Решения предложенных задач оформляются в электронном виде и высылаются на электронный адрес 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 Олимпиады по математике и криптографии

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 (цифра 4 не зашифрована):

ЦИФРА * 4 = АРФИЦ.

В ответе укажите все возможные исходные выражения, которые могли быть зашифрованы таким образом.

2. Транспозиционное преобразование заключается в следующем: буквенный текст разбивается на блоки по 20 букв в каждом. Буквы одного блока записываются построчно в таблицу 4 X 5, а затем переписываются по столбцам. Это и есть зашифрованный блок. Например:

ЗАДАЧАПОКРИПТОГРАФИИ

⇩

З	**А**	**Д**	**А**	**Ч**
А	**П**	**О**	**К**	**Р**
И	**П**	**Т**	**О**	**Г**
Р	**А**	**Ф**	**И**	**И**

⇩

ЗАИРАППАДОТФАКОИЧРГИ

а) (1 балл) Покажите, что обратное преобразование (расшифрование) также будет транспозиционным. В ответе укажите, какую таблицу следует применить для расшифрования.

б) (3 балла) Блок текста зашифрован последовательно n раз. При каком минимальном $n > 1$ он окажется незашифрованным?

3. (3 балла) Секретный PIN-код является четырехзначным числом. Известно, что при его делении на 30, 31, 33 получены остатки 10, 4, 28 соответственно. Найдите PIN.

4. (4 балла) Виктору стало известно, что Алиса для входа в систему использует пароль, состоящий из 10 символов, при этом Алиса использует только 4 различных символа (C, A, G, T), и один из символов в пароле встречается в точности 5 раз. Сколько паролей необходимо перебрать Виктору, чтобы гарантировано угадать пароль Алисы?

5. Шифр простой замены представляет собой алгоритм побуквенного зашифрования текста с помощью таблицы замены. Каждая буква открытого (зашифровываемого) текста заменяется соответствующей (стоящей под ней в таблице) буквой из таблицы. Например, слово «ГДЕ» будет зашифровано с помощью Таблицы замены 1 в слово «ВФЙ».

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	…	э	ю	я
д	о	п	в	ф	й	у	е	г	ш	з	х	щ	б	т	…	м	ч	ц

Таблица замены 1.

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

а) (1 балл) При условии, что шифр простой замены составляется для русского языка, алфавит которого состоит из 32 букв (е и ё считаются как одна буква), какое количество различных ключей (таблиц замены) можно составить?

б) (2 балла) При условии, что на Земле скоро будет проживать 7.000.000.000 человек, хватит ли уникальных (не повторяющихся) ключей для каждой возможной пары людей?

6. (3 балла) Шифр простой замены, например, для английского языка может быть реализован с помощью диска с перепайками: с каждой стороны диска расположены по кругу 26 контактов, соответствующие буквам латинского алфавита, а внутри диска эти контакты соединены попарно (каждому контакту с одной стороны сопоставлен контакт с другой) в соответствии с таблицей замены (см. рис. 1).

Рис 1. Диск с перепайками.

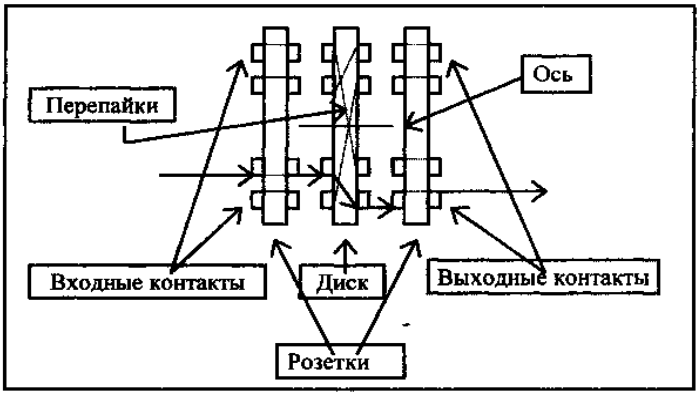


Рис. 2. Шифровальное устройство с одним диском

Шифровальное устройство, реализующее шифр простой замены, представляет собой входную и выходную розетки с 26 контактами, размещённые с двух сторон от диска на общей с диском оси. Диск может занимать одну из 26 угловых позиций на оси (для совмещения контактов). (см. рис. 2).

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
H	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**

Таблица замены 2.

При условии, что диск в некотором угловом положении реализовал Таблицу замены 2, перечислить, какие из Таблиц замен 3-10 диск реализовывает в других угловых положениях.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**R**	**Q**

Таблица замены 3.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

Таблица замены 4.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
M	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**

Таблица замены 5.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Таблица замены 6.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	B	Z	C	A	D	G	J	L	N	V	X	S	F	H	K	P	I	Y	R	W	Q	E	T	U	O

Таблица замены 7.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	X	V	T	R	P	N	L	J	H	F	D	B	A	C	E	G	I	K	M	O	Q	S	U	W	Y

Таблица замены 8.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	O	N	P	Q	R	S	T	U	V	W	X	Y	Z

Таблица замены 9.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	R	S	V	U	T	W	X	Y	Z	A	B	C	D	E	F	G

Таблица замены 10.

