

10 КЛАСС

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв

М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	
Г	Ж	И	Э	Ж	Э	Ї	Г	В	Ч	В	К	О	Н	Є	Ч

(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 **ОЛНЛМЛЗЛЦ НРГШРО ЦШЗРОЭУЦРЬ**, полученное указанным способом (возможно, с использованием другой таблицы).

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 $x_2 = 1$, то замок откроется в 75% случаев, 3) если $x_2 \cdot x_4 = 1$, то замок откроется в 50% случаев, 4) если $x_1 = 1$, то замок откроется в 25% случаев и 5) если $x_3 + x_4 = 1$, то в 62,5% случаев. Выберите комбинации, которые открывают кодовый замок (таких комбинаций среди предложенных может быть произвольное число). **Варианты ответов:** (0,0,0,0), (0,0,1,0), (1,0,0,0), (1,1,0,0).

3. В тексте, состоящем из 22 букв и записанном без пробелов, буквы переставлены по следующему правилу: 22-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 21-я – на 3-е место, 2-я – на 4-е и так далее (в конце 12-я буква поставлена на 21-е место, 11-я – на 22-е). Затем такую же процедуру повторили ещё 49 раз. В результате получилось **КБАТСТЯЕЕССОЧОТРИКОЕТИ**. 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 83. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB} = r_{83}(f(k_A, k_B)), \quad k_{AC} = r_{83}(f(k_A, k_C)),$$

где $r_{83}(z)$ – остаток от деления числа z на 83. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC} = r_{83}(f(k_B, k_C))$. Известно, что $k_A = 42$, $k_{AB} = k_{AC} = 24$, и при всех целых x выполняется равенство $r_{83}(f(x, k_A)) = r_{83}(x^2 + 28x + 76)$. Найдите ключ k_{BC} .

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

6. Известно, что целые числа a и b больше 10 и связаны соотношением $3a - 2b = 1$. Известно также, что $r_a(279) = 4$ и $r_b(279) = 7$, где $r_n(x)$ – остаток от деления числа x на n . Найдите $r_{ab}(279)$.