Задачи очного тура II Олимпиады по математике и криптографии БГУ

1. **(5 баллов)** На клавиатуре мобильного телефона каждой кнопке сопоставлено несколько букв: кнопке 2 соответствуют буквы ABC, 3 – DEF, 4 – GHI, 5 – JKL, 6 – MNO, 7 – PQRS, 8 – TUV, 9 – WXYZ. Выбор нужной буквы определяется числом нажатий на кнопку. Например, нажав на кнопку 4 один раз, получим букву G, а два нажатия на кнопку 4 дадут или букву H (если нажимать быстро), или две буквы G (если нажимать медленно). Известно, что при наборе пароля из 10 букв были нажаты последовательно кнопки 444877399999.

а) Определите число возможных вариантов паролей.

б) Тот же вопрос, если пароль может содержать еще и цифры, получаемые при длительном зажимании кнопки телефона.

2. **(6 баллов)** Символы алфавита представляются числами из множества $A = \{0, 1, ..., m-1\}$. Знайка написал программу, которая меняет каждый символ открытого текста x на символ шифртекста $y = f(x)$. Шифрование выполняется с помощью взаимно-однозначной функции f: $A \to A$ (т.е. для любого y из A, найдется ровно один x из A, что $y = f(x)$). Незнайка решил «улучшить» программу Знайки – теперь символы шифртекста определяются по правилу: $y = (f(x) + x) \pmod m$. Незнайка утверждает, что его отображение также является взаимно-однозначным и его можно использовать для шифрования.

Прав ли Незнайка, если а) $m = 26$ (английский алфавит); б) $m = 33$ (русский алфавит)? При положительном ответе приведите пример подходящей функции f.

3. **(8 баллов)** Последовательность $a_i \in \{0,1\}$ задается следующим линейным рекуррентным соотношением: $a_{i+10} = f(a_i, a_{i+1} \dots, a_{i+9}) = b_0 a_i + b_1 a_{i+1} + \cdots + b_9 a_{i+9} (mod\ 2), i \geq 1$. Кроме того известно, что среди чисел $a_1, a_2, \dots, a_{10}$ не все числа равны 0.

а) Доказать, что данная последовательность будет периодической, т.е. найдется такое число T, что для любого i будет иметь место равенство $a_i = a_{i+T}$.

б) Минимальное значение T, при котором выполнено равенство $a_i = a_{i+T}$, называется главным периодом. Найдите максимальное теоретически возможное значение главного периода T^*.

Пусть функция f такова, что главный период последовательности a_i равен T^* (известно, что она существует).

в) Какие значения может принимать сумма $a_1 + a_2 + \cdots + a_{T^*}$?

г) Функция $g(a,b) = \{1$, если $a = b$; -1, если $a \neq b\}$. Какие значения может принимать сумма $g(a_1, a_2) + g(a_2, a_3) + \cdots + g(a_{T^*-1}, a_{T^*}) + g(a_{T^*}, a_1)$?

4. **(9 баллов)** Фраза, записанная на русском языке, была передана с помощью азбуки Морзе (см. таблицу). Известно, что в каждой букве сообщения оператор произвел ровно одну замену точки на тире, либо тире на точку. Найдите исходное сообщение, если было получено сообщение:

ЙТГУМ ЩДЕГГ ОИДМН ОАМКР ГДКЧМ УТЕМТ РММДТ ЯНТВЕ АГМИМ И.

5. **(10 баллов)** Определим операцию сложения двух букв русского алфавита: буквам ставятся в соответствие их порядковые номера в русском алфавите (см. таблицу), затем эти номера складываются, и от полученного результата берется остаток от деления на 33, который задает порядковый номер результирующей буквы. Для зашифрования текста некоторой длины задается ключ такой же длины и выполняется операция побуквенного сложения (т.е. первая буква текста складывается с первой буквой ключа, вторая – со второй и т.д.).

Сообщение длиной 62 символа разбили на 2 блока по 31 символ в каждом (первый блок состоит из первых 31 символов исходного текста, второй – из последних) и каждый блок зашифровали с одним и тем же ключом K. После зашифрования получились следующие два блока:

ДЧЗВЕ БЁЬЙЖ САЛАР ЫМЗДМ ТЪНЦЩ СЬЮЧГ Е

РЛРЯО ЪУКНМ ФДСЦВ ЯТГМХ ПВЛЮО НШЕОЭ И.

а) Найдите исходное сообщение, если известно, что оно содержит указание, как можно решать эту задачу, а его второй фрагмент начинается со слова «РАЗНОСТЬ».

б) Найдите ключ, который использовался для зашифрования.

Примечание: во всех задачах при зашифровании пробелы и знаки препинания игнорировались, пробелы в приведенных зашифрованных текстах вставлены для удобства прочтения.

