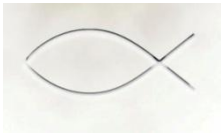
Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

7-9 классы **Заключительный этап** **2021-2022**

Задания, ответы и критерии оценивания

Шифрование — то есть сокрытие информации — появилось еще в древние времена. А уж когда возникли государства, армии, войны, разведка — то возникла необходимость тайно передавать какие-то сведения, чтобы, если вдруг они попадутся в руки врагу, тот ничего бы не понял. Нужны были тайные знаки, чтобы узнавать своих. Например, разрезали на части монету. Люди могли никогда друг друга не видеть, но если посланец предъявлял свою половинку, и при наложении обе части совпадали, значит, это свой.

А еще такой секретный знак был у первых христиан — в те века, когда за исповедание христианской веры тебя могли казнить. Как христиане могли узнавать своих — так, чтобы никто их не заподозрил и не выдал властям? У христиан был священный знак, символическое изображение рыбы (потому что если прочитать первые буквы фразы по-гречески «Иисус Христос Божий Сын Спаситель», то получалось греческое слово «ихтис», что значило рыба). Поэтому один христианин мог начертить тростью на земле дугу — сама по себе дуга еще ничего не обозначала. Но второй христианин в ответ на это чертил другую дугу, которые вместе складывались в изображение рыбы. Вот так:



И оба понимали, что они — единоверцы. А со стороны никто бы ничего не понял.

В древности люди еще и придумывали «тайные языки», на которых можно было устно разговаривать, и никто из посторонних не мог понять эту «тарабарщину». В старину на Руси были такие люди, которые назывались *офени*. Это бродячие торговцы разным мелким товаром — гребнями, бусами, нитками, пуговицами, ленточками, иголками, ножницами и так далее. Но они не только занимались торговлей, но подчас выведывали разные тайны, то есть торговля у них служила лишь прикрытием для разведки. И вот между собой они говорили на специальном языке — брали слово и переставляли местами слоги. Если слово двусложное, то сперва говорили второй слог, потом первый. Не «палка», а «капал», не «рыба», а «бары». Если слово трехсложное, то сперва говорили третий слог, потом второй, потом первый. Вместо «рыбалка» было «кабалры». Ну и так далее.

Были и другие старинные шифры. Например, слова писались не слева направо, а справа налево. Не «капуста», а «атсупак», не «бабушка», а «акшубаб». Еще в старину часто использовали шифр, когда буквы в слове писались в зеркальном отражении. Прочитать такой текст можно было, только поднеся его к зеркалу:

ЗИМА	AMNƎ
Сугробы навалило стометровые, Льдом прихватило реки и пруды, От дома дяди Кузьмича сурового Осталась только дырка от трубы.	Сугробы навалило стометровые, Льдом прихватило реки и пруды, От дома дяди Кузьмича сурового Осталась только дырка от трубы.

Но это всё довольно простые шифры, которые очень легко разгадать. Вскоре их стали понимать многие и потребовался другой, секретный канал передачи сообщений — прежде всего, в военных целях. С тех пор люди соревнуются в изобретении самых защищенных способов шифрования информации.

Шифрование сообщение происходит для защиты содержимого. Получается, что всегда есть лица, заинтересованные в данных сведениях. Люди в любом случае добиваются успехов, находя способы расшифровки кодов. Соответственно, криптография адаптируется.

В современном виде криптография далека от банальной перестановки букв по алфавиту. Головоломки имеют невероятный уровень сложности, и их решение требует огромных вычислительных

мощностей. Вместо простого смещения буквы подменяются числами, символами и проходят сотни или тысячи шагов.

С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

Сфера использования криптографии расширяется, при этом власти различных стран пытаются удержать контроль над использованием шифров. Разработки криптографов засекречиваются, от производителей шифровальных машин требуют оставлять в продуктах «черные ходы» для доступа спецслужб.

Параллельно независимые криптоаналитики разрабатывают способы шифрования, которыми могли бы пользоваться все желающие – так называемую открытую криптографию. Особенно актуально это стало с развитием интернета, где вопрос конфиденциальности информации встал очень остро. Первой криптосистемой с открытым ключом считается созданный в 1977 году алгоритм RSA, название которого является акронимом имен создателей – Риверста, Шамира и Адельмана. А в 1991 году американский программист Филипп Циммерман разрабатывает популярнейший пакет PGP с открытым исходным кодом для шифрования электронной почты.

Распространение доступного интернета по всему миру невозможно представить без криптографии. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка. Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Будущее этой науки творится на наших глазах – очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется.

Требования к оформлению заданий. При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

Задание 1. *(Максимум 14 баллов)* Для шифровки текста его записали в таблицу построчно. В каждую ячейку таблицы записывалось по одному символу. Для сокращения текста пробелы были опущены. Вместо знаков препинания были записаны буквенные последовательности ТЧК (точка) и ЗПТ (запятая). После чего столбцы были переставлены и получилась следующая таблица. Требуется расшифровать исходное сообщение.

Я	Н	Л	В	К	Р	А	Д	О	Е	Т	Е	Р	Г	О	М	И	З	Я	Е
Й	Л	Т	А	Л	Ф	Ы	И	П	Е	У	И	О	О	Г	Е	Д	Б	О	Р
Ч	Р	Д	Ч	И	Е	С	М	О	Н	Д	К	Х	И	Н	Т	И	К	Е	О
Н	У	Л	А	Е	Р	Е	Б	Ы	Ы	Е	Е	З	И	О	Н	Н	Ы	Ч	Д
С	Ж	С	Е	И	Н	У	П	Т	Л	Т	Н	З	В	Я	О	Е	Л	И	Щ
Ы	К	Д	О	-	М	Ч	П	Т	-	-	А	-	И	П	Т	-	Т	-	Л

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	0	Перепутаны местами слова «дипломаты» и «священнослужители»
2	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
3	2	Определено, что в конце текста символ ТЧК и таким образом столбцы таблицы поделены на части
4	14	Приведено достаточное решение, получен верный ответ

Ответ: Долгое время занятие криптографией было уделом одиночек. Среди них были одаренные ученые, священнослужители, дипломаты.

