Ниже приведены условия задач заочного тура олимпиады по математике и криптографии. 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 для ответов. В случае возникновения вопросов по условию задач или порядке проведения олимпиады, можете отправить вопрос на электронный адрес omc@bsu.by.

Задачи заочного тура III Олимпиады по математике и криптографии БГУ

1) (3 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:

ONE + TWO + FIVE = EIGHT.

В ответе укажите, какое число соответствует слову EIGHT.

2) (2 балла) Одним из первых физических приборов, реализующих шифр, является Сцитала (Σκυτάλη). Он был изобретён в древней Спарте во времена Ликурга. Доподлинно известно использование в конце V века до н. э. в войне Спарты против Афин.

Герб Спарты

Для зашифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся получателю сообщения.

Сцитала

Принцип действия это шифратора изложен в трудах: Аполлония Родосского Απολλώνιος Ρόδιος (род. около 290 г. до н. э.) и Плутарха из Херонеи Πλούταρχος (ок. 45 — ок. 127 гг. н.э.).

Был перехвачен ремень, содержащий следующую последовательность символов:

ПЕУС СОНД ТВДИ ЕООК ЕТЙС РПНД ТЕРА ЕОПИ ШНКЛ БЕЬА.

Восстановите исходный текст. Известно, что в передаваемом сообщении удалены все пробелы и знаки препинания, а пробелы в последовательности приведены для удобства прочтения.

3) (7 баллов) Шифр Плейфера — ручная симметричная шифрсистема, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном, но названа по имени его друга Лорда Лиона Плейфера, который внедрил данный шифр в государственные службы Великобритании.

Лорд Лион Плейфер
The Lord Lyon Playfair
(1818 –1898)

Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов.

Шифр Плейфера использует таблицу 5x5, ячейки которой заполнены символами латинского алфавита (чтобы уменьшить латинский алфавит с 26 до 25 символов, буквы «I» и «J» объединяются в одну ячейку). Данная таблица 5x5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Необходимо определить положения углов этого прямоугольника относительно друг друга. Зашифрование производится по следующим 4 правилам:

1. Если два символа биграммы совпадают, то после первого символа добавляется буква «X», после чего биграммы формируются заново.

2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

Сэр Чарльз Уитстон
Sir Charles Wheatstone
(1802—1875)

4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифрования необходимо использовать инверсию этих четырёх правил, откидывая символы «X», если они не несут смысла в исходном сообщении.

Пример зашифрования.

На ключе

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

Зашифруем сообщение «Hide the gold in the tree stump»

HI DE TH EG OL DI NT HE TR EX ES TU MP

1. Биграмма HI формирует прямоугольник, заменяем её на BM.
2. Биграмма DE расположена в одном столбце, заменяем её на ND.
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.
4. Биграмма EG формирует прямоугольник, заменяем её на XD.
5. etc…

Шифр Плейфера использовался в тактических целях британскими вооруженными силами во Второй Англо-Бурской войне и в Первой мировой войне, а также и немцами во время Второй мировой войны. Причиной использования шифра Плейфера было то, что он достаточно быстр в применении и не требует никакого специального оборудования. Основной целью использования этой системы шифрования была защита важной, но не секретной информации во время ведения боя. К тому времени, когда вражеские криптоаналитики взламывали сообщение, информация уже была бесполезна для них.

Задача.

а) (3 балла) Расшифруйте следующее сообщение, зашифрованное с помощью шифра Плейфера:

MRMD GEZF RIEU YNID RYMZ WZZY KFBC,

если известен ключ

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

б) (4 балла) Известно, что наблюдаемое подразделение противника в условиях боевых действий может отправить одно из 15 сообщений, зашифрованных на неизвестном Вам ключе шифром Плейфера:

1. CBMB JGUT YRDA; 2. MNBV CXDS HGIU; 3. PMUV YCTX RZWA;

4. QZRV TNYM UJOL; 5. PMIJ UBYG TCRD; 6. QDEG RHYK NVMC;
7. UBYB RBEB SBFB; 8. TDTG TJTL TMTB; 9. BUFT SEBU KOLP;
10. PILJ UTHF PILJ; 11. TUDG PMGD QOXM; 12. BJXF BJKO PLWQ;
13. MNLK HGVC YTRE; 14. OBAF GKML UPZH; 15. YDIN YGVX POQD;

По шифрованному тексту

TUPR EBRP FOLI

определить, какое сообщение было отправлено.

