ФГБОУ ВО «Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского»
Научно-образовательный центр «Эрудит»

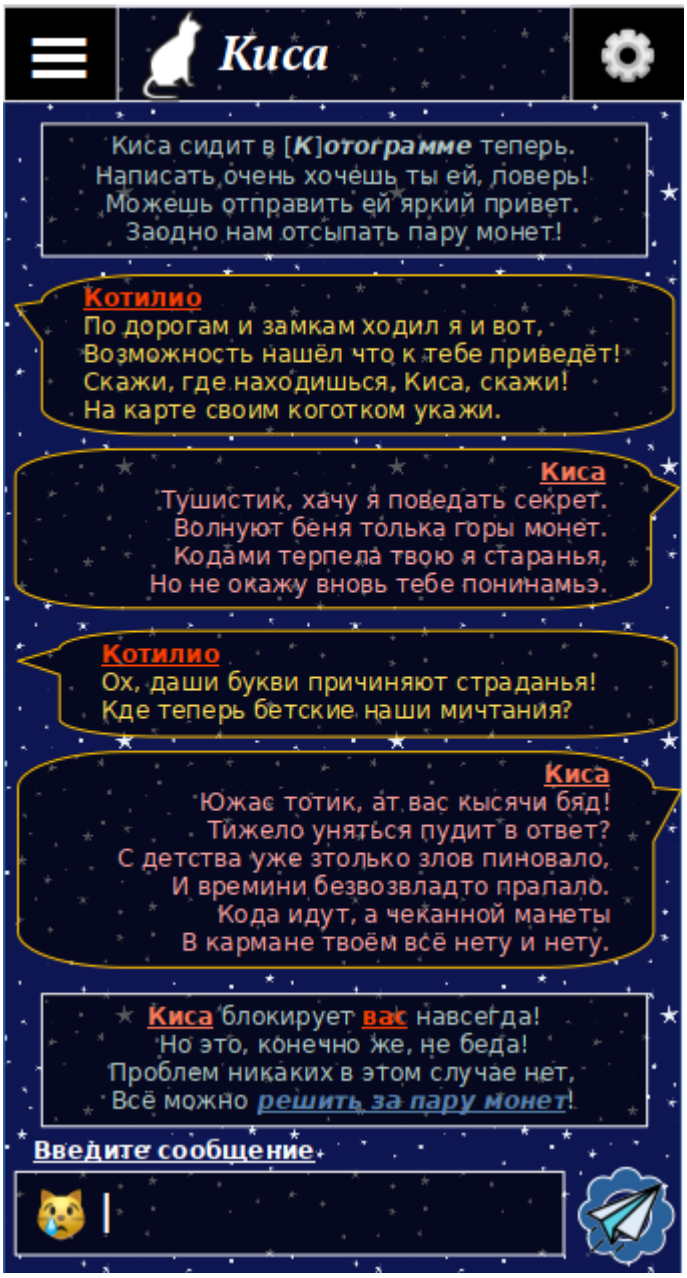
XXI открытая олимпиада школьников и студентов по криптографии

