Ниже приведены условия задач заочного тура олимпиады по математике и криптографии. Для участия в очном туре олимпиады все задачи решать не обязательно, однако чем больше задач Вы решите, тем выше будут шансы пройти дальше. После того, как Вы решите все задачи, или посчитаете, что больше задач решить Вы не в состоянии, перейдите по этой ссылке, где вам будет предложено заполнить электронную форму ответов.

В случае возникновения вопросов по условию задач или порядке проведения олимпиады, можете отправить вопрос на электронный адрес igor.bodiagin@gmail.com.

Окончание приема задач заочного тура – ***9 апреля 2017 г.***

Задачи заочного тура IV Олимпиады по математике и криптографии БГУ

1) (2 балла) Простейшим примером шифрования являются числовые ребусы, когда в верном математическом выражении различные десятичные цифры заменяются различными буквами, а одинаковые цифры – одинаковыми буквами. Расшифруйте ребус:

THREE + THREE +TWO + TWO + ONE = ELEVEN.

В ответе укажите результат выражения **THE + NEW + LEVEL**.

2) (3 балла) Шифр сдвига — это вид шифра, в котором каждый символ в исходном тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите (если левее или правее в алфавите букв больше нет, то с соответствующей стороны приписывается еще один алфавит). Например, в шифре со сдвигом вправо на 3, символ ‘А’ заменяется на ‘Г’, ‘Б’ – на ‘Д’, и так далее, ‘Я’ – на ‘В’.

В случае латинского алфавита и сдвига алфавита на 3 символа вправо шифр носит название «шифр Цезаря» в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. Благодаря тому, что большинство врагов Цезаря были неграмотными и предполагали, что сообщения были написаны на неизвестном иностранном языке, шифр был достаточно надежен.

Некоторое осмысленное слово русского языка зашифровано с помощью шифра с некоторым сдвигом. В результате получена следующая последовательность символов (пробелы добавлены для упрощения прочтения):

ЮГЙДЁ ВХЛЮФ.

Найдите исходное слово.

3) (5 баллов) Чтобы попасть на очный тур олимпиады по криптографии, каждому участнику надо указать некоторый делитель числа $2^{254542} + 1$, отличный от самого числа и 1. Если участник вводит делитель, который до него никто не вводил, то делитель принимается, в противном случае система просит ввести другой делитель. Первыми на отбор пришли Влад, Егор, Володя, Миша, Игорь и Валера. Помогите ребятам пройти отбор, для этого найдите хотя бы 6 делителей указанного числа (делители можно указывать в любом виде, понятном для проверяющих).

4) (6 баллов) Ева заразила компьютер Боба вирусом, который непрерывно размножается. Одну секунду вновь рожденный вирус обживается, а затем каждую секунду производит еще одного себе подобного. Боб обратился за помощью к Тренту. Трент провел анализ программы вируса и обнаружил, что как только количество копий станет кратно 2^{16}, все они будут мгновенно уничтожены (из-за ошибки в программе – переполнения одной из переменной) и компьютер будет спасен.

а) (3 балла) Оказалось, что через некоторое время компьютер Боба будет спасен. Найдите, через какое минимальное целое число часов компьютер Боба будет спасен.

б) (3 балла) Ева может модифицировать свой вирус таким образом, что все копии вируса уничтожались бы, как только количество копий станет кратно m, где число m выбирается Евой.

Сколько существует различных натуральных m, при которых компьютер Боба так и не смог бы самостоятельно излечиться от вируса?

5) (7 баллов) Лицензионный ключ продукта представляет собой последовательность из 16 цифр или букв латинского алфавита. Для проверки подлинности ключа поступают следующим образом. Сначала латинские буквы заменяются на числа по следующему правилу: A – 10, B – 11, …, Z – 35. Затем для полученного набора из 16 чисел (x_1, x_2, …, x_{16}) вычисляются следующие выражения:

$$A = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_9 + x_{10} + x_{11} + x_{13} + x_{14} + x_{15} \bmod 36;$$

$$B = 2x_2 + 3x_3 + 4x_4 + 6x_6 + 7x_7 + 8x_8 + 10x_{10} + 11x_{11} + 12x_{12} + 14x_{14} + 15x_{15} + 16x_{16} \bmod 36;$$

$$C = 7x_1 + 9x_2 + 9x_3 + 7x_4 + 9x_5 + 7x_8 + 9x_9 + 9x_{10} + 9x_{12} + 7x_{13} + 7x_{15} + 9x_{16} \bmod 36;$$

$$D = 2x_2 + 13x_4 + 6x_5 + 3x_6 + x_7 + 5x_8 + 6x_9 + 22x_{10} + 29x_{11} + 3x_{12} + 29x_{13} + 22x_{14} + 21x_{15} + 14x_{16} \bmod 36.$$

