Очный тур V олимпиады по математике и криптографии ФПМИ БГУ (2018 г).

1. Каждой букве русского алфавита поставлено в соответствие 5 двоичных цифр согласно таблице. Передача каждой буквы сообщения осуществляется путем передачи каждой из цифр по отдельному проводу. Два провода случайно замкнулись, и в результате на выходе этих проводов появляется 1, как только по одному из них передается 1. Какое слово передавалось, если на выходе было получено **ЬИФФАЦЮФ**?

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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

2. а) Для разблокировки телефона Максим предложил следующую систему. На экране рисуется прямоугольная область. Координаты левой нижней точки области – (0, 0), верхней правой – (5, 7). За один ход можно из точки с целочисленными координатами (x, y) перейти в точку с координатами (x+1, y) либо (x, y+1). Паролем является последовательность ходов из точки (0, 0) в точку (5, 7). Найдите количество паролей.

б) После того, как телефон Максима взломали, он решил для усложнения паролей добавить еще один разрешенный ход: из (x, y) в (x+1, y+1). Иван же предложил для пароля не фиксировать конечную точку (ей может быть любая точка из нарисованной области). Кто из ребят предложил более надежный способ защиты телефона (в каком случае различных паролей будет больше)?

3. Игорь хочет зашифровать сообщение, состоящее из цифр шестнадцатеричной системы счисления $\boldsymbol{D}$ = = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A, B, C, D, E, F*}. Для этого он использует шифрмашину, которая к каждой цифре сообщения применяет некоторую инъективную функцию S: $\boldsymbol{D} \to \boldsymbol{D}$ (инъективность означает, что для любых $d_1 \neq d_2$ $S(d_1) \neq S(d_2)$). Серёжа перехватил зашифрованное сообщение и утверждает, что если его зашифровать еще раз, получившийся результат зашифровать еще раз и повторять данную операцию далее, то через некоторое время мы получим исходное сообщение.

а) Докажите, что Серёжа прав.

б) Найдите такое наименьшее число n, что если повторить указанную в условии операцию n раз, то гарантированно, хотя бы один раз среди результатов зашифрования встретится исходный текст, независимо от исходного текста и используемой функции S.

в) Найдите такое наименьшее число n, что если повторить указанную в условии операцию ровно n раз, то на выходе гарантированно будет получен исходный текст, независимо от исходного текста и используемой функции S.

4. Для зашифрования сообщения на русском языке, знаки препинания в котором опущены, а слова отделены друг от друга знаком пробела «_», используется шифровальная машина. Она шифрует сообщения в два этапа. На первом этапе символы сообщения заменяются на числа в соответствии с таблицей, построенной по ключевому слову. В первую строку таблицы сначала записывается ключевое слово, потом символ пробела «_», затем оставшиеся буквы алфавита в обычном порядке (буквы Е и Ё не различаются). Во вторую строку по порядку записываются числа от 0 до 32. Например, для ключевого слова **БГУ** таблица примет вид:

Б	Г	У	_	А	В	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Таким образом, после первого этапа мы получаем последовательность чисел. На втором этапе происходит усложнение. Первое число остается неизменным, а к каждому следующему прибавляется число, равное произведению 17 на остаток от деления на 5 предыдущего числа. Например, слово **ФПМИ** будет зашифровано в сообщение **21 34 48 78**. Расшифруйте сообщение, полученное с помощью данной шифровальной машины с некоторым ключевым словом, если известно, что в сообщении содержалось слово «узнал»: **7 40 41 89 35 57 20 69 61 4 85 41 50 23 20 69 57 47 21 35 68 38 74 20 69 51 18 61 4 74 32 19 86 67 18 32 6 19 35 32 21 35 57 38 24 49 6 18 23 19 45 23 21 81 53 41 50 23 20 69 72 35 68 38 74 41 89 35 57 32 19 86 67 18 32 6 25 79 67 23 35 75 79 19 63 74 17 18 71 3 52 38 24 36 36 62 65.**

Текст	Ф	П	М	И
1 этап	21	17	14	10
остаток	1	2	4	0
2 этап	21	34	48	78

5. Шифр Виженера: пусть нам необходимо зашифровать текст X длиной n символов. Ключом является некоторая секретная последовательность символов K длиной m. Сперва буквы исходного текста X и ключа K заменяются на номера этих букв в алфавите начиная с нуля:

$$X \to (x_0x_1\ldots x_{n-1}),\ K \to (k_0k_1\ldots k_{m-1}),\ \text{где } x_i,\ k_i \in Z_{32}=\{0, 1,\ldots, 32\}.$$

Затем вычисляются значения $y_i = (x_i + k_{i \bmod m}) \bmod 33$, где $(\cdot) \bmod p$ означает нахождение остатка от деления на p. Результатом зашифрования является текст Y с номерами букв $(y_0y_1\ldots y_{n-1})$.

Расшифруйте шифртекст, полученный с помощью шифра Виженера с ключом длиной m = 3:

ОГЕУС ТЪЛЭГ ЛБПЕБ ЙНЮСГ ЪЙГЯН ГЫПЕЬ ФДЬКФ ЁГГЕП ОЧБХВ ЦУУОЮ ХОСКЭ РУЕЕУ ЕЩУУЯ ХУСДП ЗТОЕУ СВЁЬФ ТШГХП ФШНЯЕ ПХЧГГ ЧЧГЁЭ ЫШТХВ ДСЦПЖ УОЗЪП ГАЕГЮ ПФЁБР ШТТДБ ЕШЕОЬ ГСГСЛ ЦПЕВС ЗБОЮЭ ЛФАЁУ ЁЙГТО ЗЕШГЕ УРОКФ ЯФЙУЪ ЛЭФТД БЕЯЁР ЬАГЯН ГЫОСЦ ПСЮСЦ ЦБЖУА СЧЙРХ ШЗАЙТ ВЕТЬТ ЮХББЕ ЭФХПЛ АОГЕУ СТЪЛА ЙППШОЗ АПУЁЁ ЁУ

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	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32