Задание 2. *(Максимум 12 баллов)* Сообщение из 10 букв было зашифровано следующим образом: каждой букве присвоена цифра, соответствующая ее порядковому номеру (от 0 до 9). В выражениях, представленных ниже, цифры заменены на соответствующие им буквы. Найдите такие значения, при которых равенства будут верными, и восстановите исходное сообщение.

МИ	*	Я	=	МРМ
+		*		-
ТТ	+	Т	=	ИК
=		=		=
ЕДР	+	АО	=	ЕАИ

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	+1	За каждую верно определенную цифру
3	12	Приведено достаточное решение, получен верный ответ

Ответ: д – 0, е – 1, м – 2, о – 3, к – 4, р – 5, а – 6, т – 7, и – 8, я – 9.
Зашифрованное слово: ДЕМОКРАТИЯ.

Задание 3. *(Максимум 11 баллов)* Шифрование сообщения заключается в замене каждого его символа другим символом согласно таблице.

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

При шифровке слова ЗВЕЗДА получится комбинация ШЮЬШЫЧ. Если зашифровать полученное сообщение с помощью таблицы еще раз, то получится ИГЖИЕА. Сколько всего различных комбинаций получится, если шифровать слово ГАДИНА неограниченное количество раз?

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	2	Верно выписаны циклы
3	3	Выписаны циклы и найдена их длина
4	7	Допущена арифметическая ошибка при нахождении НОК длин циклов
5	11	Приведено достаточное решение, получен верный ответ

Ответ: г –> э –> с –> в –> ю –> г (длина 5)

а –> ч –> а (длина 2)

д –> ы –> е –> ь –> ж –> щ –> о –> д (длина 7)

и –> ц –> к –> х –> л –> ф –> м –> у –> п –> т –> р –> з –> ш –> и (длина 13)

н –> б –> я –> н (длина 3)

Все числа простые, НОК находится умножением: 5*2*7*13*3 = **2730**

Задание 4. *(Максимум 15 баллов)* Рассмотрим один из классических шифров замены – шифр Виженера. Пускай имеется сообщение X длиной n символов. Тогда все его символы можно обозначить как $x_1, x_{2,\dots,} x_n$. Также имеется ключ K длиной m, причем m<n. Обозначим символы ключа как $k_1, k_{2,\dots,} k_m$. Для шифровки сообщения необходимо записать ключ K друг за другом несколько раз так, чтобы длина полученной последовательности $k_1, k_{2,\dots,} k_m, k_1, k_{2,\dots}$ была равна n. Сообщение шифруется посимвольно: к коду первого символа сообщения добавляется код первого символа ключевой последовательности, к коду второго символа сообщения – код второго символа последовательности и т.д. Затем полученные цифры заменяются на соответствующие им буквы алфавита. Если полученная сумма была больше 32, то берется ее остаток от деления на 33.

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	27	29	30	31	32

Требуется расшифровать закодированное шифром Виженера сообщение:
ЩУФКДРШШЙДРТФКЧЯХХФОМУК. Ключ ЛОЖКА.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	• Написан верный ответ без решения, либо решение есть, но ответ из него не следует • Ключ и шифр-текст верно преобразованы в числовые комбинации
2	6	Ход решения верный, но допущены арифметические ошибки
3	15	Приведено достаточное решение, получен верный ответ

Ответ:

Щ	У	Ф	К	Д	Р	Ш	Ш	Й	Д	Р	Т	Ф	К	Ч	Я	Х	Х	Ф	О	М	У	К
26	20	21	11	4	17	25	25	10	4	17	19	21	11	24	32	22	22	21	15	13	20	11
Л	О	Ж	К	А	Л	О	Ж	К	А	Л	О	Ж	К	А	Л	О	Ж	К	А	Л	О	Ж
12	15	7	11	0	12	15	7	11	0	12	15	7	11	0	12	15	7	11	0	12	15	7

Вычитаем из 2-го столбца четвертый

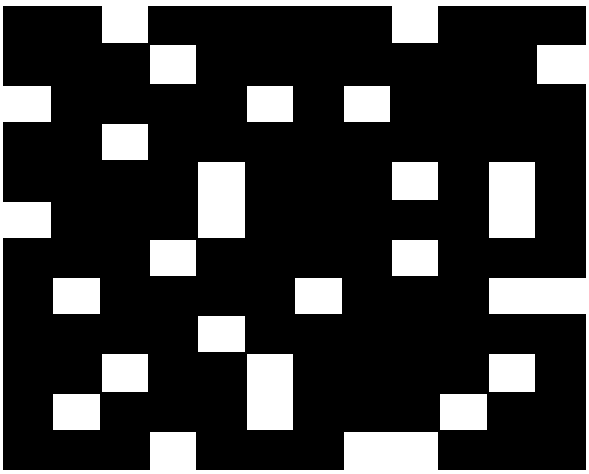
14	5	14	0	4	5	10	18	32	4	5	4	14	0	24	20	7	15	10	15	1	5	4
Н	Е	Н	А	Д	Е	Й	С	Я	Д	Е	Д	Н	А	Ч	У	Ж	О	Й	О	Б	Е	Д

Не надейся дед на чужой обед

Задание 5. *(Максимум 8 баллов)* В предыдущих заданиях были рассмотрены способы криптографического шифрования. Их основой является изменение текста таким образом, чтобы не была понятна его суть. Существует также другой метод – стеганография. Данный метод позволяет не изменять передаваемое сообщение, а спрятать его среди другой информации. При сокрытии информации таким методом используют стеганографические решетки – это прямоугольные сетки, в которых прорезаны квадратики. Такая решетка накладывается на лист бумаги и в ее отверстия записываются буквы сообщения без пробелов и знаков препинания(по одной в каждое), после чего решетка убирается и в оставшиеся клетки дописывают случайные символы. Расшифровать скрытый текст может только владелец такой же решетки.