7. (6 баллов) Шифровальное устройство из предыдущей задачи можно развить, если к одному диску на общую ось добавить ещё 2 диска так, чтобы контакты дисков соприкасались. Тогда сигнал зашифрования будет проходить по схеме, изображенной на рис 3.

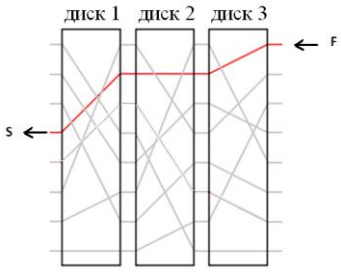


Рис. 3. Шифровальное устройство с 3 дисками.

Знаменитая шифровальная машина «Энигма» (*Enigma*), которая обширно пользовалась ведомствами Третьего Рейха, в том числе и армией, во время Второй мировой войны, была построена по изложенному выше принципу с небольшими отличиями. После зашифрования одного символа диски смещаются по закону одометра (диск 3 смещается на 1 сектор, после полного оборота диска 3, диск 2 смещается на 1 сектор; после полного оборота диска 2, диск 1 смещается на 1 сектор). Одним из отличий является размещение после 3 диска «отражателя». Отражатель – это диск, у которого контакты располагались только с одной стороны и пришедший электрический сигнал диск «отражал» назад на 3 диска. Таким образом, сигнал дважды проходил через 3 диска. Контакты отражателя были соединены перепайками внутри диска всегда попарно. Схема шифрования показана на рис. 4. Остальные отличия от «Энигмы» не влияют на решение задачи.

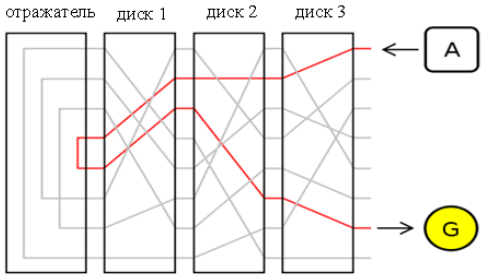
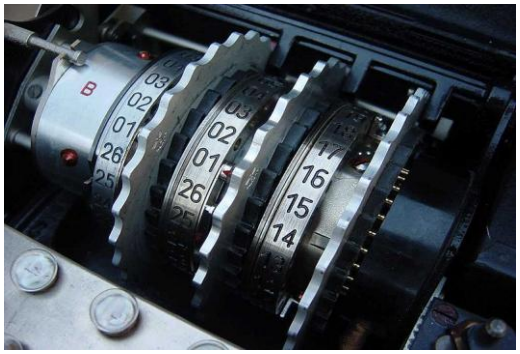


Рис. 4. Шифровальное устройство с 3 дисками и отражателем.

Разведка перехватила сообщение, зашифрованное шифровальной машиной «Энигма»:
ISWQFXSWIHMKQSNKIEZVBK
Доподлинно известно, что в данном сеансе связи передано одно из 10 сообщений. Не располагая таблицами замен, которые реализуют диски, определите, какое из 10 сообщений было передано.
10 возможных сообщений:
1. ITWILLBEVERYIMPORTANTM
2. OSWINDOWSISVERYRELIABL
3. THEPASSWORDISTHESECRET
4. BILLFOUNDVERYIMPORTANT
5. THEPASSWORDISQWERTYUIO
6. THEREWILLBEKOMAROVBAND
7. THISISIMPORTANTMESSAGE
8. DOWSONWILLBETHEREATFIV
9. THISISSERIOUSQAPROBLEM
10. FORQUICKACCESSENTERPIN

Фотография 1. Передвижной командный пункт командира 19 моторизованного корпуса Гейнца Вильгельма Гудериана во Франции, 1940 год. На переднем плане шифрмашина «Энигма».



Фотография 2. Три диска внутри шифровальной машины «Энигма» и отражатель, помеченный буквой B.

8. (8 баллов) Найдите секретное сообщение x, если оно является наименьшим общим элементом геометрической прогрессии $\{4^m | \ m \in \mathrm{N}\}$ и арифметической прогрессии $\{4\,000\,000\,007n + 2 | \ n \in \mathrm{N}\}$. В ответе указать сумму цифр числа $\log_2 x$.

