



# XXII открытая олимпиада школьников и студентов по криптографии

Для студентов

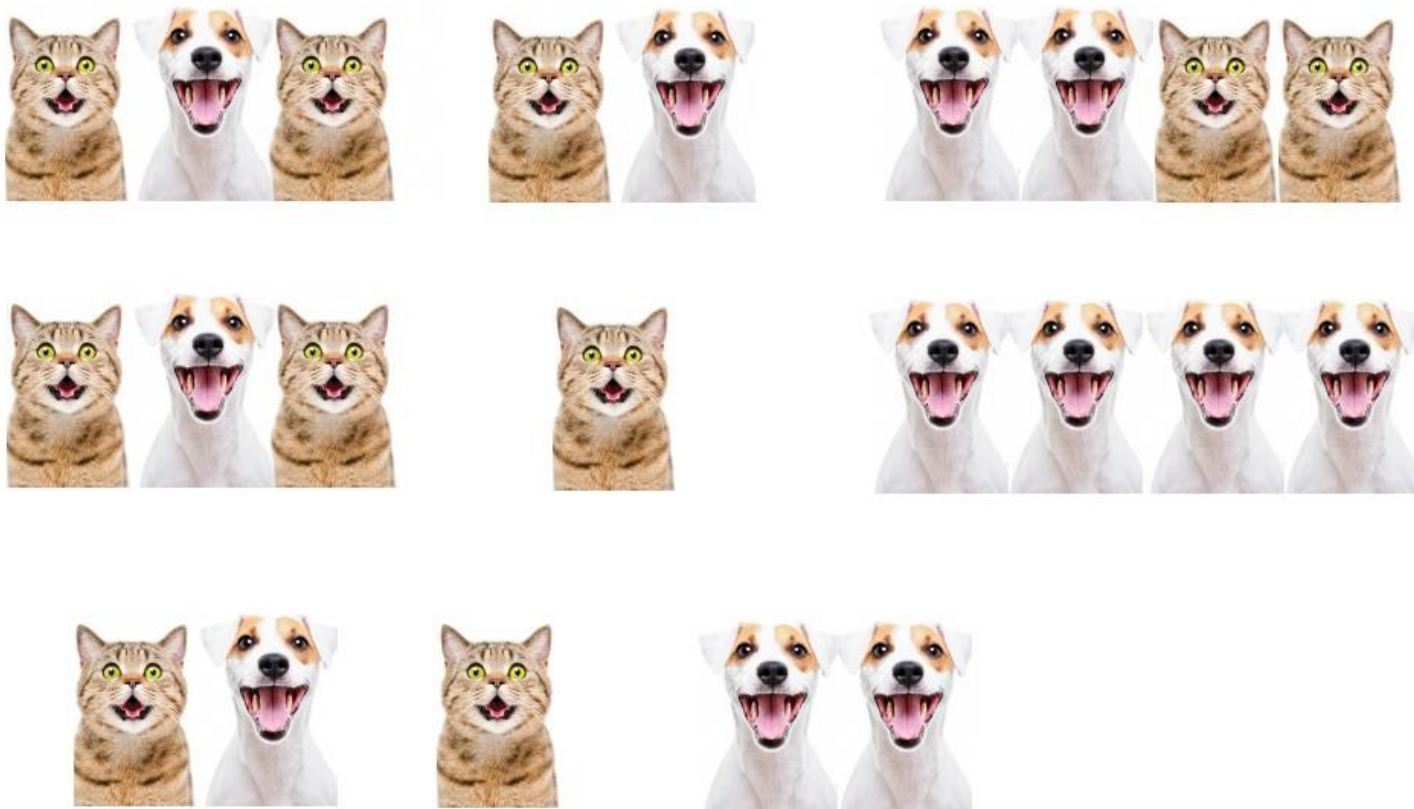
Задания I (дистанционного) тура

4-10 декабря 2023 года

**Задание № 1.** Кошки и собачки играли в чехарду. Только правила были не обычные, а слегка измененные. Каждый котик должен перепрыгнуть через трёх собачек, а затем собачка должна перепрыгнуть через двух котиков. Вдохновившись игрой, Павел решил зашифровать сообщение для своего друга. Расшифруйте сообщение и запишите полученный результат заглавными буквами без пробелов.