В данном задании стенографическая решетка была приложена к листу бумаги 2 раза (в исходном виде, а затем повернутая на 90º. Требуется расшифровать закодированное сообщение.

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



Критерии оценивания:

Номер критерия	Кол-во баллов	Описание
1	2	Если решетка была приложена 1 раз
2	8	Получен верный ответ

Ответ: При первом наложении решетки: Стеганография позволяет тайно пер
При повороте на 90 градусов и втором наложении: едать информацию без её шифрования
Стеганография позволяет тайно передать информацию без её шифрования

Практическое задание. *(Максимум 40 баллов)* Не смотря на кажущуюся эффективность шифры замены легко поддаются взлому, в том числе методом частотного анализа. В тексте на любом языке разные символы попадаются с различной частотой. Например, в русском языке чаще всего в текстах встречаются буквы: О, А, И, Т, В, Е, Л. Таким образом, проанализировав частоту появления символа, можно предположить какой именно букве он соответствует. Также при расшифровке текста следует обратить внимание на сочетания букв, союзы и приставки.

В представленном ниже тексте буквы русского алфавита заменены на другие символы, причем одинаковым буквам соответствуют одинаковые символы. Пунктуация в тексте сохранена. Требуется расшифровать исходный текст, при условии, что буквы Е и Ё заменены одним символом, а также в тексте встречается слово «книжки».

Afsyktdm df*m+f, +t+ hwzdjf =jlkq *ld>d! Bl yzal* q fx*qbydmzq, +t+ +tb>+y*w +fbv>*>zm > aj>u*t afjt >sd> = u+f*y. Cl*fl *ldf q df*m+f > sl*t*, vdf hlxt* af y*>ctk st >xjt* = nydhf*, t f +b>r+te strl afgthw* syktdm. Df lzdm q v>dt* >bfxst +b>r+>, df*m+f bl yvlhbwl, t +t+>l-b>hysm z+tg+> >*> jtzz+tgw, t dt+ vdfh afgtb>ktdmzq af jyzz+fky qgw+y >*> af tj>nkld>+l – pdfxf bl hw*f. Af jyzz+fky q > dt+ efjfuf yv>*zq, t tj>nkld>+> bl *oh>*. Eyrl =zlxf s*q klbq hw*f – pdf gtstv> jlutdm. F*mxt B>+f*tl=bt strl efdl*t stdm kbl jthfdy bt *ldf af tj>nkld>+l, bf afdfk afrt*l*t > aljl=l*t = vld=ljdwi +*tzz dt+, hlg jthfdw.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	4	Правильно найдено слово «книжки»
3	+1	За каждую верно расшифрованную букву кроме К, Н, И, Ж
4	40	Верно расшифрован весь текст, приведено обоснование решения

Ответ: Слово КНИЖКИ зашифровано как +b>r+>. Т.о. + – к, b – н, > – и, r – ж.

Зашифрованный текст:

Подумать только, как быстро время летит! Не успел я оглянуться, как каникулы кончились и пришла пора идти в школу. Целое лето я только и делал, что бегал по улицам да играл в футбол, а о книжках даже позабыл думать. То есть я читал иногда книжки, только не учебные, а какие-нибудь сказки или рассказы, а так чтоб позаниматься по русскому языку или по арифметике - этого не было. По русскому я и так хорошо учился, а арифметики не любил. Хуже всего для меня было - это задачи решать. Ольга Николаевна даже хотела дать мне работу на лето по арифметике, но потом пожалела и перевела в четвертый класс так, без работы.

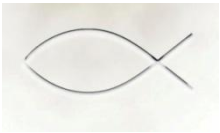
Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

10-11 классы **Заключительный этап** **2021-2022**

Задания, ответы и критерии оценивания

Шифрование — то есть сокрытие информации — появилось еще в древние времена. А уж когда возникли государства, армии, войны, разведка — то возникла необходимость тайно передавать какие-то сведения, чтобы, если вдруг они попадутся в руки врагу, тот ничего бы не понял. Нужны были тайные знаки, чтобы узнавать своих. Например, разрезали на части монету. Люди могли никогда друг друга не видеть, но если посланец предъявлял свою половинку, и при наложении обе части совпадали, значит, это свой.

А еще такой секретный знак был у первых христиан — в те века, когда за исповедание христианской веры тебя могли казнить. Как христиане могли узнавать своих — так, чтобы никто их не заподозрил и не выдал властям? У христиан был священный знак, символическое изображение рыбы (потому что если прочитать первые буквы фразы по-гречески «Иисус Христос Божий Сын Спаситель», то получалось греческое слово «ихтис», что значило рыба). Поэтому один христианин мог начертить тростью на земле дугу — сама по себе дуга еще ничего не обозначала. Но второй христианин в ответ на это чертил другую дугу, которые вместе складывались в изображение рыбы. Вот так:



И оба понимали, что они — единоверцы. А со стороны никто бы ничего не понял.

В древности люди еще и придумывали «тайные языки», на которых можно было устно разговаривать, и никто из посторонних не мог понять эту «тарабарщину». В старину на Руси были такие люди, которые назывались *офени*. Это бродячие торговцы разным мелким товаром — гребнями, бусами, нитками, пуговицами, ленточками, иголками, ножницами и так далее. Но они не только занимались торговлей, но подчас выведывали разные тайны, то есть торговля у них служила лишь прикрытием для разведки. И вот между собой они говорили на специальном языке — брали слово и переставляли местами слоги. Если слово двусложное, то сперва говорили второй слог, потом первый. Не «палка», а «капал», не «рыба», а «бары». Если слово трехсложное, то сперва говорили третий слог, потом второй, потом первый. Вместо «рыбалка» было «кабалры». Ну и так далее.

