Условия задач 9-11 класс

Войдите в тестирующую систему.

Муниципальный этап Всероссийской олимпиады Калужская область. ИБ. 2025-2026 (9-11 класс)

https://official.contest.yandex.ru/contest/85920

Нажмите на ссылку «*Войти*» в верхнем правом углу страницы (или на ссылку «*Авторизоваться*»).

Введите логин и пароль, указанные на листе, который выдан организаторами олимпиады.

После входа в систему будут доступны закладки: «*Задачи*», «*Посылки*», «*Сообщения*».

Вам будет предложено несколько заданий. При решении заданий Вам необходимо найти флаг вида KALUGA{W3lc0M3_t0_t3h_G4M#} (в фигурных скобках может быть указана любая последовательность букв, цифр и специальных знаков, например, символов _#@% и т.д.). Найденный флаг нужно отправить в тестирующую систему на проверку.

Если флаг указан верно, то Вы получаете штраф – число секунд, прошедших с начала соревнования. За каждый неправильный флаг начисляется штраф в 10 очков. Побеждает тот, кто найдет больше флагов и получит наименьший штраф.

1. «Secret message in the code of a web page»

Программист, создававший web-страницу, оставил в нем секретное сообщение. По ссылке «Скачать условие» Вам будет доступен архив некоторой webстраницы. Исследуйте его тщательно, чтобы найти то, что он скрывает.

Пример посылки ответа на задачу в тестирующую систему: **KALUGA{Hallo!}**

2. «RSA»

Алиса с Бобом решили обмениваться секретными сообщениями. Для шифрования они решили использовать алгоритм шифрования с открытым ключом RSA.

Алгоритм RSA работает следующим образом: берутся два достаточно больших простых числа p и q и вычисляется их произведение $n=p\cdot q$ (n называется модулем). Затем выбирается число e, удовлетворяющее условию

$1<e<(p-1)\cdot(q-1)$ и не имеющее общих делителей кроме 1 (взаимно простое) с числом $(p-1)\cdot(q-1)$.

Затем вычисляется число d таким образом, что $(e\cdot d-1)$ делится на $(p-1)\cdot(q-1)$.

(n; e) – открытый (public) ключ.

(n; d) – закрытый (private) ключ.

Для шифрования некоторого сообщения нужно представить его в виде чисел. Например, будем каждую букву заменять на ее код в таблице ASCII. Чтобы получить зашифрованное сообщение C из сообщения M, нужно

$C = M^e \pmod n$ (возвести сообщение M в степень e и найти остаток от деления на n).

Для расшифровки сообщения нужно $M = C^d \pmod n$(возвести сообщение C в степень d и найти остаток от деления на n).

Например, они могли выбрать $p = 7$ и $q = 13$, тогда $n=7\cdot 13=91$. Можно взять $e=5$. Оно будет взаимно простым с числом $(7–1)\cdot(13–1) = 72$. Открытый ключ (91, 5) – с помощью него было зашифровано сообщение. Число $d = 29$, поскольку $(5\cdot 29-1)$ делится на 72. Закрытый ключ (91, 29) – с помощью него можно расшифровать сообщение.

Сообщение «AB» (латинские буквы) будет представлено в виде чисел 65 и 66. Его можно зашифровать следующим образом:

$$65^5 \pmod{91} = 39;\ \ 66^5 \pmod{91} = 40.$$

При расшифровке сообщения 39 и 40 нужно сделать следующие действия:

$$39^{29} \pmod{91} = 65;\ \ 40^{29} \pmod{91} = 66.$$

Получили ASCII-коды букв «A» и «B». В этом случае в тестирующую систему надо будет отправить ответ:

KALUGA{AB}

Для того чтобы сообщение было сложно расшифровать, нужно, чтобы простые числа, которые используются для получения числа n, были достаточно большими.

Алиса и Боб не стали использовать достаточно большие числа. К вам попало зашифрованное сообщение:

68 63 108 61 51 64 68 108 83

Открытый ключ (111, 65)

Расшифруйте сообщение. Оно и будет искомым флагом.

Примечание.

Таблица ASCII

A - 65 B - 66 C - 67 D - 68 E - 69 F - 70 G - 71 H - 72 I - 73 J - 74
K - 75 L - 76 M - 77 N - 78 O - 79 P - 80 Q - 81 R - 82 S - 83 T - 84
U - 85 V - 86 W - 87 X - 88 Y - 89 Z - 90

3. «Secret chat»

Два участника олимпиады Алиса и Боб вели переписку в защищённом чате. По крайней мере, так они думали. Но забыли одно простое правило: **«Если не шифруешь – все читают».**

Вы перехватили их сессию. Найдите то, что они хотели скрыть

По ссылке «*Скачать условие*» Вам будет доступен файл – дамп сетевого трафика **secret_chat.pcap.**

Проанализируйте его и найдите флаг в формате KALUGA{...}.

4. «V1g3n3r3 Brute»

В архиве лежит зашифрованное сообщение, найденное в старом ноутбуке хакера 2007 года.

По слухам, он использовал **шифр Виженера** – «непробиваемый» в своё время.

Для зашифровывания используется таблица алфавитов, называемая *tabularecta* или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на одну позицию больше чем предыдущая. Первые строки таблицы имеют вид:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
```
и т.д.

На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Запишем циклически ключевое слово, пока его длина не будет соответствовать длине исходного текста. Первый символ исходного текста будет зашифрован последовательностью, которая является первым символом ключа.Точно так же для второго символа исходного текста используется второй символ ключа и т.д.

Ключ – одно английское слово, связанное с CTF.

Расшифруйте письмо и найдите флаг.

По ссылке «*Скачать условие*» Вам будет доступен файл **cipher.txt**, содержащий зашифрованный текст.

Известно:

- Алфавит: только заглавные латинские буквы (A–Z), всё остальное (пробелы, знаки) сохранено как есть.
- Ключ — одно слово на английском, длина от 3 до 8 букв.
- Флаг имеет формат KALUGA{...} и находится внутри расшифрованного текста.

5. «Matryoshka of Encodings»

Хакер спрятал флаг в матрёшке из кодировок.

Чтобы добраться до сердцевины, нужно раскодировать слой за слоем: сначала один, потом другой, потом третий…

В файле **layer.txt** лежит строка. Это – самый внешний слой матрёшки.

Раскодируйте его и Вы получите следующий слой.

Повторяйте, пока не найдёте флаг в формате KALUGA{...}.

Подсказка: Все кодировки – текстовые и обратимые.

6. «Reverrrs!»

В далёком цифровом городе Калуга-Сити жил-был молодой хакер по имени Реверс. Он не взламывал банки и не крал пароли – он раскрывал тайны, спрятанные в коде.

Однажды злобный Мусорный Бот зашифровал секретный флаг и разбросал его по памяти, окружив ложными следами, мусорными функциями и фальшивыми флагами!

«Пусть попробуют найти настоящий!» – злорадно хихикнул Бот и ушёл в глубины бинарника.

Но Реверс не сдался. Он взял свой любимый отладчик, открыл дизассемблер и начал анализировать шаг за шагом…

Сможете ли Вы повторить путь Реверса и восстановить настоящий флаг?

По ссылке «*Скачать условие*» Вам будет доступен файл **reverrrs.exe**, содержащий бинарный код.