

Решения предложенных задач оформляются в электронном виде и высылаются на электронный адрес [omc@bsu.by](mailto:omc@bsu.by). В высылаемом решении для каждой из предложенных задач необходимо указывать только ответ! Вместе с решением необходимо выслать ваши фамилию, имя, отчество, класс, номер школы и город. Также можете указать электронный адрес, на который мы впоследствии вышлем а) вашу сумму баллов по результатам проверки заочного тура и б) приглашение на участие в очном туре, в случае успешного выступления на заочном туре. Если такого адреса указано не будет, то ответ будет выслан на адрес, с которого было отправлено письмо.

## Задачи заочного тура II Олимпиады по математике и криптографии БГУ

**1. (3 балла)** Для зашифрования текста над каждой буквой производятся следующие преобразования: 1) буква исходного текста заменяется на номер этой буквы в алфавите начиная с нуля (так, а – 0, б – 1 и т.д., я – 32); 2) по полученному таким образом номеру  $x$  вычисляется значение  $y = (a * x + b) \bmod 33$ , где натуральные числа  $a$  и  $b$  – это ключ шифра, а запись  $( ) \bmod 33$  означает нахождение остатка от деления на 33; 3) буква с номером  $y$  в алфавите и есть результат зашифрования буквы исходного текста. Например, при ключе  $(a, b) = (2, 1)$  буква б, имеющая номер 1, при зашифровании перейдет в букву г, имеющую номер 3, а буква я перейдет сама в себя. В криптографии описанный шифр называется аффинным.

**а) (1 балл)** Зашифровать слово «криптография» с ключом  $(a, b) = (19, 2)$ .

**б) (2 балла)** Найдите количества различных ключей (учтите, что ключ должен быть таким, что любое зашифрованное с его помощью сообщение должно однозначно расшифровываться).

**2. (5 баллов)** Простейшим примером шифрования являются числовые ребусы, когда в верном математическом выражении различные десятичные цифры заменяются различными буквами, а одинаковые цифры – одинаковыми буквами. Расшифруйте ребус:

$$\text{ЕВА} * \text{БОБ} = \text{АЛИСА} \text{ и } \text{А} + \text{Б} = \text{В}.$$

**а) (2 балла)** В ответе укажите, какие числа соответствуют словам АЛИСА и БОБ.

**б) (3 балла)** Сколько решений будет иметь ребус, если убрать условие  $\text{А} + \text{Б} = \text{В}$ ?

**3. (4 балла)** Комбинация  $(x, y, z)$  трех натуральных чисел, лежащих в диапазоне от 10 до 20 включительно, является отпирающей для кодового замка, если выполнено соотношение  $F(x, y, z) = 215$ . Найдите все отпирающие комбинации для замка с

$$F(x, y, z) = 5x^2 - 3y^2 - 11z.$$

**4. (6 баллов)** Числовой код, состоящий из 8 цифр, будем называть надежным, если в нем никакие две соседние цифры не совпадают и никакая цифра не встречается в нем более трех раз. Сколько всего существует надежных кодов?

**5. (6 баллов)** Для формирования общего ключа, при передаче сообщений по открытому каналу связи Алиса и Боб решили воспользоваться протоколом Диффи-Хеллмана. Для этого они выбрали простое число  $p = 101$  и число  $q = 5$ . Затем Алиса и Боб выбрали некоторые произвольные натуральные числа  $a$  и  $b$  соответственно. После чего Алиса передала Бобу число  $A = q^a \bmod p$ , а Боб Алисе передал число  $B = q^b \bmod p$ . И, наконец, Алиса и Боб смогли сформировать общий ключ  $k = B^a = A^b = q^{ab} \bmod p$ . Были перехвачены числа  $A = 84$  и  $B = 71$ . Найдите ключ  $k$  (Задача является иллюстрацией того факта, что при использовании протокола Диффи-Хеллмана, задача формирования

общего ключа  $k$  для злоумышленника является вычислительно сложной даже при перехвате сообщений  $A$  и  $B$ , передаваемых по открытому каналу связи).

**6. (4 балла)** В первом столбце зашифровано стихотворение В.И. Малюгина «Про Ното», «ключом» к расшифровке которого является отрывок из известной поэмы, «записанный» во втором столбце. Восстановите текст зашифрованного стихотворения.

