Очный тур VI олимпиады по математике и криптографии ФПМИ БГУ (20.04.19)

1. (3 балла) Ключ – пара целых чисел (a, b), $a < b$, $b > 0$.

Алгоритм зашифрования:

1) Открытый текст выписывается в одну строку без пробелов и знаков препинания. В нем выделяется каждый a-ый и b-ый по счёту символ, после чего они переписываются в шифртекст в том порядке, в котором они идут в открытом тексте (например, если $a = 3$, $b = 5$, то будут выписаны символы с номерами мест 3, 5, 6, 9, 10 именно в таком порядке). Если $a < 0$, то выписывать только каждый b-ый символ.

2) Выписанные символы вычёркиваются из открытого текста.

3) Повторяются шаги 1 – 2 до тех пор, пока в открытом тексте количество символов не станет меньше b.

4) Переопределяем a и b следующим образом: $a = a - 1$, $b = b - 1$. Если $b > 0$, то перейти к шагу 3).

Известно a = 7, b = 9. Найти исходный текст, если шифртекст:

ЯОЯОХОГРАШОПАДДГНСОЕ

2. (6 баллов) Кодовая книга – книга, в которой хранятся ключи для зашифрования и расшифрования. Анаграмма – слово, которое может быть получено из исходного перестановкой букв. Биграмма – два символа на соседних позициях. Кодовая книга состоит из трёх ключей, длина каждого из них – 10 символов:

1) ЗАВТРАШНИЙ; 2) ВСТРУХНУТЬ; 3) ПОЛИГИМНИЯ.

В случае, если данная книга будет утеряна, необходимо составить новую. Сколькими способами можно это сделать, если для создания новой книги необходимо использовать анаграммы ключей из старой? При этом недопустимо, чтобы в словах (ключах) любая из биграмм состояла из двух одинаковых букв.

3. (6 баллов) Максим решил зашифровать сообщение используя интеллектуальный ввод (T9). Алгоритм шифрования выглядит следующим образом: каждый пробел в сообщении заменяется на очередную букву секретного слова: первый – на первую, второй – на вторую, и т.д. Затем полученный набор букв набирается на клавиатуре мобильного телефона. При этом при вводе каждой буквы осуществляется лишь однократное нажатие соответствующей клавиши (см. рис), а программа интеллектуального ввода по нажатым кнопкам сама неизвестным образом выбирает слова из словаря. Например, мы хотим зашифровать слово "кот", мы нажимаем по одному разу на кнопки "ийкл" (соответствует букве "к"), "мноп" ("о"), "рсту" ("т"), после чего программа может выдать нам 2 слова "и", "ор", т.к. этим словам соответствуют те же кнопки. Полученные таким образом осмысленные слова (включая предлоги) разделяются запятыми и передаются. Найдите исходное сообщение, если получен следующий набор слов:

мой, о, еж, цру, виа, я, собр, ласка, иди, у, лор, нас,
ахия, до, предел, до, оно, ранит, лом, ей.

4. (8 баллов) Сначала Егор каждую букву русского алфавита (кроме Ё) кодирует последовательностью из 5 бит (0 или 1) в соответствии с таблицей (пробелы и знаки препинания опускаются). Для проверки того, что символы сообщения были переданы правильно, Егор добавляет к кодировке каждой буквы шестой бит, который вычисляется как $x_6 = x_2 * x_3 * x_4$. Далее Егор шифрует получившуюся битовую последовательность следующим образом: он выбирает ключ, состоящий из нескольких бит, и записывает его на листе бумаги столько раз подряд, чтобы длина получившейся ключевой последовательности стала не меньше длины закодированного сообщения, после чего *i*-ый бит сообщения складывает по модулю 2 с *i*-ым битом ключевой последовательности (*i* изменяется от 1 до длины сообщения в битах). Например, Егор хочет передать сообщение "АУ", согласно таблице А – 00000, У – 10011. Он добавляет по шестому биту и получает сообщение 000000 100110. Пусть ключ *k* = 0110, тогда в результате зашифрования Егор получит 011001 000000.

