МАТЕРИАЛЫ ЗАДАНИЙ МЕЖРЕГИОНАЛЬНОЙ ОЛИМПИАДЫ ШКОЛЬНИКОВ ИМЕНИ И.Я. ВЕРЧЕНКО ПО ПРОФИЛЮ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ» (2024/2025 УЧЕБНЫЙ ГОД)

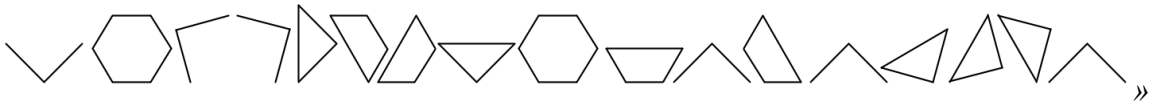
ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП
11 КЛАСС

Задача 1. Солнечный шифр

Вариант 1

Отдел информационной безопасности перехватил подозрительные письма от одного из сотрудников компании на подозрительный почтовый ящик. Письма всегда содержали время, странную последовательность символов и вложение с геометрической фигурой. Вот последнее сообщение, которое удалось перехватить:

«В – 12 часов, и – 25-35 минут, буду ждать тебя



В ходе анализа отдел информационной безопасности не смог расшифровать часть, где встречались странные символы. Было установлено, что это побитая кодировка, однако после этих сообщений были зафиксированы утечки конфиденциальной информации. Также, во вложении к письму была прикреплена картинка со странной геометрической фигурой и расположенными на ней буквами (рисунок 1).

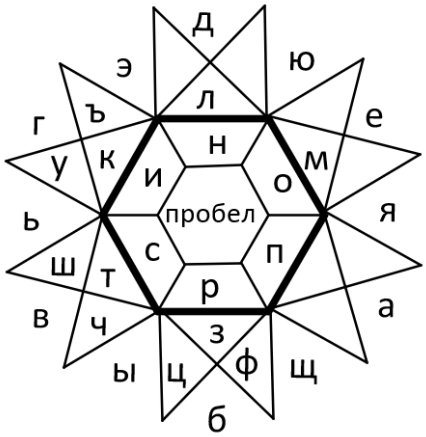


Рисунок 1 – Странная геометрическая фигура

Отдел информационной безопасности считает, что с помощью этой фигуры и предоставленного письма можно расшифровать сообщение. Ваша задача на основе предоставленных данных установить место очередной передачи конфиденциальной информации. В ответе укажите исходное сообщение.

Вариант 2

Отдел информационной безопасности перехватил подозрительные письма от одного из сотрудников компании на подозрительный почтовый ящик. Письма всегда содержали время, странную последовательность символов и вложение с геометрической фигурой. Вот последнее сообщение, которое удалось перехватить:

«В – 6 часов, и – 5-15 минут, буду ждать тебя

»

В ходе анализа отдел информационной безопасности не смог расшифровать часть, где встречались странные символы. Было установлено, что это побитая кодировка, однако после этих сообщений были зафиксированы утечки конфиденциальной информации. Также, во вложении к письму была прикреплена картинка со странной геометрической фигурой и расположенными на ней буквами (рисунок 1).

.

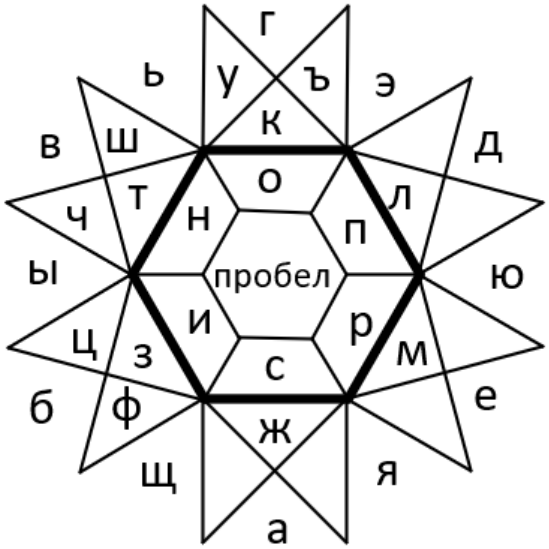


Рисунок 1 – Странная геометрическая фигура

Отдел информационной безопасности считает, что с помощью этой фигуры и предоставленного письма можно расшифровать сообщение. Ваша задача на основе предоставленных данных установить место очередной передачи конфиденциальной информации. В ответе укажите исходное сообщение.