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
•–	–•••	•– –	– –•	–••	•	X	•••–	– –••	••	•– – –	–•–	•–••	– –	– •	– – –	•– –•	•–•	•••

т	у	ф	х	ц	ч	ш	щ	ъ	Ы	ь	Э	ю	я
19	20	21	22	23	24	25	26	27	28	29	30	31	32
–	••–	••–•	••••	–•–•	– – –•	– – – –	– –•–	•– –•–•	–•– –	–••–	•••–•••	••– –	•–•–

Задачи очного тура II Олимпиады по математике и криптографии БГУ

1. **(5 баллов)** На клавиатуре мобильного телефона каждой кнопке сопоставлено несколько букв: кнопке 2 соответствуют буквы ABC, 3 – DEF, 4 – GHI, 5 – JKL, 6 – MNO, 7 – PQRS, 8 – TUV, 9 – WXYZ. Выбор нужной буквы определяется числом нажатий на кнопку. Например, нажав на кнопку 4 один раз, получим букву G, а два нажатия на кнопку 4 дадут или букву H (если нажимать быстро), или две буквы G (если нажимать медленно). Известно, что при наборе пароля из 10 букв были нажаты последовательно кнопки 444877399999.

а) Определите число возможных вариантов паролей.

б) Тот же вопрос, если пароль может содержать еще и цифры, получаемые при длительном зажимании кнопки телефона.

2. **(6 баллов)** Символы алфавита представляются числами из множества $A = \{0, 1, ..., m-1\}$. Знайка написал программу, которая меняет каждый символ открытого текста x на символ шифртекста $y = f(x)$. Шифрование выполняется с помощью взаимно-однозначной функции f: $A \to A$ (т.е. для любого y из A, найдется ровно один x из A, что $y = f(x)$). Незнайка решил «улучшить» программу Знайки – теперь символы шифртекста определяются по правилу: $y = (f(x) + x) \pmod m$. Незнайка утверждает, что его отображение также является взаимно-однозначным и его можно использовать для шифрования.

Прав ли Незнайка, если а) $m = 26$ (английский алфавит); б) $m = 33$ (русский алфавит)? При положительном ответе приведите пример подходящей функции f.

3. **(8 баллов)** Последовательность $a_i \in \{0,1\}$ задается следующим линейным рекуррентным соотношением: $a_{i+10} = f(a_i, a_{i+1} \dots, a_{i+9}) = b_0 a_i + b_1 a_{i+1} + \cdots + b_9 a_{i+9} (mod\ 2), i \geq 1$. Кроме того известно, что среди чисел $a_1, a_2, \dots, a_{10}$ не все числа равны 0.

а) Доказать, что данная последовательность будет периодической, т.е. найдется такое число T, что для любого i будет иметь место равенство $a_i = a_{i+T}$.

б) Минимальное значение T, при котором выполнено равенство $a_i = a_{i+T}$, называется главным периодом. Найдите максимальное теоретически возможное значение главного периода T^*.

Пусть функция f такова, что главный период последовательности a_i равен T^* (известно, что она существует).

в) Какие значения может принимать сумма $a_1 + a_2 + \cdots + a_{T^*}$?

г) Функция $g(a,b) = \{1$, если $a = b$; -1, если $a \neq b\}$. Какие значения может принимать сумма $g(a_1, a_2) + g(a_2, a_3) + \cdots + g(a_{T^*-1}, a_{T^*}) + g(a_{T^*}, a_1)$?

4. **(9 баллов)** Фраза, записанная на русском языке, была передана с помощью азбуки Морзе (см. таблицу). Известно, что в каждой букве сообщения оператор произвел ровно одну замену точки на тире, либо тире на точку. Найдите исходное сообщение, если было получено сообщение:

ЙТГУМ ЩДЕГГ ОИДМН ОАМКР ГДКЧМ УТЕМТ РММДТ ЯНТВЕ АГМИМ И.

5. **(10 баллов)** Определим операцию сложения двух букв русского алфавита: буквам ставятся в соответствие их порядковые номера в русском алфавите (см. таблицу), затем эти номера складываются, и от полученного результата берется остаток от деления на 33, который задает порядковый номер результирующей буквы. Для зашифрования текста некоторой длины задается ключ такой же длины и выполняется операция побуквенного сложения (т.е. первая буква текста складывается с первой буквой ключа, вторая – со второй и т.д.).

Сообщение длиной 62 символа разбили на 2 блока по 31 символ в каждом (первый блок состоит из первых 31 символов исходного текста, второй – из последних) и каждый блок зашифровали с одним и тем же ключом K. После зашифрования получились следующие два блока:

ДЧЗВЕ БЁЬЙЖ САЛАР ЫМЗДМ ТЪНЦЩ СЬЮЧГ Е
РЛРЯО ЪУКНМ ФДСЦВ ЯТГМХ ПВЛЮО НШЕОЭ И.

а) Найдите исходное сообщение, если известно, что оно содержит указание, как можно решать эту задачу, а его второй фрагмент начинается со слова «РАЗНОСТЬ».

б) Найдите ключ, который использовался для зашифрования.

Примечание: во всех задачах при зашифровании пробелы и знаки препинания игнорировались, пробелы в приведенных зашифрованных текстах вставлены для удобства прочтения.

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
•–	–•••	•– –	– –•	–••	•	X	•••–	– –••	••	•– – –	–•–	•–••	– –	– •	– – –	•– –•	•–•	•••

т	у	ф	х	ц	ч	ш	щ	ъ	Ы	ь	Э	ю	я
19	20	21	22	23	24	25	26	27	28	29	30	31	32
–	••–	••–•	••••	–•–•	– – –•	– – – –	– –•–	•– –•–•	–•– –	–••–	•••–•••	••– –	•–•–