XXXIV

Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

УСЛОВИЯ И РЕШЕНИЯ

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

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

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

Найдите $f(100,101,102,103)$.

2. Найдите все решения системы сравнений $\begin{cases} x^2 = 1 (mod\ 33) \\ x \cdot y^2 = 1 (mod\ 33) \end{cases}$, где $x,y \in \{1,2,\dots,32\}$.

3. В канале связи, имеющим пять входов и пять выходов (Рис. 1), информация передается по пяти линиям. Для обеспечения секретности входы и выходы «перемешивают» (делают, например, так, чтобы сигнал, поданный на вход линии 1, в итоге пришел бы, скажем, на выход линии 4 и т.п.). Для этого некоторые пары линий соединены блоками. Каждый из 8-ми блоков независимо от других находится в одном из двух состояний: *верхняя линия на вход – верхняя на выход, нижняя на вход – нижняя на выход* (Рис. 2а) либо *верхняя на вход – нижняя на выход, нижняя на вход – верхняя на выход* (Рис. 2б). Сколькими способами можно выбрать состояния блоков так, чтобы «перемешивания» не было, то есть, если подать сигнал на вход 1, то он придет на выход 1, сигнал, поданный на вход 2, придет на выход 2 и т.д.?

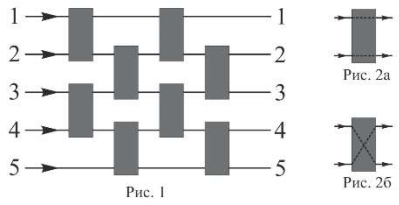


Рис. 1

Рис. 2а

Рис. 2б

4. Знайка использует для зашифрования таблицу:

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Произвольное сообщение $(x_1, x_2, \dots, x_t)$, состоящее из цифр $\{1,2,3,4\}$ на ключе $(k_1, k_2, \dots, k_t)$, $k_i \in \{1,2,3,4\}$ преобразуется в шифртекст $\left(b_{k_1 x_1}, b_{k_2 x_2}, \dots, b_{k_t x_t}\right)$. Например, сообщение $(4,3,1,1)$ на ключе $(1,2,4,4)$ даст шифртекст $(4,1,2,2)$. Незнайка решает для

пущей надежности добавить шифрование на этом же ключе $(k_1, k_2, \dots, k_t)$, но с использование другой таблицы D также размером 4×4. Какими свойствами должна обладать таблица D, чтобы после двукратного шифрования с использование таблиц B и D имелась возможность по известным открытому и шифрованному текстам однозначно восстанавливать ключ? Приведите пример подходящей таблицы D.

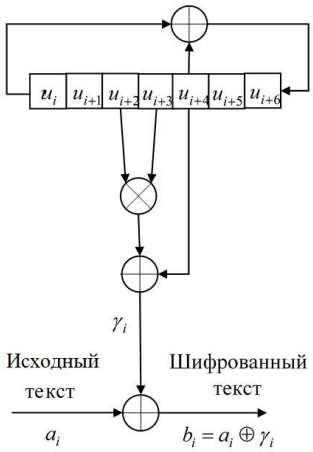
5. Шифрование цифрового текста задается следующим правилом. Каждая цифра x текста заменяется цифрой с помощью функции $f(x) = (b \cdot (x^3 + a) + c)(mod 10)$, $x, a, b, c \in \{0,1, \dots, 9\}$. При каких a, b, c возможно однозначное расшифрование? Найдите многочлен расшифрования при $b = 3$. Ответ обоснуйте.

6. Для зашифрования текста на русском языке его буквы заменяются наборами из 0 и 1 длины 5 по таблице 1. Затем вырабатывается секретная последовательность (*гамма*) $\gamma_0, \gamma_1, \dots$, также состоящая из 0 и 1, и с ее помощью i-я буква исходного текста $\boldsymbol{a_i} = (a_{5i}, a_{5i+1}, a_{5i+2}, a_{5i+3}, a_{5i+4})$, $i = 0,1,2, \dots$ 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 1.

Гамму получают с помощью изображенного на рисунке устройства следующим образом: сначала выбирается ключ $k = (u_0, u_1, \dots, u_6), u_i \in \{0,1\}$ 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: $(u_1, u_2, \dots, u_6, u_7)$, где $u_7 = u_0 \oplus u_4$ При этом $\gamma_0 = u_2u_3 \oplus u_4$. После первого такта регистр примет вид $(u_2, u_3, \dots, u_6, u_7, u_8)$, 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 **щнщшйхс**. Также известны первая и вторая буквы исходного текста **ст**. Найдите ключ k и исходный текст.

Таблица 1

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	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