Были и другие старинные шифры. Например, слова писались не слева направо, а справа налево. Не «капуста», а «атсупак», не «бабушка», а «акшубаб». Еще в старину часто использовали шифр, когда буквы в слове писались в зеркальном отражении. Прочитать такой текст можно было, только поднеся его к зеркалу:

ЗИМА	Сугробы навалило стометровые, Льдом прихватило реки и пруды, От дома дяди Кузьмича сурового Осталась только дырка от трубы.

Но это всё довольно простые шифры, которые очень легко разгадать. Вскоре их стали понимать многие и потребовался другой, секретный канал передачи сообщений — прежде всего, в военных целях. С тех пор люди соревнуются в изобретении самых защищенных способов шифрования информации.

Шифрование сообщение происходит для защиты содержимого. Получается, что всегда есть лица, заинтересованные в данных сведениях. Люди в любом случае добиваются успехов, находя способы расшифровки кодов. Соответственно, криптография адаптируется.

В современном виде криптография далека от банальной перестановки букв по алфавиту. Головоломки имеют невероятный уровень сложности, и их решение требует огромных вычислительных мощностей. Вместо простого смещения буквы подменяются числами, символами и проходят сотни или тысячи шагов.

С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

Сфера использования криптографии расширяется, при этом власти различных стран пытаются удержать контроль над использованием шифров. Разработки криптографов засекречиваются, от производителей шифровальных машин требуют оставлять в продуктах «черные ходы» для доступа спецслужб.

Параллельно независимые криптоаналитики разрабатывают способы шифрования, которыми могли бы пользоваться все желающие – так называемую открытую криптографию. Особенно актуально это стало с развитием интернета, где вопрос конфиденциальности информации встал очень остро. Первой криптосистемой с открытым ключом считается созданный в 1977 году алгоритм RSA, название которого является акронимом имен создателей – Риверста, Шамира и Адельмана. А в 1991 году американский программист Филипп Циммерман разрабатывает популярнейший пакет PGP с открытым исходным кодом для шифрования электронной почты.

Распространение доступного интернета по всему миру невозможно представить без криптографии. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка. Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Будущее этой науки творится на наших глазах – очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется.

Пояснение к заданиям. Для шифрования фразы сначала записываются в одну строку без использования пробелов. После чего выполняется шифрование фразы. При дешифрации соответственно получается строка без пробелов. Правильным ответом считается как данная строка, так и первоначальная фраза.

Все вычисления производятся в кольце вычетов. Для того, чтобы понять: что же такое кольцо вычетов, необходимо представить циферблат часов. На обыкновенных часах со стрелкой 12 делений, таким образом получается 12 чисел. Только, в отличие от часов, в криптографии нумерация начинается с нуля. Получается, что циферблат можно представить так: 0, 1, 2, ..., 11. Этот циферблат называется кольцо вычетов с 12 числами или Z_{12}. Размеры циферблата могут быть разными, т.е. существует много разных систем. В данных заданиях используются два кольца: Z_{26} (латинский алфавит) и Z_{33} (русский алфавит). Операция «добавление единицы» в кольце вычетов «зацикливается», т.е если к последнему числу кольца прибавить единицу, то мы получим 0 (первое число). Для Z_{12}, например, 11+1 = 0. Проще говоря, если при совершении операций в кольце Z_{12} мы получаем число, больше либо равное 12, то необходимо вычитать из него 12 до тех пор, пока не получится число, входящее в данное кольцо. Например, при умножении 11*7 получается число 77. Данное число можно представить как 12*6+5. Таким образом, в кольце Z_{12} результатом умножения 11*7 является число 5.

Открытый текст (текст до шифрования) представляется как $X = (x_1, x_2, x_3, \ldots, x_n)$

Шифртекст (текст после шифрования) представляется как $Y = (y_1, y_2, y_3, \ldots, y_n)$

Символ		Индекс	Двоичная запись
Лат.	Рус.		
A	А	0	00000
B	Б	1	00001
C	В	2	00010

Символ	ASCII
a	97
b	98
c	99

D	Г	3	00011
E	Д	4	00100
F	Е	5	00101
G	Ё	6	00110
H	Ж	7	00111
I	З	8	01000
J	И	9	01001
K	Й	10	01010
L	К	11	01011
M	Л	12	01100
N	М	13	01101
O	Н	14	01110
P	О	15	01111
Q	П	16	10000
R	Р	17	10001
S	С	18	10010
T	Т	19	10011
U	У	20	10100
V	Ф	21	10101
W	Х	22	10110
X	Ц	23	10111
Y	Ч	24	11000
Z	Ш	25	11001
+	Щ	26	11010
*	Ъ	27	11011
!	Ы	28	11100
1	Ь	29	11101
2	Э	30	11110
3	Ю	31	11111
4	Я	32	100000

d	100
e	101
f	102
g	103
h	104
i	105
j	106
k	107
l	108
m	109
n	110
o	111
p	112
q	113
r	114
s	115
t	116
u	117
v	118
w	119
x	120
y	121
z	122

Требования к оформлению заданий. При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

Задание 1. *(Максимум 14 баллов)* Ключом в шифре Хилла является пара матриц:

$A = \begin{pmatrix} 3 & 7 \\ 1 & 9 \end{pmatrix}$, $B = \begin{pmatrix} 10 \\ 4 \end{pmatrix}$. Расшифровать сообщение РДОИШИЙЮЩЭ.