9. Разведка сумела перехватить зашифрованное сообщение. Известно, что использовалось следующее шифрование: телеграмма вписывалась построчно в прямоугольную таблицу ширины $N<50$ (высота таблицы выбиралась таким образом, чтобы последний символ сообщения попадал в последнюю строку таблицы), причем, если в последней строке было записано менее N символов, то в конец сообщения дописывались ничего не значащие одинаковые символы, отличные от последнего символа сообщения; затем N столбцов таблицы перемешивались в некотором порядке и, наконец, шифртекст выписывался построчно из новой таблицы. Ниже приведен текст перехваченного сообщения (при перехвате могло исказиться несколько букв, знаки препинания и пробелы пропущены, пробелы в шифртексте служат лишь для удобного восприятия и не обозначают пробелы между словами):
УСЕБЫ ЙТВЬА РРСДП НРЙНА ЖОЫАБ КРЕЕС ЬРТШШ ИНАОУ СВИСМ МЗЙНЙ ТЧОЕН ЕООЕЛ УОКТЕ ЛИЬЛМ ХЛНЧЫ ЧЕВАВ ЛЯХЧС РЬАУЕ НИНЦС ОЕАКГ РОНЛО ЬНВЦП АВЕИЫ ОХЯЛБ СОРТК НЯАГЧ

ГЕЛИО ОИРВН ЕРЕЯЯ ИИОДН ЫИВЛН ЕЕОДГ ООЧБН ТТЕОЗ ЬКЛНВ ЮОССЮ КПУОК УЕРРС БТЖЮО ЗКЧСЬ БЛУОИ ССИЕВ ЛЕЫОЕ МЧДЛН СЫООИ ТРЕОА КЬВИЯ ЬТТЧТ ЫТЧЛЗ ЯЕООЛ ТЬНБЭ ПЗИРР ИСОВТ ЛАОКЕ ОООЙЛ СХХОТ ООИТО

а) (1 балл) Укажите возможные варианты значения *N* для перехваченного шифртекста.

б) (8 баллов) Помогите разведке расшифровать сообщение.

10. (10 баллов) Было перехвачено зашифрованное сообщение. Известно, что для зашифрования использовался шифр простой замены (см. задачу 5). Расшифруйте сообщение (знаки препинания пропущены, пробелы служат лишь для удобного восприятия и не обозначают пробелы между словами). Текст перехваченного сообщения:

ЫГРЯР ЛЮМЫЮ ЫЗЫЭВ РИЧЫЭ ЩЯРЙМ ЧЫЮДЩ ЙЛЩБП ЯЩМЧР ЕЫДЫЧ ЫУЕЩН ГЩЙЗТ ЕЭЩЫД
ЕЧАДЫ КЫДПЕ ЮДШЛЩ БПЯЙП ДЮЙЯЩ ЕЩЕТХ ДЫЗТЕ ЭТЩОИ ЩЭРДЩ ЭЫЛБЫ НЯЫЯЩ ДТНПЮ
ЩБТХГ ОЙШДЫ КЫЫДМ ЧЩЭРД ПОЪЮЫ ЫЗФПЯ РЙГЫО НПЯЛЯ ЩДЪЯЩ ЕЩЕТХ ЗТЕЭТ ЭВРИЧ
ЫДПЕЮ ДПЮОП ГТПДЛ ЩБПЯР ДЪЕЩН ГТХЗТ ЕЭТЫД ЕЧАДЫ КЫДПЕ ЮДЩГП ВРИЧЫ ЭФРЕМ
ЫЭДЫЧ ЙПДЭЫ ЗЧЩДЯ ЫБМЫЧ ЙГЕПЭ ЮПГПУ ЮДЭРЙ ВРИЧЫ ЭЩОЪФ РЕЩЧЩ ЮЕЧАЭ ЩЙДПБ
ЮЩБАБ ЮЫГПЧ НЩЯРП ЮЫЫЗФ ПЯРЙЕ ОХЬЕГ ЩЯЯЫБ ТВРИЧ ТЮЫЮД ЫРДРЛ ДЩЗОР ЦАЮЫГ
ПЧНЩФ ПУЫДЕ ЧАДАУ РВРИЧ ЫЭЩОЪ ЯАУЩО ИЩЭРД АЭЕЫД ЫЧЫУТ ЕЩЛАЭ ЩПДЮЙ ЯЩЕЩЕ
ТХЗТЕ ЭТЭВР ИЧЫДП ЕЮДПЮ ОПГТП ДЛЩБП ЯРДЪЗ ТЕЭТЫ ДЕЧАД ЫКЫДП ЕЮДЩЭ ДЩЕЫУ
ЕЧРМД ЫКЧЩИ РЬПЮЕ ЫУЮРЮ ДПБПМ ЧПГМЫ ОЩКЩП ДЮЙЬД ЫЩОКЫ ЧРДБВ РИЧЫЭ ЩЯРЙЫ
ЗФПРЛ ЭПЮДП ЯДЫКГ ЩЕЩЕЕ ОХЬГЫ ЮДТМП ЯДЫЮЪ ЕЫЫДМ ЧЩЭРД ПОХРМ ЫОТЬЩ ДПОХЮ
ЫЫДЭП ДЮДЭТ ХФРЖЮ ЫЫЗФП ЯРУ

Указание: Рассмотрите частоты встречаемости символов в шифртексте и частоты встречаемости символов в русском языке.