1	И постоянно спотыкался,	Идет направо – песнь заводит,
2	И не умея управлять,	Там о заре прихлынут волны
3	Его развития, прогресс –	И тридцать витязей прекрасных;
4	Что можно Sapiensом стать,	Стоит без окон, без дверей;
5	Но вскоре вновь все забывал.	Русалка на ветвях сидит;
6	Издравле Ното проживал.	Златая цепь на дубе том:
7	Так коротал земной свой срок,	Там на неведомых дорожках
8	Страдалец полагал наивно,	Избушка там на курьих ножках
9	Виня во всем судьбу и рок.	Следы невиданных зверей;
10	Всем, что линейно и дискретно	Идет, бредет сама собой;
11	Расставил фильтры тут и там,	Через леса, через моря
12	Когда окончил ФПМ.	И там я был, и мед я пил.
13	Не зная правил адаптивных	Там лес и дол видений полны;
14	Наивность, видно, не порок –	Там королевич мимоходом
15	В случайном, ненормальном мире	У лукоморья дуб зеленый,
16	Из шишек он извлек урок.	Пленяет грозного царя;
17	В каком-то смысле рекуррента	Чредой из вод выходят ясных,
18	Не осознав, что эвольвента	На брег песчаный и пустой,
19	Стал оптимально управлять,	Там ступа с Бабою Ягой
20	И адаптивный генератор –	Колдун несет богатыря;
21	Соорудил классификатор,	Там в облаках перед народом
22	И непременно все терял,	Налево - сказку говорит.
23	Не мог сыскать сигнал в эфире,	И днем и ночью кот ученый
24	Не оптимально управлял,	Всё ходит по цепи кругом;
25	А после долго возмущался,	Там чудеса: там леший бродит,
26	Стал мыслить гибко и конкретно,	А бурый волк ей верно служит;
27	Разумным Ното стал совсем,	Там русской дух... там Русью пахнет!
28	И Ното было не узнать.	Там царь Кашей над золотом чахнет;
29	Заслон помехам и шумам.	В темнице там царевна тужит,
30	И стохастический процесс.	И с ними дядька их морской;

**7. (7 баллов)** Алгоритм Евклида нахождения НОД двух натуральных чисел  $a, b$  ( $a \geq b$ ) состоит в следующем. Строим последовательность упорядоченных пар  $(a_i, b_i)$ ,  $i=1, \dots, k+1$ , где  $a_{(i+1)}=b_i$ ,  $b_{(i+1)}=a_i \pmod{b_i}$ ,  $i=1, \dots, k$ ,  $a_1=a$ ,  $b_1=b$ ,  $b_i > 0$  при  $i \leq k$ ,  $b_{(k+1)}=0$ . При этом  $\text{НОД}(a, b)=b_k$ . Модифицированным алгоритмом Евклида нахождения НОД двух натуральных чисел  $a, b$  ( $a \geq b$ ) назовём следующую процедуру. Строим последовательность упорядоченных пар  $(a_i, b_i)$ ,  $i=1, \dots, m+1$ , где  $a_{(i+1)}=b_i$ ,  $b_{i+1} = \min\{a_i \pmod{b_i}, |b_i - (a_i \pmod{b_i})|\}$ ,  $i=1, \dots, m$ ,  $a_1=a$ ,  $b_1=b$ ,  $b_m > 0$  при  $i \leq m$ ,  $b_{(m+1)}=0$ . При этом  $\text{НОД}(a, b)=b_m$ . Числа  $k$  и  $m$  назовем длинами алгоритма Евклида и модифицированного алгоритма Евклида для пары чисел  $a, b$  и обозначим  $L_1(a, b)$  и  $L_2(a, b)$  соответственно. Найти такие

пары натуральных чисел  $a, b$  ( $a \geq b$ ) и  $c, d$  ( $c \geq d$ ), для которых  $L_1(a, b) = L_2(c, d) = 2015$  и  $a, c$  принимают минимальные возможные значения. В ответе указать число  $[\lg a] + [\lg b] + [\lg c] + [\lg d]$ .

**8. (11 баллов)** Цилиндр Джефферсона – один из первых современных шифраторов, созданный Джефферсоном между 1790 г. и 1800 г. Джефферсон назвал свою систему шифрования «дисковым шифром». Сам он не был уверен в надежности своего изобретения, поэтому относился к нему с осторожностью и, будучи президентом США, не использовал его, а продолжил применять традиционные коды и шифры, поэтому само изобретение довольно скоро попало в архив. В XX веке, когда изобретение нашли и вновь о нем вспомнили, оно было признано как очень стойкое к криптоанализу шифровальное устройство, а самого Джефферсона назвали "отцом американского шифровального дела".

Рассмотрим конструкцию шифратора: деревянный цилиндр надет на ось и разрезан на  $N$  дисков, на каждый из этих дисков в произвольном порядке нанесен некоторый алфавит (например, русский), состоящий из  $M$  символов. Диски могут вращаться независимо друг от друга. Над поверхностью цилиндра выделяется линия, под которой будет собираться открытый текст. Текст, который необходимо зашифровать разбивается на блоки по  $N$  символов. Первая буква блока находится на первом диске и фиксируется под выделенной линией, вторая — на следующем диске и т. д. Зашифрованный текст считывается с любой другой строки, кроме строки открытого текста. Расшифрование осуществляется на таком же шифраторе: шифртекст составляется под выделенной линией, открытый текст ищется среди параллельных линий, путем отыскания осмысленного сообщения.