Пояснение к задаче 1. Шифрование. Открытый текст разбивается на блоки длины **m** (где **m** – количество символов в матрице B) и каждый блок ($x_1,\ldots,x_m$) шифруется по правилу

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \boldsymbol{A}\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} + \boldsymbol{B}.$$

Расшифровка. Шифртекст разбивается на блоки длины **m** и каждый блок ($y_1,\ldots, y_m$) расшифровывается по правилу $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \boldsymbol{A^{-1}}\left(\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} - \boldsymbol{B}\right)$, где $\boldsymbol{A^{-1}}$ – обратная матрица.

Операции с матрицами: Матрица A – это матрица с элементами a_{ij}. Все элементы матрицы обозначаются следующим образом: a_{ij}, где i – номер строки, а j – номер столбца.

Сложение матриц (сумма матриц) **A + B** есть операция вычисления матрицы C, все элементы которой равны попарной сумме всех соответствующих элементов матриц **A** и **B**, то есть каждый элемент матрицы **C** равен: $c_{ij} = a_{ij} + b_{ij}$.

Вычитание матриц (разность матриц) **A - B** есть операция вычисления матрицы **C**, все элементы которой равны попарной разности всех соответствующих элементов матриц **A** и **B**, то есть каждый элемент матрицы **C** равен: $c_{ij} = a_{ij} - b_{ij}$.

Умножение матрицы **A** *на число* **k** есть операция вычисления матрицы **C**, все элементы которой равны произведению всех соответствующих элементов матрицы **A** на число **k**, то есть каждый элемент матрицы **C** равен: $c_{ij} = k * a_{ij}$.

Произведением двух матриц A размером m*p и *B* размером p*n называется матрица *C размером* m*n, элемент которой, находящийся на пересечении *i*-й строки и *j*-го столбца, равен сумме произведений элементов *i*-й строки матрицы *A* на соответствующие (по порядку) элементы *j*-го столбца матрицы *B*. Из этого определения следует формула элемента матрицы *C*: $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj}$.

Нахождение обратной матрицы для матрицы размером 2x2. $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

$A^{-1} = \frac{1}{det\ A}\tilde{A}^t$

$\det A = a_{11}a_{22} - a_{21}a_{12}$

$\frac{1}{det\ A}$ – число, которое при умножении на det A, дает 1 (Для данной задачи 1 – остаток от деления данного произведения по модулю 33. Например, 2*17=34, а 34(mod33)=1)

$\tilde{A} = \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix}$. В кольце не существует отрицательных чисел. Для получения эквивалентного положительного всегда можно добавить модуль (в данном случае это 33).

Для получения матрицы $\tilde{A}^t$ необходимо столбцы матрицы $\tilde{A}$ записать как строки. Например, из матрицы $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ получится матрица $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$.

Т.к. в данной задаче используется кольцо вычетов Z_{33}, то при получении элемента больше, чем 32 требуется взять его остаток от деления по модулю 33.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	• Написан верный ответ без решения, либо решение есть, но ответ из него не следует • Верный ход нахождения обратной матрицы, но есть арифметическая ошибка
2	3	Верно найдена обратная матрица
3	5	Ход расшифровки после нахождения обратной матрицы верный, но допущена арифметическая ошибка
4	14	Приведено достаточное решение, получен верный ответ

Ответ: Находим обратную матрицу:

detA = 20, 1/detA = 5

$\tilde{A} = \begin{pmatrix} 9 & -1 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 9 & 32 \\ 26 & 3 \end{pmatrix}$

$\tilde{A}^t = \begin{pmatrix} 9 & 26 \\ 32 & 3 \end{pmatrix}$

Т.о. находим обратную матрицу $A^{-1} = 5 * \begin{pmatrix} 9 & 26 \\ 32 & 3 \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix}$

РДОИШИЙЮЩЭ = (17, 4, 15, 9, 25, 9, 10, 31, 26, 30)

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \left(\begin{pmatrix} 17 \\ 4 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \begin{pmatrix} 7 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 31 \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \left(\begin{pmatrix} 15 \\ 9 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \begin{pmatrix} 5 \\ 5 \end{pmatrix} = \begin{pmatrix} 17 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \left(\begin{pmatrix} 25 \\ 9 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \begin{pmatrix} 15 \\ 5 \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \left(\begin{pmatrix} 10 \\ 31 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \begin{pmatrix} 0 \\ 27 \end{pmatrix} = \begin{pmatrix} 12 \\ 9 \end{pmatrix}$$

$$\begin{pmatrix} x_9 \\ x_{10} \end{pmatrix} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \left(\begin{pmatrix} 26 \\ 30 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix} * \begin{pmatrix} 16 \\ 26 \end{pmatrix} = \begin{pmatrix} 8 \\ 13 \end{pmatrix}$$

Получаем (18, 31, 17, 17, 5, 0, 12, 9, 8, 13) = **СЮРРЕАЛИЗМ**

Задание 2. *(Максимум 10 баллов)* Имеется криптограмма HTSLWFYZQFYNTSX. Найдите исходное сообщение, если известно, что преобразование заключается в следующем. Пусть x_1, x_2 – корни трехчлена $x^2 + 5x + 2$. К индексу каждой буквы шифруемого сообщения прибавлялось значение выражения $f(x) = x^6 + 5x^5 + 2x^4 + 2x^3 + 13x^2 + 19x + 11$ вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	2	Верно выполнено деление многочленов
3	10	Приведено достаточное решение, получен верный ответ

Ответ: При делении многочленов получаем, что $f(x) = (x^2 + 5x + 2)(x^4 + 2x + 3) + 5$

H	T	S	L	W	F	Y	Z	Q	F	Y	N	T	S	X
7	19	18	11	22	5	24	25	16	5	24	13	19	18	23
2	14	13	6	17	0	19	20	11	0	19	8	14	13	18
C	O	N	G	R	A	T	U	L	A	T	I	O	N	S

CONGRATULATIONS

Задание 3. *(Максимум 11 баллов)* Для шифра RSA n=33, e=7. Расшифровать ЧЛНКМЗЪЁЬЯВР

Пояснение к заданию 3. Криптографическая сложность RSA основана на трудности задачи о факторизации. Для генерации ключей данного шифра выбирают два простых числа таких, чтобы удовлетворялось условие n = p * q. Затем вычисляется m = (p – 1) (q – 1). Выбираются числа c и e, такие что c * e = 1 (mod m). Пара чисел (n,e) – открытый ключ, а c – секретный. Шифруется текст посимвольно.

