Задачи Очного тура III Олимпиады по математике и криптографии ФПМИ БГУ

1. (**2 + 3 балла**) Сотрудники отдела «Ъ» хотят выяснить, куда ездит автобус с номером "ПИ-3141" из Минска. Для этого в автобусный парк был внедрен тайный агент с позывным «МАЗила». И вот спустя пару месяцев развоза бабулек по рынкам и школьников по макдональдсам он получает задание… МАЗиле был выдан комплект (см. на рисунке справа) и зашифрованное сообщение: (←←↑↑,→→↑←↑,←↓↓↓,↑↑→→↑←,↑←↓↓↓,↓↓↓↓). **а)** Сотрудники отдела «Ъ» просят вас помочь с расшифровкой сообщения. **б)** Через неделю маршрут автобуса меняется. МАЗила передал, что теперь автобус будет ездить в город Беларуси, зашифрованный как (↑←↑↑←↓↓↓→→→↑↑←↑→↑). Но при передаче пропали запятые. Куда будет ездить автобус?

2. (**3 + 3 балла**) Доступ к смарт-карте открывается после установки правильного 4-битового кода доступа в защищенной ячейке памяти. С помощью специального оборудования Виктор может инвертировать любой отдельный бит этой ячейки (заменить 0 на 1 или наоборот). **а)** Сможет ли Виктор наверняка подобрать нужный код за 15 инверсий? **б)** Какое наименьшее количество инверсий понадобиться, чтобы гарантированно получить доступ к смарт-карте, если установить надо n-битовый код? Ответ обоснуйте.

3. (**6 баллов**) В шифре Хилла зашифрование происходит следующим образом. Исходные символы сообщения заменяется на их порядковые номера (см. таблицу внизу страницы). Ключом является четверка чисел (a_1, a_2, b_1, b_2) из множества Z_m = {0, 1, ..., m-1} (где m – количество букв в используемом алфавите, в русском алфавите $m = 33$). Далее сообщение разбивается на пары символов и каждая пара зашифровывается независимо от остальных по следующему правилу:

$$(x_1, x_2) \rightarrow ((a_1 * x_1 + b_1 * x_2) \bmod m, (a_2 * x_1 + b_2 * x_2) \bmod m).$$

После чего полученные пары объединяются в итоговый шифртекст.

Был перехвачен шифртекст и стало известно часть открытого текста (см. таблицу), символом * показаны совпадающие символы. Найдите исходное сообщение и ключ.

Открытый текст	В	О					В	*					*	О		
Шифртекст	Е	Д	Ч	Ф	Щ	Е	Ч	Т	Р	Ю	Щ	З	Н	Т	Е	М

4. (**6 баллов**) Шифр *Bifid*, имеющий простое правило зашифрования, использует в качестве ключа квадратную таблицу, в которой в некотором порядке записаны буквы латинского алфавита (буквы I и J отождествлены). Результатом зашифрования фразы WELCO MEOLY MPIAD на приведенном ключе является "Фраза" WITTM LOOOD KKGYQ. Расшифруйте на том же ключе фразу XMFRV SOHHP CPKUW.

	1	2	3	4	5
1	B	S	U	C	R
2	Y	P	T	O	A
3	D	E	F	G	H
4	I	K	L	M	N
5	Q	V	W	X	Z

5. (**12 баллов**) Игорь пользуется телефоном марки *иТелефон*. Для разблокировки на экране появляется 16 кружочков, расположенных в виде таблицы 4 на 4, после чего надо провести пальцем по экрану линию, идущую по последовательности ключевых кружочков (в правильном порядке). В ключевой последовательности соседние кружочки являются соседними в таблице (по стороне или диагонали); ни один из кружочков в ключевой последовательности не повторяется; начальный кружочек ключевой последовательности может быть любым; длина ключевой последовательности 5 кружочков.

Хакер Влад придумал устройство, позволяющее для введенной последовательности из пяти кружочков определить, сколько кружочков из нее содержится в ключевой последовательности и сколько еще и на нужной по счету позиции. За какое наименьшее число попыток Влад может гарантированно разблокировать телефон Игоря? (Можно привести пример алгоритма, позволяющий гарантированно найти ключевую последовательность не обязательно за минимальное число попыток. Чем меньше попыток при этом требуется, тем больше баллов Вы получите).

Символ	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Номер	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32