin{pmatrix} 13 & 17 \\ 26 & 12 \end{pmatrix} \vec{x} = \begin{pmatrix} 3 \\ 17 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$
3. 1 и 4: $\begin{pmatrix} 13 & 17 \\ 13 & 20 \end{pmatrix} \vec{x} = \begin{pmatrix} 3 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$
4. 1 и 5: $\begin{pmatrix} 13 & 17 \\ 23 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 3 \\ 13 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$
5. 2 и 3: $\begin{pmatrix} 5 & 13 \\ 26 & 12 \end{pmatrix} \vec{x} = \begin{pmatrix} 1 \\ 17 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 14 \\ 17 \end{pmatrix} \implies s = 14$
6. 2 и 4: $\begin{pmatrix} 5 & 13 \\ 13 & 20 \end{pmatrix} \vec{x} = \begin{pmatrix} 1 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 25 \\ 15 \end{pmatrix} \implies s = 25$
7. 2 и 5: $\begin{pmatrix} 5 & 13 \\ 23 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 1 \\ 13 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 21 \\ 21 \end{pmatrix} \implies s = 21$
8. 3 и 4: $\begin{pmatrix} 26 & 12 \\ 13 & 20 \end{pmatrix} \vec{x} = \begin{pmatrix} 17 \\ 16 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$
9. 3 и 5: $\begin{pmatrix} 26 & 12 \\ 23 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 17 \\ 13 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$
10. 4 и 5: $\begin{pmatrix} 13 & 20 \\ 23 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 16 \\ 13 \end{pmatrix} \implies \vec{x} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \implies s = 2$

Теперь заметим, что $s = 2$ встретилось чаще всего, а значит это и будет правильным секретом.

Врёт участник №2

Задание C1[6] (0.3)

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

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

Ответ: $s = 0$, причём $f(x) = 10x^2 + 10x$

Задание C2[6] (0.45)

Для реализации схемы Шамира в качестве поля взяли $\mathbb{Z}_{64}$. Восстановить секрет могут 3 участников, но вам известны лишь $3 - 1$ точка: $(2, 61), (3, 62)$

Необходимо выяснить чётность секрета.

Авторское решение

Пусть $y = c_0 + c_1 x + c_2 x^2$

Составим СЛАУ и решим её: $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \vec{c} = \begin{pmatrix} 61 \\ 62 \end{pmatrix} \implies \vec{c} = \begin{pmatrix} 59 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ -\frac{5}{6} \\ \frac{1}{6} \end{pmatrix}$ Здесь видно, что t должно делиться на 6, иначе результат не будет представим в кольце вычетов. Следовательно t будет чётно, а значит сам секрет будет нечётен

P.S. Секрет был $s = 41$

Задание C3[6] (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?

Решение:

Проведём многочлен через точки $[(2, 0), (3, 0), (4, 0), (0, 30)]$: в нуле равен 30, в точках остальных участников равен нулю. Получим многочлен $9x^3 + x^2 + 29x + 30$ (искать целиком не обязательно на самом деле)

Нам нужно только его значение в точке $x = 1$; там он равен 28.

Теперь прибавим это к известному выданному y и получим $y' = 16 + 28 = 3$.

Значит нужно назвать точку $(1, 3)$

P.S. **Процесс восстановления**:

Через точки $[(1, 16), (2, 18), (3, 16), (4, 39)]$ проходит $f(x) = 39x^3 + 10x^2 + 27x + 22$

Но в результате атаки через $[(1, 3), (2, 18), (3, 16), (4, 39)]$ был проведён $f'(x) = 7x^3 + 11x^2 + 15x + 11$.

Получили: $s = f(0) = 22$ и $s = f'(0) = 11$, что и требовалось