Выражение … mod 36 означает нахождение остатка от деления на 36. Ключ признается подлинным, если одновременно выполняются следующие 4 равенства: A = 1, B = 2, C = 3, D = 4.

Обозначим через S_1 – количество подлинных ключей, начинающихся 4 нулями, а через S_2 – количество подлинных ключей, заканчивающихся 4 нулями.

В ответе укажите, чему равна разность $S_1 - S_2$ (ответ может быть числовым выражением).

6) (8 баллов) В настоящее время для многих целей используют блочно-итерационные шифры (по-научному их называют криптосистемами). Дадим их краткое описание. Всё исходное сообщение делится на блоки одинаковой длины, скажем 32 или 64 бита. В данном случае говорят о битах, т.к. почти все современные такие криптосистемы реализуются на компьютере. Бит – это один из символов 0 или 1. Любой символ естественного языка, будь то буква, цифра или знак препинания, может быть представлен в виде последовательности из 8, 16 или 32 битов в зависимости от используемой таблицы кодировки.

Итак, исходное сообщение разбито на блоки по 32 или 64 бита. Каждый такой блок зашифровывается по отдельности. К блоку X последовательно применяются одинаковые преобразования, отличающиеся лишь некоторым специальным параметром k, называемым тактовым ключом. Как правило, эти преобразования заключаются в сложении входного блока с тактовым ключом k, некоторой замене бит и перестановке бит. Таким образом, исходный блок X изменяется данным преобразованием с тактовым ключом k_1, на выходе мы получаем блок Y_1. Затем Y_1 изменяется тем же преобразованием, но уже с тактовым ключом k_2, на выходе мы получаем Y_2 и так далее. Данные шаги повторяются несколько раз, как правило, не менее 8 (число таких повторов – итераций – оговаривается заранее). Тактовые ключи k_1, k_2, … генерируются на основе некоторого начального ключа, по заранее оговоренному алгоритму.

Стала известна следующая информация о блочно-итерационной криптосистеме, которую использует хулиган Вася. Алгоритм Васи работает с блоками из 64 битов. Блок X делится на 2 равные по длине части X_1 и X_2 по 32 бита каждая. Это будем записывать так: $X = X_1 \,||\, X_2$. Затем на каждом шаге (итерации) применяется следующее преобразование:

$$\Sigma_k(X_1 \,||\, X_2) = X_1 \oplus f_k(X_1 \oplus X_2) \,||\, X_2 \oplus f_k(X_1 \oplus X_2),$$

где $\oplus$ – операция "взаимоисключающее или", выполняемая для каждого двоичного разряда по отдельности. Ниже приведена таблица для вычисления $\oplus$ от двух аргументов:

x	1	1	0	0
y	1	0	1	0
$x \oplus y$	0	1	1	0

Как видно из приведенной выше формулы, на выходе используемого преобразования получается блок длиной 64 бита, разделенный на 2 блока по 32 бита каждый. Вместо k при зашифровании подставляются тактовые ключи.

Всего было 12 итераций. Однако, к сожалению, узнать что-либо о тактовых ключах k_1, k_2, …, k_8 или о преобразовании f_k так и не удалось.

