10 класс XXVII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
(сайт олимпиады www.cryptolymp.ru) 26.11.2017

2 вариант

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв (например, от М до Ы). Остальные части ленты располагаются под ним "вверх ногами" так, чтобы на краях получившейся таблицы друг над другом оказались соседние буквы алфавита. Для зашифрования сообщения каждую его букву заменяют на вторую букву, стоящую в том же столбце таблицы. Например, зашифровав слово ДЕПО с помощью таблицы на рисунке, получим ТСЗИ. Расшифруйте сообщение **ЕВПРШЛОЯЖЗЗ ГЗЖВЕРЗ ЗОРГВОЗШ**, полученное указанным способом (возможно, с использованием другой таблицы).

М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы
Ы	Ж	И	Э	Ж	Э	Й	Л	Я	Я	А	Ъ	О	Ю	Ч

2. Отпирающие комбинации кодового замка представляют собой набор из четырех цифр x_1, x_2, x_3, x_4, каждая из которых равна либо 0, либо 1. Про эти комбинации известно следующее: 1) ровно половина всех наборов открывают замок, 2) если в наборе $x_4 = 1$, то замок откроется в 75% случаев, 3) если $x_2 \cdot x_4 = 1$, то замок откроется в 50% случаев, 4) если $x_3 = 1$, то замок откроется в 25% случаев и 5) если $x_1 + x_2 = 1$, то в 67,5% случаев. Найдите все отпирающие комбинации.

3. В тексте, состоящем из 18 букв и записанном без пробелов, буквы переставлены по следующему правилу: 18-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 17-я – на 3-е место, 2-я – на 4-е и так далее (в конце 10-я буква поставлена на 17-е место, 9-я – на 18-е). Затем такую же процедуру повторили ещё 73 раза. В результате получилось **РЙОТЕЕЯЕВТТОЯСНРИО.** Найдите исходный текст.

4. Для формирования защищенного соединения Алиса, Боб и Стелла используют хранящийся в секрете многочлен с целыми коэффициентами a, b, c вида

$$f(x, y) = ax^2 + bx + cxy + by + ay^2,$$

и целые числа (ключи) k_A, k_B, k_C, которые имеют различные остатки при делении на 173. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB} = r_{173}\big(f(k_A, k_B)\big), \qquad k_{AC} = r_{173}\big(f(k_A, k_C)\big),$$

где $r_{173}(z)$ – остаток от деления числа z на 173. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC} = r_{173}\big(f(k_B, k_C)\big)$. Известно, что $k_A = 22$, $k_{AB} = k_{AC} = 41$, и при всех целых x выполняется равенство $r_{173}\big(f(x, k_A)\big) = r_{173}(x^2 + 62x + 37)$. Найдите ключ k_{BC}.

5. *Латинским квадратом порядка* n называется квадратная таблица из n строк и n столбцов, заполненная натуральными числами от 1 до n таким образом, что каждый столбец и каждая строка не содержат одинаковые числа. Пусть L – латинский квадрат порядка n. Число, стоящее в этом квадрате в строке с номером i и столбце с номером j, обозначим $L(i, j)$.

Два латинских квадрата L_1 и L_2 назовем *ортогональными*, если при их "наложении" не образуется одинаковых пар элементов в разных ячейках таблицы. А именно, если $(i, j) \neq (s, t)$, то $\big(L_1(i, j), L_2(i, j)\big) \neq \big(L_1(s, t), L_2(s, t)\big)$.

а) Постройте пару ортогональных латинских квадратов порядка 5.

б) Докажите, что множество, состоящее из попарно ортогональных латинских квадратов порядка n, не может содержать более чем $n - 1$ квадрат.

6. **(Встреча посередине.)** Шифратор принимает на вход и выдает на выход 8-битное число (1 байт). Поданный на вход байт $\boldsymbol{x^{in}} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ преобразуется в выходной байт $\boldsymbol{x^{out}}$ за 8 тактов. На 1-м такте входной байт $\boldsymbol{x^{in}}$ преобразуется в байт $\boldsymbol{x^{(1)}} = (x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_4^{(1)}, x_5^{(1)}, x_6^{(1)}, x_7^{(1)}, x_8^{(1)})$ по формулам $x_1^{(1)} = x_2 \oplus k_1$, $x_2^{(1)} = x_3$, $x_3^{(1)} = x_4 \oplus k_1$, $x_4^{(1)} = x_5$, $x_5^{(1)} = x_6 \oplus k_1$, $x_6^{(1)} = x_7$, $x_7^{(1)} = x_8 \oplus k_1$, $x_8^{(1)} = x_2 x_7 \oplus x_1$. Здесь k_1 – секретный ключ 1-го такта ($k_1 \in \{0,1\}$); $\oplus$ стандартная операция сложения битов ($0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$). Полученный на 1-м такте байт $\boldsymbol{x^{(1)}}$ на 2-м такте преобразуется в байт $\boldsymbol{x^{(2)}} = (x_1^{(2)}, \dots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2$, ... На 8-м такте вычисляется выходной байт $\boldsymbol{x^{out}} = \boldsymbol{x^{(8)}}$. Найдите ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, на котором байт $\boldsymbol{x^{in}} = (0,0,0,0,0,0,0,0)$ преобразуется в байт $\boldsymbol{x^{out}} = (0,0,1,0,0,1,1,1)$.