Для студентов

Задания I (дистанционного) тура

5-11 декабря 2022 года

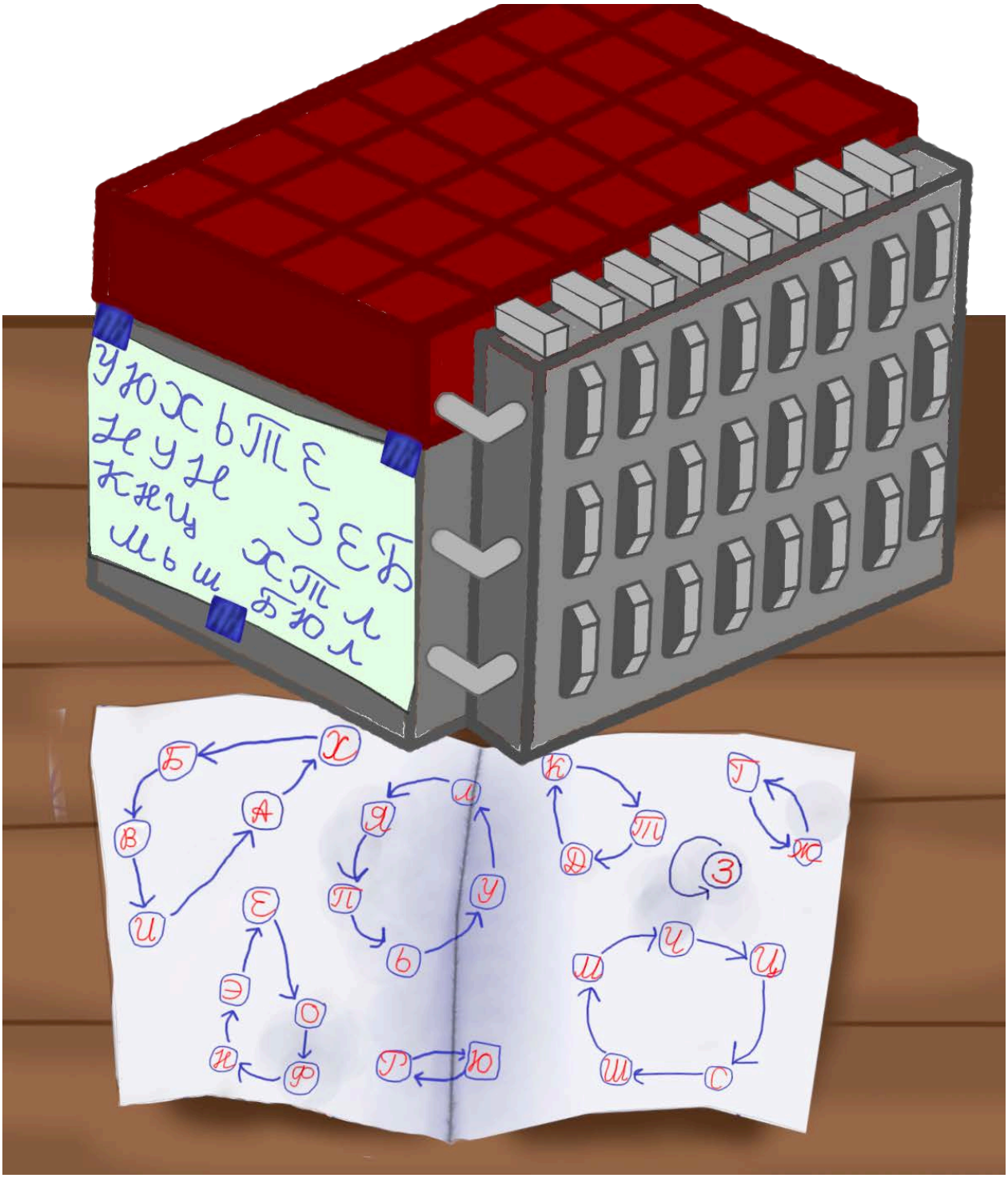
Задание № 1. Котограмм



«О киса...» – подумал бедный Котилио,
Но не поддался чувству уныния!
Детские тайны он помнил, и вот,
Снова в дорогу отправился кот.

В словах персонажей сокрытый секрет
Заглавными буквами впишите в ответ.
Пробелы в ответе не принимаем.
Ну что, к решению приступаем?

Задание № 2. Иван Васильевич меняет профессию



Иван Васильевич очень уважаемый человек. В свои шесть лет он, как выдающийся криптограф, разработал новый шифр «Непростая замена». Он основан на многократном применении шифра «Простая замена».

Иван Васильевич решил спрятать до дня рожденья мамы её любимое лакомство в коробочку и запер на электронный замок с паролевым замком, а то такие подарки постоянно куда-то пропадают до момента дарения. Для этого в течение 10 дней он зашифровывал пароль, чтобы никто не смог вскрыть шкатулку без его ведома. Целых **9987** раз пришлось выполнять шифр простой замены. Результат Иван Васильевич предусмотрительно записал на зелёном листочке. Ключ для шифра простой замены был зарисован на бумаге и хранился у сердца.

Вот настал день «икс». Через час маме нужно дарить подарок. Иван Васильевич забыл пароль. Чтобы расшифровать пароль, нужно снова потратить 10 дней.

Но это не беда. Иван Васильевич меняет профессию, теперь он – ведущий криптоаналитик с десятилетним стажем. Теперь ему по силу взломать этот шифр за 5 минут. А вам?

В ответе запишите заглавными буквами без пробелов, какой пароль использовал Иван Васильевич для того, чтобы закрыть шкатулку.