Хакер Влад перехватил зашифрованное сообщение:

000010 010110 010110 011101 011000 100010 011010 101110 011011 111111 101010 001111 111001 010100 101111 011001 000110 000101 111010 100010 010010 000101 111101 001100 110010 111001 111100 101111 000011.

Какое сообщение было передано, если известно, что длина ключа равна 13 бит?

	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
x_1	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
x_2	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
x_3	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
x_4	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
x_5	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

5. (9 баллов) Володя использует шифр Виженера. Пусть n – количество букв в алфавите, x_i – номер i-ой буквы сообщения, k_j – номер j-го символа ключа, m – длина ключа. Тогда зашифрование осуществляется по формуле:

$$y_i = x_i + k_{i \,(\mathrm{mod}\ m)\,+\,1} \ (\mathrm{mod}\ n),$$

где запись (mod n) означает нахождение остатка от деления на n.

Для того, чтобы письмо никто не прочёл, он решил использовать предложенный шифр, а для увеличения объема текста он каждый пробел заменил словом «ПРОБЕЛ». Расшифруйте письмо (пробелы вставлены для удобства прочтения)

СЧЬБЪ ПЪШЭУ ШЕЮЦЫ БЁВБГ КЕУЭФ ОБАЩЫ ЁЬЛБЁ ЬЬСЭУ ТОАЮВ БПФЬЫ ССЖРБ ЁРЗЕБ АВМТП ЦЮЬПА ЩЫЁЬЛ ЪЕЩЫА ЧРЗЛФ ЭТЧЪС АЩЫЁЬ ЛЮЙЮЙ ТЫБГК ЕУЭЮО ТХЩСФ ЗОУЙЧ НЭЯАУ БПЫСЕ УЬРЫХ ЬЬСЭН ШЛЮЭТ ЧЗЧЩЭ БЫЮЭШ ЭУШЕЮ ИЧЫЭЯ АУБПМ ЯБЖФЪ ШЭУШЕ ЮУГБЫ КБГКЕ УЭЫЬВ ХЩСЦЕ ОВХЪЭ ТЪЯТЛ ФЭТЧЪ ЯРЩМЪ ЖРБЁР ЗЭЭБГ КЕУЭТ ЪТХЙЭ ЙЖРБЁ РЗЦЮВ БЭИЪЮ ТБФЭИ ЯНОЕД ПЪИБЮ ВБЭИЪ САОЫЩ РАФЗО УЙЧЫЭ ЯАУБП ЮААНЫ АЩЫЁЬ ЛЙЧЪЛ ЮЭТЧЗ РОДЧЫ ПГСЧЕ ЖРБЁР ЗПЮВБ ЭИЪУЁ ЦФАЩЫ ЁЬЛГЕ ЭЖЮЭЦ ЕНГЮВ БПФЬЪ ЫЖЬРК ЙЩЙЬЮ ВБЭИЪ ГВЯЮС НШИЗУ ХУХЛЮ ЭТЧЗХ БАГЭЭ ЛШЭУШ ЕЮТЛЛ ЮЭТЧЗ ШОЬЁЪ ЛГИЯН ЩЕВХЪ ЭТЪББ ЛФЭТЧ ЪЪБСЬ ЧЁГГЕ АЕЦЮВ БЭИЪЮ НЮАЯЙ СРАЗЁ ЬЛЗЦЮ ВБЭИЪ ЙЫГАЛ ШЭУШЕ ЮТЛФЦ ДБГКЕ УЭВЯФ ФУЫЖЖ РБЁРЗ ЦЮВБЭ ИЪБГЭ ЗЬДВФ ЗОУЙЧ НАЭЭЧ ОМШБГ ЭРХФЪ ЕЫЕРЦ ЗЛЮЭТ ЧЗЦУТ ЧЮАЯЙ СРЕЕВ ХЪЭТЪ ГБНЦО УЫБЯБ ЧНЙГТ ГШПЬЭ ЯАУБП ЮВБЁФ ВЫИФЗ ОУЙЧЩ АЭБГК ЕУЭВЧ БМХЫФ ЗОУЙЧ НЭЯАУ БПВУТ ХФЮСС СЖРБЁ РЗАРА ЬЛФЭТ ЧЪУБЬ П.

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