ОТБОРОЧНЫЙ ЭТАП

УСЛОВИЯ И ОТВЕТЫ
отборочного этапа Межрегиональной олимпиады школьников
им. И.Я. Верченко по математике и криптографии

11 КЛАСС

ВАРИАНТ 1

1. Функция от 4-х переменных $f(x, y, z, t)$, где $x, y, z, t \in \mathbb{R}$ обладает тремя свойствами:

1. $f(x, 0,0, t) = xt$;
2. $f(z, t, x, y) = -f(x, y, z, t)$;
3. $f(x, y, z + \lambda x, t + \lambda y) = f(x, y, z, t)$ для всех $\lambda \in \mathbb{R}$.

Найдите $f(1, 5, 7, 6)$.

2. Найдите все решения системы сравнений

$$\begin{cases} x^2 \equiv 1 (\mathrm{mod}\ 15) \\ x \cdot y^2 \equiv 1 (\mathrm{mod}\ 15) \end{cases},$$

где $x, y \in \{1,2, \dots ,20\}$. В качестве ответа укажите через запятую x и y, для которых сумма $x + y$ максимальна. Например, для $x = 2$ и $y = 3$ запишите «2,3».

3. Для зашифрования текста на русском языке его буквы заменяются наборами из 0 и

1 длины 5 по таблице приведённой ниже. Затем вырабатывается секретная последовательность *(гамма)* $\gamma_0, \gamma_1, \ldots$ также состоящая из 0 и 1, и с ее помощью i-я буква исходного текста $\boldsymbol{a_i} = (a_{5i}, a_{5i+1}, a_{5i+2}, a_{5i+3}, a_{5i+4})$, $i = 0,1,2, \ldots$ заменяется буквой $\boldsymbol{b_i}$ по правилу:

$$\boldsymbol{b_i} = (a_{5i} \oplus \gamma_{5i}, a_{5i+1} \oplus \gamma_{5i+1}, a_{5i+2} \oplus \gamma_{5i+2}, a_{5i+3} \oplus \gamma_{5i+3}, a_{5i+4} \oplus \gamma_{5i+4}).$$

Здесь $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$. Далее $\boldsymbol{b_i}$ заменяется на букву из таблицы. Гамму получают с помощью изображенного на рисунке устройства следующим образом: сначала выбирается ключ $k = (u_0, u_1, \ldots, u_6)$, $u_i \in \{0,1\}$ и его биты последовательно слева направо записывают в семь ячеек *регистра сдвига.*

На i-м такте работы регистра производятся следующие действия:

1) вычисляется знак гаммы $\gamma_i = u_{i+2}u_{i+3} \oplus u_{i+4}$;

2) вычисляется значение $u_{i+7} = u_i \oplus u_{i+4}$;

3) заполнение регистра сдвигается на одну ячейку влево, при этом в крайнюю правую ячейку записывается значение u_{i+7}.

Например, после нулевого такта работы заполнение регистра будет таким: $(u_1, u_2, \ldots, u_6, u_7)$, где $u_7 = u_0 \oplus u_4$. При этом $\gamma_0 = u_2u_3 \oplus u_4$. После первого такта регистр примет вид $(u_2, u_3, \ldots, u_6, u_7, u_8)$, где $u_8 = u_1 \oplus u_5$. Очередной знак гаммы будет равен $\gamma_1 = u_3u_4 \oplus u_5$.

В результате зашифрования был получен текст **люхёчбэ**. Также известны первая и вторая буквы исходного текста **ка**. Найдите исходный текст.

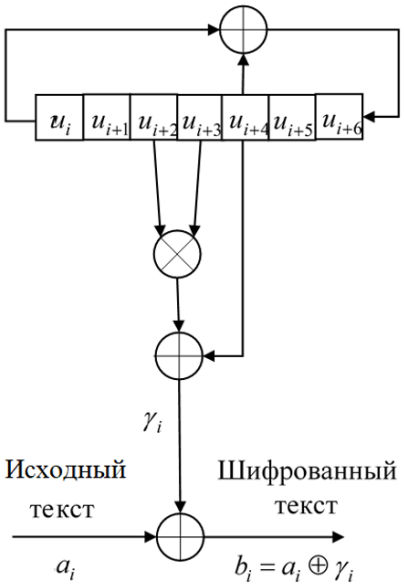


Таблица 1.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь Ъ	Ы	Э	Ю	Я
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111

4. При передаче сообщений используется некоторый шифр. Пусть известно, что каждому из трёх шифрованных текстов

1) **ПНБЙЕОКЛЗТУАОСРЖХ**
2) **УСНГЧЕБКЮФТОАЩЭРД**
3) **БВНОЕЖКИПТЕГАСРЬ**

соответствует исходное сообщение **НЕКТАР**.

Попробуйте расшифровать три текста

1) **СОШЕЛРИФГМЙДПХИВЕАЭДСМАО**
2) **ЕГФРЖИАСМНОЕХТЦАЩП**
3) **ЯСОЧЬЛАИЖМКЦПЬАИЩАУСДЗЬАФ**

при условии, что двум из них соответствует одно и то же сообщение. В качестве ответа укажите слово, которое зашифровано дважды.

5. Известно, что p, p_1, p_2, p_3 – различные простые числа, и $p^3 - 2p^2 - 16p = p_1 \cdot p_2 \cdot p_3 - 32$. Найдите все такие числа p, p_1, p_2, p_3. В качестве ответа укажите все возможные значения числа p.

6. Для шифрования русского слова используется последовательность натуральных чисел $y_1, y_2, \ldots$, которая формируется так: y_1 выбирается произвольно, а остальные члены последовательности вычисляются по формуле $y_{n+1} = 4y_n + 23$, $n = 1,2,\ldots$ Зашифрование производится следующим образом. Первая буква слова заменяется числом согласно таблице ниже и умножается на y_1. Затем также заменяется вторая буква и умножается на y_2 и т.д. Далее все произведения заменяются остатками от деления на 32.
В результате зашифрования получилась последовательность: 20, 27, 16, 10, 29, 22, 7, 10, 19, 22, 20. Какое слово было зашифровано?

Таблица 2

ОТВЕТЫ

1. -29.
2. 4,13.
3. Камелия.
4. Олимпиада.
5. 7.
6. Абитуриент.