Был перехвачен следующий блок зашифрованной битовой последовательности:

0001 0100 1011 0010 1110 0100 1001 0100 1010 1010 0011 0001 1000 1110 0001 1001

Известно, что Вася отправил одно из следующих 10 сообщений:

1) 1101 1000 1010 1010 0011 0100 1110 1000 1110 0011 1000 1001 1000 1101 1010 0011;
2) 1111 1000 0011 0100 0100 1111 0111 1000 0011 0000 1010 0000 0001 1101 0100 1001;
3) 1010 1101 0110 0010 1001 0001 1010 1001 0111 1101 1101 0100 1100 0010 0011 0011;
4) 1011 1011 0101 0100 0010 0101 1101 1010 0111 0100 1000 1101 0000 0110 1110 1010;
5) 1010 0101 0010 0010 1001 0011 1010 0010 0010 1011 1101 0010 0111 0000 1000 1111;
6) 1011 1110 0101 0100 1101 1110 1011 1011 0000 0000 1101 0111 1011 0100 0011 0110;
7) 1111 1111 0000 0000 1111 1111 0000 0000 1111 0000 1111 0000 0000 1111 0000 1111;
8) 0011 0010 0001 1111 1101 1000 0001 1100 1010 1001 1011 1011 0011 0101 1101 1111;
9) 1100 0011 1100 0011 0011 1100 0011 1100 1010 0101 1010 0101 0101 1010 0101 1010;
10) 1111 1111 1111 1111 0000 0000 0000 0000 1111 1111 1111 1111 0000 0000 0000 0000.

В ответе укажите номер исходной битовой последовательности.

7) (16 баллов) Шифр простой замены. Шифр простой замены представляет собой алгоритм побуквенного зашифрования текста с использованием таблицы замены. Каждая буква открытого (исходного) текста заменяется соответствующей (стоящей под ней в таблице) буквой из таблицы. Например, слово «КОД» будет зашифровано с помощью следующей таблицы замены в слово «БПХ».

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
Ч	Г	Н	У	Х	Ы	Е	В	Ё	К	Э	Б	Ц	Ъ	Л	П	С	О	Т	И	М	Ю	Я	З	Ж	Р	Ф	Ш	А	Щ	Д	Й	Ь

В первой строке таблицы замены последовательно размещены все буквы алфавита. Понятно, что во второй строке таблицы каждая буква может встречаться ровно один раз (в противном случае текст невозможно будет расшифровать однозначным образом). Такая таблица является ключом шифра простой замены.

а) (1 балл) С помощью представленной таблицы было зашифровано некоторое слово, в результате чего был получен следующий шифртекст (пробелы вставлены для удобства чтения):

ГЫЁП СЧТЛ ПТИЩ

Какое слово было зашифровано?

б) (5 баллов) Сколько существует для алфавита из 9 букв таблиц замены таких, что ни один символ при зашифровании не переходит сам в себя?

в) (10 баллов) Следующий шифртекст был получен с помощью шифра простой замены с помощью некоторой неизвестной таблицы замены (в исходном тексте были удалены все пробелы и знаки препинания, пробелы вставлены для удобства прочтения):

ХФЭЧК ЁЧЦРЁ ЧЗЧЭД ЖЧЯЁЧ ЪАЭЧБ ФЮПЧУ ЁЧФШР ЩХФУБ ЧФЁЧЁ ЗЁЧБШ ХФКШЭ ФЙЧБШ ЮШЭФЖ ХФЭШЭ УГБФК ЬХЬЦА ЦЬЭЬЛ ДЮПЬГ ПЗЧЦУ ЧЭБФР БЧЦУК ФЁФЦЧ ЕБЧЪА ЭЧПШЫ ЙЭГХФ ЁДЁФБ ДХШЬЁ ЧЧРФБ ДУЭШЪ ЩОЬБФ КФПБЩ О.

Затем приведенный шифртекст еще раз зашифровали с помощью шифра простой замены с тем же ключом. Эту процедуру повторили и с новым шифртекстом. В результате был получен следующий шифртекст (результат трехкратного зашифрования):

ЬЦГПЫ ЁПЕЮЁ ПАПГИ ФПЙЁП УЛГПС ЦЧОПВ ЁПЦЭЮ КЬЦВС ПЦЁПЁ АЁПСЭ ЬЦЫЭГ ЦБПСЭ ЧЭГЦФ ЬЦГЭГ ВНСЦЫ ХЬХЕЛ ЕХГХЯ ИЧОХН ОАПЕВ ПГСЦЮ СПЕВЫ ЦЁЦЕП МСПУЛ ГПОЭШ БГНЬЦ ЁИЁЦС ИЬЭХЁ ППЮЦС ИВГЭУ КРХСЦ ЫЦОСК Р.

Найдите исходное сообщение. (Указание к решению задачи: подсчитайте частоты встречаемости символов в шифртексте)