Рисунок 1. – Цилиндр Джефферсона

**а) (1 балл)** Ключом шифратора Джефферсона является некоторая перестановка дисков. Какое минимальное и максимальное количество ключей может иметь шифратор Джефферсона.

**б) (2 балла)** Сколько существует различных цилиндров Джефферсона?

**в) (8 баллов)** Разведчику Виктору удалось установить, что Алиса и Боб используют шифратор Джефферсона с  $N = 14$  дисками, для которых известно расположение букв на дисках:

**абвгдеёжзийклмнопрстуфхцшщъыьэюя**  
**пъздфхжынэгаквлъйчшёиеорсцбщтюмя**  
**фдпеёцсчхнюоушйрэашъыияьзбгжмтвлк**  
**ьвзгфжямэуыаьлшдющпсрботчхйнёкие**  
**зглсьтхаёкжунчйодбщюрцмышфпэевяи**  
**оьсуеынхвчдиэрьальцгмйкфшжтёпябщюз**  
**ьяёпжзсеынмхкачфйуюцдвозьлгтщбшри**  
**ржыхиабксндутмеьцэшлопьюгёящзфйвч**  
**кцтврыуеампдюйбхэщчшжъёялиьзнгсфо**  
**цэтсфдьгюмыжеовблхучёькрийяппазщш**

эотывхжизючдлпщъашруеямбгфьцкёйис  
шсючёобдйъркепфэухаляжцмнштиьвзыг  
ъщгфбцешлвютйожзкрёяхчндимыуэпяс  
трэчацксёьгъщульжфгхндьбпвеюмзяишо

но неизвестно, в каком порядке эти диски были установлены в шифраторе. Кроме того, Виктору удалось перехватить сообщение, зашифрованное с помощью данного шифратора:

**мжцьёефхкарзжы хшэбпъмряычцюф.**

Восстановите вторую часть исходного сообщения, если известно, что в первой части зашифрован текст «алисаибобзнают».

**9. (10 баллов)** Известно, что некоторая фраза записана на 5 языках без знаков препинания и пробелов: на белорусском, русском, английском, немецком и латинском. Сообщение было передано с помощью азбуки Морзе (для кодировки сообщения на языках с соответствующими алфавитами использовались стандартные таблицы кода Морзе; для белорусского языка использовалась приведенная таблица с заменой «і» на «и» и «ѣ» на «щ»). Известно, что в каждой букве каждого сообщения оператор произвел произвольное количество замен точки на тире, либо тире на точку (соответственно произошла замена каждой буквы сообщения на какую-то другую).

Полученное сообщение на английском языке:

**МАЕСТНТSNAINMWONKEFTURGWIAGETGKROKIDONEPKDUNAWEQTRSUWDMGSWU**

Полученное сообщение на немецком языке:

**MNIMQIADKIKUIGSWKEKMOUIWUSKEUIDHTNKDEEDMGUIWGWKDEONGDKEE**

Полученное сообщение на латинском языке:

**ANVKMAFNQAWTKIEZTGCWNTTEZTGCWNTKIEIJWGGTWNTEGTWDTKIEZTGCWN**

Полученное сообщение на русском языке:

**ДАНЖИПТЩШЗКВЦГУДМАКПДУВХЪЖКДЫКУННВФДУВЖЯЮРЗВД**

Полученное сообщение на белорусском языке:

**МИЛИХНЕГСЖЬПВКПРУМАКЗГУНШЖЬДГХСКММЬВКНАЛХЖВРПСУИ**

Восстановите фразу на любом удобном для Вас языке.

A	● ■■	N	■■ ●	А	■ ■■	Р	● ■■ ●
B	■■ ●●●	O	■■■■ ■■	Б	■ ●●●	С	●●●
C	■■ ●■■●	P	● ■■■■ ●	В	● ■■■	Т	■
D	■■ ●●	Q	■■■■ ●■■■	Г	■ ■■●	У	●●■■
E	●	R	● ■■ ●	Д	■ ●●	Ф	●●■■●
F	●●■■■●	S	●●●	Е	●	Х	●●●●
G	■■■■ ●	T	■	Ж	●●●■■	Ц	■■■■■●
H	●●●●	U	●●■■■	З	■ ■■■●	Ч	■■■■■■●
I	●●	V	●●●■■■	И	●●	Ш	■■■■■■■■
J	●■■■■■■■	W	●■■■■■	Й	●■■■■■■■	Щ	■■■■■■■■■
K	■■■●■■	X	■■■●●■■■	К	■■■■■■■	Ъ	■■■■■■■■■
L	●■■■●●	Y	■■■●■■■■■	Л	●■■■●●	Ы	■■■■■■■■■
M	■■■■	Z	■■■■●●●	М	■■■■	Ь	■■■■■■■■■
				Н	■■■■	Э	●●●■■■■●●●
				О	■■■■■■■	Ю	●●■■■■■
				П	●■■■■■	Я	●■■■■■

Рисунок 2. – Стандартные таблицы кода Морзе