Тсьзпцнсызъзн  
ожпюъж, щжоургвм?  
ТсхспцъхсТгезо  
рмвйвнубфтжфюжлмръжщмлр

**Задание № 2.** Котики и собачки не перестают проводить время вместе. Павел решил тоже поиграть с ними. Но котики и собачки были непросты, поэтому, чтобы разрешить Павлу играть с ними, придумали ему испытание. Сможете помочь Павлу пройти тест? Запишите в ответе сообщение заглавными буквами.



**Задание № 3.** Важные фигуры мирового масштаба выбирают кнопочные мобильные устройства для обеспечения своей конфиденциальности и предотвращения отслеживания со стороны неприятеля. У этих устройств есть одна особенность: для ввода буквы необходимо несколько раз нажать на соответствующую кнопку. Однако этого недостаточно для соблюдения стандартов безопасности. Чтобы обеспечить их, была создана комиссия из множества криптографов. В ходе продолжительных дискуссий молодой специалист внес предложение: «Коллеги, мы на пороге 2024 года. Многие давно используют смайлики. Почему бы и нам не последовать трендам и не внедрить подобный способ общения?». Все члены комиссии поддержали эту идею единогласно.

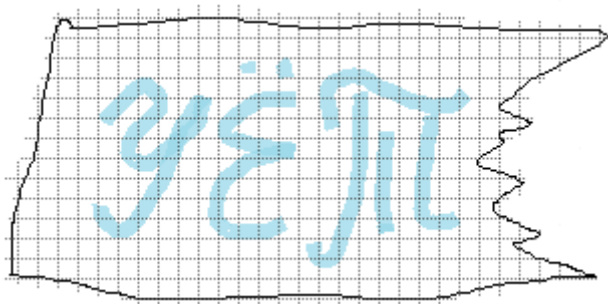
Юноша предложил всем пример клавиатуры для мобильных устройств, которая выглядит следующим образом:

			
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 !	? . <пробел>

В качестве демонстрации, он ввёл первое, что пришло ему в голову, но его устройство сломалось и стало объединять два соседних смайлика в один, сохраняя из каждого что-то. Раскодируйте сообщение, которое он передал чиновникам:

**Задание № 4.** Лилия Никифорова в четверг захотела отправить подруге важное секретное сообщение. Она выбрала ключ ГОРОДКИ4 и начала шифровать сообщение «Нам обязательно нужно научиться учиться», получая шифртекст



Попробуйте перехватить весь шифртекст, записав ответ заглавными буквами без пробелов.

**Задание № 5. Никак вы... читать... не научитесь**

В корчме охотник письмо получил,  
 В письме том он о встрече прочёл.  
 На плечи мечи свои грузно взвалил,  
 Но кое-что всё же он не учёл.

Шутку с ним злую сыграла судьба:  
 В этот миг от напитка не ждал он подвоха,  
 Кто-то подлил ему что-то туда.  
 Охотник почувал себя крайне плохо.

Место, в которое нужно прибыть,  
 В глазах всё продолжало двоиться,  
 Ни с того, ни с сего буквы стали ходить,  
 Не на свои места становиться!

Зелье, подлитое негодеям,  
 Покою охотнику не даёт.  
 Но мы-то с вами не прогадаем,  
 Скажем, куда дорога ведёт!

Чтобы ответ на задание дать,  
 Улицу нужно тебе указать,  
 Следом за улицей дом написать,  
 Например, **ПРОСТОКВАШИНО 5.**



АРАВРВ	ИВИЗВЗ	ВОВЛОЛ
АНАОНО	ЛАЛЧАЧ	ОМОМО
АТАСТС	НИНМИМ	ШЕШУЕУ
ВДВЬДЬ	АНААНА	ВЕВЛЕЛ
ОПОПО	ЕЛЕСЛС	ЯРЯРПР
ЛОЛМО	ЕВЕЕВЕ	НВНЕВЕ
БЬБЬОВО	ЕЛЕСЛС	АКАГКГ
ОРОПРП	ДОДХОХ	БЬШИШИ
ОДОВДВ	ДЬДЬЛЛ	ЕРЕРЕ
ЮНЮВНВ	ЯРЯРПР	ОДОМДМ
МОМДОД	ИВИОВО	ШЕШДЕД
ВИВЬИВ	БЗБИЗИ	КШКУШУ
ПСПЕСЕ	ВАВВАР	ЕМЕАМА
УЯУНЯН	НЕНЖЕЖ	ДЙДАЙА
БЬШЕШЕ		

Твоя й.