Задание № 3. Очень простой шифр без буквы Ё

На примере *победитель* – ОПАЖГЙСЖКЭ установите правило, по которому при шифровании производится замена букв открытого текста, и прочтите сообщение

ЧЙУ СЬУ НУЯ КМЬ ИАЖ ЬЙЕ КАР ПНВ ШОЗ ЛНГ

Запишите ответ заглавными буквами без пробелов.

Задание № 4. Зная, что ключом шифра является стихотворение Лермонтова «Из Гёте», прочтите сообщение

ВНСЕЕПЗЫ НЛАИМТЕД НОИРТОЫГ ЕАМНАЕТД ЕРМОАЖТА
ИТКЛИИБС ЫТЛЫИПКО РДИОПЖТД ОИГНРЕАМ ФНАОМГИО

Запишите ответ заглавными буквами без пробелов.

Задание № 5. Прочитайте цитату:

П18о11д10т06м10м16н01с10п18о19т10т06н01м15а26е19ч01с20ь06

В ответе запишите фамилию автора заглавными буквами.

Задание № 6. Мария отправила Владиславу сообщение

ЭФУ ЮБВ ПГЯ ЖЮЮ ВЮЬ ЛЫЮ АЮЬ ГЖШ ВЛШ
ЮПЮ ШОЭ ПУЮ ЭРЩ ВШШ ЬЯА ШЫЮ ЧФЮ ШФ

В процессе передачи оно повредилось, найдите количество ошибок. В ответе запишите только число.

Задание № 7. В городе Базеле рядом с домом Леонарда Эйлера была найдена загадочная записка

Попробуйте восстановить пропуски. Ответ запишите единым числом.

Задание № 8. Перед вами записка, оставленная обмотанной бинтами женщиной с рыжими волосами. Текст в записке – это набор больших букв русского алфавита в кодировке UTF-8. На записке указаны байты:

```
1D 02 1C F6  19 EE 11 F0  23 EC 1F F1  14 ED 25 E4
24 F8 20 E3  23 F0 27 DF  22 F3 1D F6  1C EF 19 F3
11 FA 23 E7  1F EB 14 EA  25 EA 24 EA  20 E3 23 FF
```

Известно, что использовался шифр Вижинера на байтах, а в качестве ключа использовалось слово из 13 букв, представленное в кодировке ASCII. В ответе укажите, какой ключ использовался при шифровании.

Задание № 9. Дано множество точек (x, y). Сложение точек $P = (x_p, y_p)$ и $Q = (x_q, y_q)$ происходит по следующему правилу:

$$P + Q = R$$
$$(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$$
$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

где

$$\lambda = \frac{3x_p^2 + a}{2y_p} \quad \text{если } x_p = x_q$$

$$\lambda = \frac{y_q - y_p}{x_q - x_p} \quad \text{если } x_p \neq x_q$$

Также $mP = P + \ldots + P$ (сложение m раз), где m – целое число

Если координата y точки $P = (x, y)$ не равна 0, то $-P = (x,-y)$.

Если координата y точки $P = (x, y)$ равна 0, то $-P = (x, y)$.

Найдите точку $-4P$, где $P = (2,1)$, $a = 9$ и все вычисления проводятся в кольце вычетов по модулю 11. В ответе запишите координаты точки P через пробел.

Задание № 10. AES – симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США по результатам конкурса AES в 2001 году. Найдите произведения байт, используя алгоритм в данном стандарте шифрования, и в ответ запишите наибольший из результатов – последовательность бит без скобок, пробелов и иных знаков препинания.

(0, 1, 1, 1, 1, 1, 1, 0)(0, 1, 0, 1, 0, 1, 0, 1);
(0, 0, 1, 0, 1, 0, 1, 0)(1, 1, 0, 1, 0, 1, 0, 1);
(1, 1, 1, 0, 0, 1, 1, 1)(0, 0, 0, 0, 1, 0, 1, 1);
(0, 0, 1, 0, 1, 1, 1, 0)(0, 1, 1, 0, 1, 1, 0, 0);
(1, 1, 1, 1, 1, 1, 1, 1)(0, 0, 0, 1, 1, 0, 0, 0).

Ответы нужно ввести на сайте олимпиады до 21.00 часов 11 декабря 2022 года: https://erudit-online.ru/sarcrypt.html