4) (11 баллов) Шифр Вернама. Пусть нам необходимо зашифровать текст X длиной n символов. Ключом является некоторая секретная последовательность символов K тоже длины n. Сперва буквы исходного текста X и ключа K заменяется на номера этих букв в алфавите начиная с нуля (так, а – 0, б – 1 и т.д., я – 32): $X \to (x_1x_2\ldots x_n)$, $K \to (k_1k_2\ldots k_n)$, где $x_i, k_i \in Z_{32} = \{0,1,\ldots,32\}$. Затем вычисляются значения $y_i = (x_i + k_i) \bmod 33$, где запись $(\ ) \bmod 33$ означает нахождение остатка от деления на 33. Результатом зашифрования является текст Y с номерами букв $(y_1y_2...y_n)$. Так, например, при зашифровании слова X = ПРИМЕР с ключом K = АЯАУМФ получим шифртекст Y = ППИАСЕ. Важным требованием является то, что для зашифрования нового сообщения обязательно необходимо использовать новый ключ.

Шифр Вернама является абсолютно стойким, то есть перехват шифртекста не даёт никакой информации о сообщении. С точки зрения криптографии, невозможно придумать систему безопаснее шифра Вернама. Требования к реализации подобной схемы достаточно нетривиальны, поскольку необходимо обеспечить наложение уникального ключа, равного длине сообщения, с последующим его гарантированным уничтожением. В связи с этим коммерческое применение шифра Вернама не так распространено в отличие от многих других схем и он используется, в основном, для передачи сообщений особой важности государственными структурами.

а) (3 балла) Расшифруйте сообщение

Y = **КГПЧ СЫШД ЧЮМЖ ЯВЬМ СИМЁ ИЧБЁ ЮЦВО ПЯРШ ТЁЯБ ТЭ**

с помощью ключа

K = **ЭЮБЦ ЬМФЫ КПДХ ПУРР ЙЪКЁ ЦЫТВ РЗСО ЗРОЭ НЫУГ ЫФ**.

б) (8 баллов) Алиса переслала Бобу следующее зашифрованное с помощью шифра Вернама сообщение, зашифрованное с помощью некоторого ключа,

Y_1 = **ЛРЬЕ ЧПЯР ЗЖХК ЕБСВ ХЯФР ИЙМГ ЫИАВ ЖГ**.

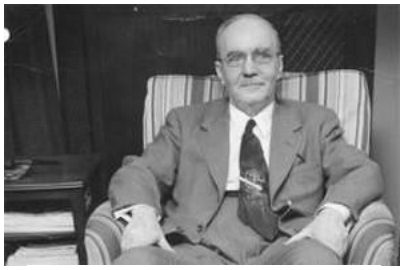
Боб принял и расшифровал переданное сообщение, получил исходное сообщение $(x_1x_2...x_{30})$. После чего для подтверждения получения сообщения он зашифровал текст $(x_{29}x_{30}x_1...x_{28})$, полученный из исходного циклическим сдвигом в право на два символа, шифром Вернама и передал Алисе следующий шифртекст:

Y_2 = **ЬЫЛЁ ЕИДЦ ЩЖСН ОЭИХ УЙЩЧ ЕЧСГ ЖРЭИ ЩШ**.

Разведчик Ева перехватила обе эти передачи. Кроме того, Еве стало известно, что Боб по ошибке для зашифрования использовал тот же ключ, что и Алиса. Помогите Еве восстановить сообщение, которое Алиса передала Бобу.

5) (10 баллов) Шифр Хилла. Зашифрование происходит следующим образом. Как и в шифре Вернама, исходные символы сообщения заменяется на их порядковые номерами. Ключом является четверка чисел (a_1, a_2, b_1, b_2) из множества $Z_m = \{0, 1, ..., m\text{-}1\}$ (где m – количество букв в используемом алфавите). Далее сообщение разбивается на пары символов и каждая пара зашифровывается независимо от остальных по следующему правилу:

$$(x_1, x_2) \to ((a_1 * x_1 + b_1 * x_2) \bmod m, (a_2 * x_1 + b_2 * x_2) \bmod m).$$



Лестер Сандерс Хилл
Lester S. Hill
1890 - 1961

После чего полученные пары объединяются в итоговый шифртекст.