**Задание № 6.** На одной из планет далекой галактики обнаружен старинный свиток с фразой, написанной на неизвестном языке. Ученые предполагают, что для раскрытия тайны этого языка необходимо применить шифр подстановки.

Фразы на свитке:

*o dxlz fgz ytkq. ytkq ol zit dofr-aosstk. ytkq ol zit sozzst-rtqzi ziqz wkoful zgzqs gwsotkqzogf. o voss yqet dn ytkq. o voss htkdoz oz zg hqll gctk dt qfr zikgxui dt. qfr vitf oz iql ugft hqlz o voss zxkf zit offik tnt zg ltt ozl hqzi. vitkt zit ytkq iql ugft zitkt voss wt fgziofu. gfsn o voss ktdqof*

Вот часть ключа для шифрования:

$d \rightarrow r, i \rightarrow o, m \rightarrow d, n \rightarrow f, o \rightarrow g, p \rightarrow h, q \rightarrow j, r \rightarrow k, v \rightarrow c, w \rightarrow v, y \rightarrow n, z \rightarrow m$

Расшифруйте фразу и напишите в качестве ответа последнее предложение (заглавными буквами без пробелов).

**Задание № 7.** Мария Медведева очень любит простые числа и решала узнать, сколько для простого числа  $p$  есть решений уравнения  $x^p = 1 \pmod p$ ,  $x \in \{0, 1, \dots, p - 1\}$ . Найдите ответ вместе с ней.

**Задание № 8. Мама, я шифр сломал**

Знакомьтесь, это Иван Васильевич. В свои 7 лет он – криптоаналитик с десятилетним стажем – решает взяться за новую задачу. Кто-то выложил в сеть обезличенные бюллетени тайного электронного голосования в тайном обществе «Правители мира». Рекламу данного голосования Иван Васильевич видел на двери подъезда соседнего многоэтажного дома. Вооружившись фотографией рекламы и бюллетенями, он быстро определил нового главу тайного общества. А вы? Номер победителя напишите в ответ на задание.

### ПРАВИТЕЛИ МИРА

В это воскресенье мы выбираем главного правителя мира. Вы все являетесь нашими подданными и обязаны проголосовать за того, кто поведёт вас из светлого настоящего в ещё более светлое будущее!


Повелеваем, заходите на сайт и голосуйте:  
[типд://правители.мир/голосование](http://типд://правители.мир/голосование)  
 Ну пожалуйста!

При голосовании нужно указать зашифрованный номер кандидата:


3. Эгги М. «Никаких ежей в моей лаборатории!»
5. Мегастул «Предводитель злобных роботов и любитель машинного масла»
7. Кощей «Обещаю, что в правительство войдут мои доверенные лица: дуб, сундук, заяц, утка, яйцо и игла»
9. Тонус «Я позабочусь о вас своими пятью пальцами»
11. Воля-де-Морте «Абра-кадабра! Мандарин-апельсин! Дайте мне мою волшебную палочку!»
13. Баба Я.Г. «Яна Георгиевна о вас позаботится, внучки»

ВАЖНО!

Для голосования применяется шифр RSA.  
 Открытый ключ - два числа:  
 $n = 974219641100664809131$   
 $9322294311222673270133939$   
 $2960684923488294783852624$   
 $4214860863537832998972236$   
 $2354288708811469255603961$   
 $1392913483315870886121102$   
 $89763339$   
 $e = 65537$



Анонимность гарантируем!