Шифрование. $x \rightarrow y = x^e (mod\ n)$

Расшифровка. $y \rightarrow x = y^c (mod\ n)$

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	• Написан верный ответ без решения, либо решение есть, но ответ из него не следует • Правильно найден ключ c
2	3	Ход решения верный, но допущена арифметическая ошибка
3	11	Приведено достаточное решение, получен верный ответ

Ответ: n = 3 * 11, значит m = 20

c * e = 1 (mod m) –> **c = 3**

ЧЛНКМЗЪЁЬЯВР = (24, 12, 14, 11, 13, 8, 27, 6, 29, 32, 2, 17)

Расшифровка: $x_1 = y_1{}^c (\text{mod } n) = 24^3 (\text{mod } 33) = 30$

Аналогичным образом считаются остальные символы, получаем (30, 12, 5, 11, 19, 17, 15, 18, 2, 32, 8, 29) = **ЭЛЕКТРОСВЯЗЬ**

Задание 4. *(Максимум 11 баллов)* Сообщение шифруется путем побитового сложения по модулю два каждого символа передаваемой информации с символом ключа. Злоумышленник смог перехватить зашифрованное сообщение I!YMA*BJYE и уговорил пользователя переслать сообщение еще раз, добавив к сообщению «1» первым символом. В итоге получил новое сообщение: S3XMFDZWCMN. Требуется расшифровать исходное.

Пояснение к заданию 4. Побитовое сложение по модулю 2 (исключающее или). При сложении двух разных битов получается 1, иначе 0.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	• Написан верный ответ без решения, либо решение есть, но ответ из него не следует • Найден первый символ ключа
2	3	Найден весь ключ
3	11	Приведено достаточное решение, получен верный ответ

Ответ: S -> 10010, 1 -> 11101. Путем побитового сложения находим первый символ ключа 01111 -> P.

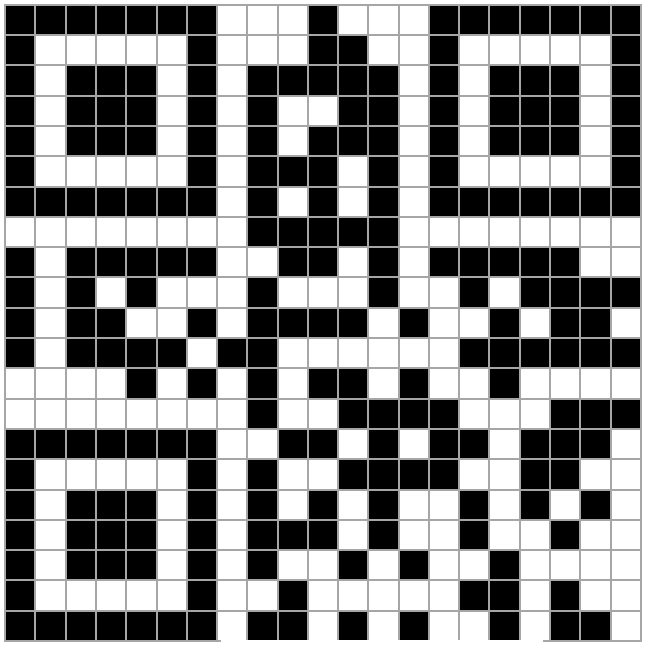
I -> 01000, P -> 01111. Находим 1 символ исходного сообщения 00111 -> H

H -> 00111, 3 -> 11111. Находим 2 символ ключа 11000 -> Y

Y -> 11000, ! -> 11100. Находим 2 символ сообщения 00100 -> E.

И т.д. Ключ **PYTHON**, сообщение **HELLOWORLD**

Задание 5. *(Максимум 14 баллов)* Требуется расшифровать QR-код.

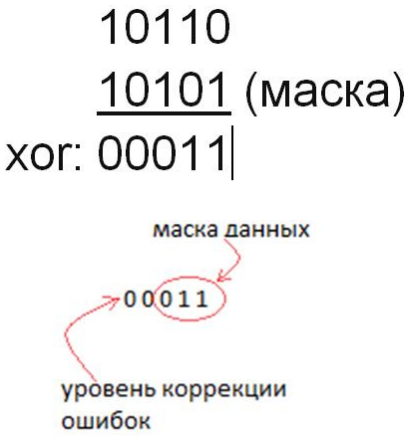


Пояснения к заданию 5. QR-код. Взглянув на картинку, можно заметить несколько отчётливых областей. Эти области используются для детектирования QR кода. Эти данные не представляют интереса с точки зрения записанной информации, но их нужно вычеркнуть или просто запомнить их расположение, чтобы они не мешали. Всё остальное поле кода несёт уже полезную информацию. Её можно разбить на две части: системная информация и данные. Также существует информация о версии кода. От версии кода зависит максимальный объём данных, которые могут быть записаны в код. При повышении версии – добавляются специальные блоки. Коды высоких версий обычно нецелесообразно считывать вручную.

Размещение системной информации показано на рисунке:

Системная информация дублируется, что позволяет значительно понизить вероятность возникновения ошибок при детектировании кода и считывании. Системная информация – это 15 бит данных, среди которых первые 5 — это полезная информация, а остальные 10 — это BCH(15,5) код, который позволяет исправлять ошибки в системных данных.