а) (5 баллов) Расшифровать сообщение Y = **РЛОЕ РХХБ ЯФТЁ ТКДД УАОБ**, если ключ равен ($a_1 = 31$, $a_2 = 30$, $b_1 = 28$, $b_2 = 2$).

б) (5 баллов) Оказывается, не все четверки чисел могут быть ключами в шифре Хилла. При некоторых из них сообщение не удается расшифровать (подумайте почему). Найдите количество возможных ключей в случае если размер алфавита $m = 5$.

6) (7 баллов) Игорь пользуется телефоном марки *иТелефон*. Разблокировка этого телефона осуществляется следующим образом. На экране появляется 16 кружочков, расположенных в виде таблицы 4 на 4, после чего надо провести пальцем по экрану линию, идущую по последовательности ключевых кружочков (в правильном порядке). Последовательность ключевых кружочков обладает следующими свойствами: соседние в последовательности кружочки являются соседними в таблице (по стороне или диагонали); ни один из кружочков в последовательности не повторяется; начальный кружочек может располагаться где угодно; длина ключевой последовательности 5 кружочков.

Володя, использующий обычный телефон, в котором для разблокировки используется четырехзначный пинкод, утверждает, что его телефон более надежный. Проверьте, прав ли Володя, подсчитав, сколько различных ключевых последовательностей существует в телефоне Игоря.

7) (4 балла) В школе, в которой учится хакер Витя, все оценки хранятся в компьютере. Оценки в памяти компьютера представляются следующие образом: 0 – 0000, 1 – 0001, 2 – 1111, 3 – 1100, 4 – 0101, 5 – 0100, 6 – 1101, 7 – 0010, 8 – 1011, 9 – 1000, 10 – 1110. После ввода учителем каждой новой оценки на компьютере специальная программа сохраняет в защищенной области памяти количество оценок по данному предмету и хэш-значение, которое вычисляется следующим образом. Все оценки разбиваются на пары $X_{1,2}=(x_1, x_2)$, $X_{3,4}=(x_3, x_4)$, ..., $X_{(n-1),n} = (x_{n-1}, x_n)$, если оценок нечетное количество, то добавляется еще одна оценка $x_{n+1} = 0$. Далее над представлением этих оценок в памяти компьютера выполняются следующие операции:

$$h = 10101010 \text{ XOR } X_{1,2} \text{ XOR } ... \text{ XOR } X_{(n-1),n},$$

где XOR – операция "взаимоисключающее или", выполняемое для каждого двоичного разряда по-отдельности. Ниже приведена таблица для вычисления XOR от двух аргументов:

x	1	1	0	0
y	1	0	1	0
x XOR y	0	1	1	0

У Вити по русскому языку стоят следующие оценки: 4, 2, 2, 5, 1, 6, 3, 3, 2, 1 (именно в таком порядке). Он может взломать компьютер и заменить одну или несколько оценок (хоть все) на любые другие, но не может получить доступ к защищенной области и поменять число оценок либо хэш-значение. Если после замены оценок хэш-значение не будет соответствовать хранящимся оценкам, Витю поймают. Какой максимальный средний балл может сделать себе Витя и при этом не быть пойманным?

8) (5 баллов) Известно, что число $N = 2016343583$ является произведением двух простых чисел p и q, а количество натуральных чисел, меньших N и взаимно простых с N , равно 2016253248. Найдите числа p и q.

Примечание: Такие числа $N = p * q$ используются в ряде современных алгоритмов зашифрования. При этом в качестве чисел p и q используются большие простые числа (порядка 2^{1000} и больше). Для взлома таких шифров необходимо уметь разложить число N на простые множители (это так называемая задача факторизации числа), что, вообще говоря, является вычислительно трудной задачей. В случае нашей задачи у Вас есть дополнительная информация, позволяющая достаточно легко найти искомое разложение.