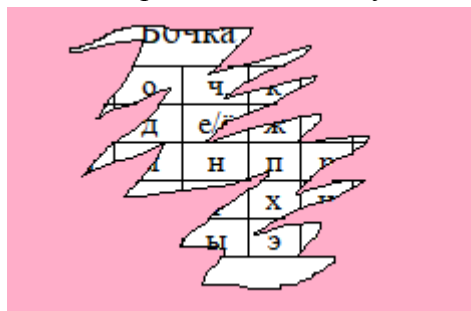


#### Коммунальная строка

иван@комп\$ открыть\_голосование.бд  
 Бюллетень | Голос

№	Голос
1	696079336131745927675855355236420585986847009457209788 904953098519940038268193871643754058940528746719612865 9038790842077160850104480952602825690216932176
2	529635882611209943820346211751472208224683434986170978 779583725385521410796698945389581515373698924059776543 529312327960268046550504923711442833450377560
3	955603500613993447308009163970315524026395569944974692 393320543720480131949692517382030657493514901316036170 4629540812038250013260660858489618165900861638
4	874142321488434128356492771778075783527832738176845231 458065938839716762557380071002994497322493470385722291 8560149909574420235443669140168678259076233602
5	233775232386708550326865466488404199166942865991289923 806102406622504769100564535065939291874481425175022384 0526577477041566575904796955581730377052167629
6	955603500613993447308009163970315524026395569944974692 393320543720480131949692517382030657493514901316036170 4629540812038250013260660858489618165900861638
7	507209838401084018104815130104311047821786818747333365 051406703502204474736161237928593987628654140300595893 036931003543812407943293024433031913756237528
8	955603500613993447308009163970315524026395569944974692 393320543720480131949692517382030657493514901316036170 4629540812038250013260660858489618165900861638
9	955603500613993447308009163970315524026395569944974692 393320543720480131949692517382030657493514901316036170 4629540812038250013260660858489618165900861638
10	874142321488434128356492771778075783527832738176845231 458065938839716762557380071002994497322493470385722291 8560149909574420235443669140168678259076233602
11	955603500613993447308009163970315524026395569944974692 393320543720480131949692517382030657493514901316036170 4629540812038250013260660858489618165900861638
12	874142321488434128356492771778075783527832738176845231 458065938839716762557380071002994497322493470385722291 8560149909574420235443669140168678259076233602

**Задание № 9.** Роман Лазарев нашёл странный ключок бумаги



Рядом с ним была надпись:

*ИШГНН ФРЧЪВ ШИГЫЧ ЗШЛВШ БМРФД НЕНМБ ЧИАЖР ЧСЕДН*

Роману стало очень любопытно, что это такое. Попробуйте найти ответ вместе с ним, записав его заглавными буквами без пробелов.

**Задание № 10.** Алиса и Боб обмениваются зашифрованными сообщениями, используя шифр подстановки с ключом. Ключ представляет собой вектор  $(a_1, a_2, a_3)$ , где каждая компонента является натуральным числом. Алиса отправляет Бобу зашифрованное сообщение:

в"д#удсзо#сркпвррк#нвффроюмс"сузкфсронкоуё/"цхр"ђ"мгм"дхжхр"дэ"циз#уфс"фукнокрррд#оконкэт  
жсд"озф#стсикевè#нв#фтлнлрпгч"л"фукнокррвч#фвнкч#из#снзпзх."нвм#яфг"Йионђ."пиз#яфсф"пкт#в  
гфрнёфпс"сспèхзп/"к#è"кжзфю"лых#фроюмс"рзпржр"0"ссмрђ."цокурфертипкђ"к#дрх"яхрл#евуорркк/"  
рх"уокёркè#у"дзунрпищпс"дищпюо.#рф#уркзтицвлё"езнлмржр"чтвнфвоюпсер#срзрглè"л"рх"дсф"èфр  
жр"квоищвхзняпржр"еузижкруфев"фхыиуфев.#гзфмррзцирр"езицррес."нхжг"пл"ссуосфтл."ишрфя"дженх  
дю"0"гиумспзъпр#оворз/"чсфю#ддюую#/"дзунрпищпсз"дрняъри."трпловиъю

Алиса хочет, чтобы Боб расшифровал сообщение. Помогите Бобу расшифровать сообщение, зная, что оригинальный текст начинается со следующего отрывка: «Я ...»

В ответе запишите заглавными буквами третье слово с конца.



Ответы нужно ввести на сайте олимпиады до 21.00 часов 10 декабря 2023 года:  
<https://erudit-online.ru/sarcrypt.html>