Чтение 5 бит системной информации. Как уже говорилось, интерес представляют только первые 5 бит. Из которых 2 бита показывают уровень коррекции ошибок, а остальные 3 бита показывают какая маска из доступных 8 применяется к данным. В рассматриваемом QR-коде системная информация содержит:



Маска для системной информации. Кроме уже озвученных схем защиты системной информации, вдобавок, используется статическая маска, которая применяется к любой системной информации. Она имеет вид: **101010000010010**. Так как имеет интерес только первые 5 бит, то маску можно сократить и легко запомнить: **10101** (десять — сто один). После применения операции «исключающего или» (xor) получаем информацию.

Возможные уровни коррекции ошибок:

L	01	~7%
M	00	~15%
Q	11	~25%
H	10	~30%

Возможные маски:

000	(i + j) mod 2 = 0
001	i mod 2 = 0
010	j mod 3 = 0
011	(i + j) mod 3 = 0
100	((i div 2) + (j div 3)) mod 2 = 0
101	(i j) mod 2 + (i j) mod 3 = 0
110	((i j) mod 2 + (i j) mod 3) mod 2 = 0
111	((i+j) mod 2 + (i j) mod 3) mod 2 = 0

Чтение заголовка данных. Чтобы понять с какими данными предстоит иметь дело, необходимо изначально прочитать 4-х битный заголовок, который содержит в себе информацию о режиме. Специфика чтения данных изображена на картинке:

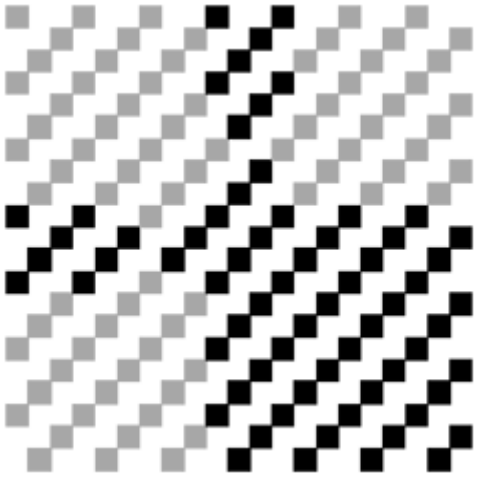
Читают «змейкой» снизу

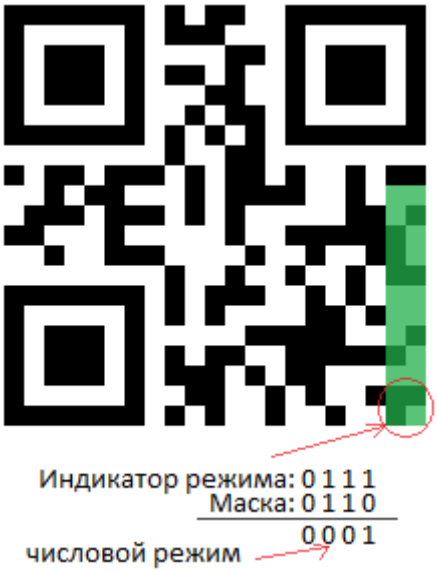
…	…
6	5
4	3
2	1

Список возможных режимов:

ECI	0111
Числовые	0001
Буквенно-числовые	0010
8-битный (байтный)	0100
Kanji	1000
Структурированное дополнение	0011
FNC1	0101 (1-я позиция) 1001 (2-я позиция)

После извлечения 4-х бит, описывающих режим, необходимо к ним применить маску. Маска определяется выражением, приведённым в таблице выше. Если данное выражение сводится к TRUE (верное) для бита с координатами *(i,j)*, то бит инвертируется, иначе всё остаётся без изменений. Начало координат в левом верхнем углу *(0,0)*. Взглянув на выражения, можно заметить в них закономерности. Для рассматриваемого QR-кода, маска будет выглядеть как на рисунке справа.





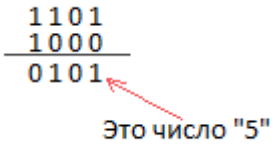
Получаем режим.

Чтение данных. После получения данных о режиме можно приступать к чтению информации. Надо оговорить, что наиболее интересно считывать числовые и буквенно-числовые данные, так как они легко интерпретируются. Но также не стоит бояться 8-битных. Это может быть также легко интерпретируемая информация. Например, многие онлайн генераторы QR текст кодируют в этом режиме, используя ASCII. Ещё одна причина, почему следует изначально прочитать режим, это то, что от него зависит количество пакетов данных. Которая также зависит и от версии кода. Для версий с первой по девятую длины блоков для более читабельных режимов:

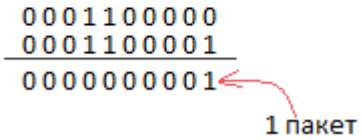
Числовые	10 бит / 4 бита
Буквенно-числовые	9 бит
8-битный (байтный)	8 бит

Первый блок после указателя режима — это количество символов (в двоичном виде). Для числового режима количество закодировано в 10 следующих битах, а для 8-битного режима в 8 битах.

Продолжаем чтение вышестоящих битов и получаем



На рисунке видно, что в QR-коде записана цифра 5. Это видно по указателю количества символов и последующим после него 4 битам. В числовом режиме наряду с 10-битными блоками используются 4-х битные блоки для экономии места, если в 10-битном объёме нет необходимости.



В случае, если по левым двум столбикам не понятно, что за информация зашифрована (например, требуется не 1, а 5 пакетов данных), то расшифровку продолжают с использованием следующих двух, только меняется направление считывания. Производится аналогично «змейкой», но уже сверху:

2	1
4	3
6	5
…	…

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	2	Верно найдена маска данных
3	4	Верно прочитан заголовок
4	6	Верно определено число пакетов данных
5	8	Верно указана запись зашифрованного сообщения в двоичном виде
6	14	Приведено достаточное решение, получен верный ответ

Ответ: Первые 5 бит системной информации: 10111. Маска для системной информации 10101.

Т.о. получаем 00010, где 00 – уровень коррекции ошибок (~15%), **а 010 – маска данных j mod 3 = 0**

Заголовок – первые 4 бита информации 0100 (маска 0000) – **режим 8-ми битный**

По следующим 8-ми битам определяется число пакетов. **00000100** (маска 00000000) - **4 пакета (символа).**

Читаем 1 символ **01110011** (маска 00000000). В десятичной СИ это число 115. Из таблицы ASCII получаем символ «s».

Читаем 2 символ 01111110 (маска 00001010) -> **01110100** -> 116 -> «t»

Читаем 3 символ 11001011 (маска 10101010) -> **0110001** -> 97 -> «a»

Читаем 4 символ 11011000 (маска 10101010) -> **01110010** -> 114 -> «r»

Зашифрованное слово: **star**

Практическое задание. *(Максимум 40 баллов)* Не смотря на кажущуюся эффективность шифры замены легко поддаются взлому, в том числе методом частотного анализа. В тексте на любом языке разные символы попадаются с различной частотой. Таким образом, проанализировав частоту появления символа, можно предположить какой именно букве он соответствует.

В представленном ниже тексте буквы русского алфавита заменены на другие символы, причем одинаковым буквам соответствуют одинаковые символы. Пунктуация в тексте сохранена. Требуется расшифровать исходный текст.

E gnvkvl vqtrlrovq8 l yrhrqu nuqmvo8mv jnu3. Vns u45 pry sqqoujvlros hu4up2 s eqtrnvlsos, ctv lv3ts kv6nv tvo8mv cupuy Gorln2u lvpvtr, lqu 6u vqtro8n2u vtlupqtsb, luje4su l Gvpe (mpvku fvmvlv3 jlups), jrlnv yrlroun2 Qkvgvk, s vt nsd nu vqtrovq8 s qoujr. Hvitvke gnvk2 equpjnv lybosq8 empuhobt8 gorln23 ldvj s hpvmorj2lrt8 m nuke nvlea tpvhe. Lnetps nrxovq8 knv6uqtlv ovhrt, tvhvpvl s kvovtmvl, vqtrlxsdqb vt qtrpsnn2d pejvmvhvl s hovtnsmvl, r lv lqud itsd lsjrd prfvt gnvk2 hv-hpu6nuke nu ynros qufu prln2d.

Hvmr vns tpejsosq8, lvpvn2 hvqtvbnnv hpsnvqsos sk luqts. Trm, gnvk2 eynros, ctv mvpvo8 io8wvl hvlupneo m vyupe, — ynrcst, lpukb u45 uqt8. L2bqnsorq8 u45 vjnr hpsbtnrb nvlvqt8: e io8wvl efu6ros nuqmvo8mv hvns s qu3crq fpvjsos qrks hv qufu nr fupugrd F2qtpvtucnv3 pums nujroumv vt f2lxugv orgupb gnvkvl, gju qvdprnsosq8 mvu-mrmsu yrhrq2 hpvlsyss. Lvpvn vtl5o tejr Wsos s Msos, vns hv3kros hvns s hpsluyos nr nsd lq5, ctv qkvgos.

Для частотного анализа можно использовать представленный ниже фрагмент текста.

Странное дело: о том, что хорошо, о днях, которые провёл приятно, рассказывается скоро, и слушать про них не так уж интересно. А вот про то, что неприятно, что вызывает страх или отвращение, рассказы получаются долгими и захватывающими. Путешественники провели в гостеприимном доме немало дней, по меньшей мере четырнадцать, и покидать его им не хотелось. Бильбо с радостью оставался бы там ещё и ещё, даже если бы мог без всяких хлопот по одному только желанию перенестись домой, в хоббичью норку. И всё же рассказать об их пребывании там почти нечего. Хозяин дома Элронд был друг эльфов и предводитель тех людей, у которых в предках числились эльфы и открыватели Севера. Он был благороден и прекрасен лицом, как повелитель эльфов, могуч, как воин, мудр, как колдун, величествен, как король гномов, и добр, как нежаркое лето. Дом Элронда был само совершенство; там было хорошо всем – и тем, кто любит поесть и поспать, и тем, кто любит трудиться, и кто любит слушать или рассказывать истории, петь или просто сидеть и думать, и тем, кому нравится всё понемножку.

Критерии оценивания:

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения, либо решение есть, но ответ из него не следует
2	4	За составление частотной таблицы
3	+1	За каждую верно расшифрованную букву
4	40	Верно расшифрован весь текст, приведено обоснование решения

Ответ:

У гномов оставалось в запасе несколько дней. Они еще раз исследовали пещеры и установили, что войти можно только через Главные ворота, все же остальные отверстия, ведущие в Гору (кроме боковой двери), давно завалены Смогом, и от них не осталось и следа. Поэтому гномы усердно взялись укреплять главный вход и прокладывать к нему новую тропу. Внутри нашлось множество лопат, топоров и молотков, оставшихся от старинных рудокопов и плотников, а во всех этих видах работ гномы по-прежнему не знали себе равных.

Пока они трудились, вороны постоянно приносили им вести. Так, гномы узнали, что король эльфов повернул к озеру, - значит, время еще есть. Выяснилась еще одна приятная новость: у эльфов убежали несколько пони и сейчас бродили сами по себе на берегах Быстротечной реки недалеко от бывшего лагеря гномов, где сохранились кое-какие запасы провизии. Ворон отвел туда Фили и Кили, они поймали пони и привезли на них все, что смогли.