Задача 2. Таблица символов

Вариант 1

В предполагаемом месте встречи агента был найден ноутбук. В ходе анализа его содержимого была обнаружена таблица символов (таблица 1) и скриншот формулы (рисунок 1).

Экспертами установлено, что в таблице символов скрыт пароль от рабочего стола ноутбука, каждая буква которого находится на определенной позиции, вычисляемой с помощью указанной формулы.

Определите пароль, если известно, что координаты первого символа: $(x_0, y_0) = (5, 6)$, длина пароля – *13* символов, и пароль является осмысленным словом. В ответе укажите сам пароль и значения параметров формулы.

Таблица 1 – Таблица символов

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
1	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	О	Ю	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	О	Ю
2	Я	А	Б	В	Г	Н	Е	Ё	Ж	Ф	И	Й	К	Л	М	Н	Я	Ц	Б	В	Г	Н	Е	Ё	Ж	З	И	Й	К	Л	М	Н
3	О	П	Р	С	Т	У	Ф	Ч	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	О	П	Р	С	Т	У	Ф	Ч	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
4	Ю	Я	А	Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Ю	Я	А	Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
5	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ц	Ш	Щ	Ъ	Ы	Ь	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ц	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	А	Б	К	Г	Д	Е	Ё	Ж	З	И	С	К	Л	Э	Ю	Я	А	Б	К	Г	Д	Е	Ё	Ж	З	И	Я	К	Л
7	М	Н	О	П	Р	С	Т	У	Н	Х	Ц	Ч	Ш	Щ	Ъ	Ы	М	Н	О	П	Р	С	Т	У	Н	Х	Ц	Ч	Ш	Щ	Ъ	Ы
8	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	Е	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	Е
9	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
10	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	И	И	Й	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	И	И	Й
11	К	Л	М	Н	С	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	К	Л	М	Н	С	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
12	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	О	Ё	Ж	З	И	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	О	Ё	Ж	З	И
13	Й	К	Е	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Й	К	Е	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
14	Щ	А	Ы	Ь	Э	Ю	Я	А	Б	Т	Т	Д	Е	Ё	Ж	З	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	Т	Т	Д	Е	Ё	Ж	З
15	Л	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Л	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
16	А	Б	В	Г	Д	Е	Ё	И	З	И	Й	К	Л	М	Н	С	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	И
17	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	О	Ю	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	О	Ю
18	Я	А	Б	В	Г	Н	Е	Ё	Ж	З	И	Й	К	Л	М	Н	Я	А	Б	В	Г	Н	Е	Ё	Ж	З	И	Й	К	Л	М	Н
19	О	П	Р	С	Т	У	Ф	Ч	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	О	П	Р	С	Т	У	Ф	Ч	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
20	Ю	Я	А	Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Ю	Я	А	Я	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
21	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ц	Ш	Щ	Ъ	Ы	Ь	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ц	Ш	Щ	Ъ	Ы	Ь
22	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
23	М	Н	О	П	Р	С	Т	У	Н	Х	Ц	Ч	Ш	Щ	Ъ	Ы	М	Н	О	П	Р	С	Т	У	Н	Х	Ц	Ч	Ш	Щ	Ъ	Ы
24	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	Е	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	Е
25	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
26	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	И	И	Й	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	И	И	Й
27	К	Л	М	Н	С	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	К	Л	М	Н	С	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
28	Ъ	Ы	Ь	И	Ю	Я	А	Б	В	Г	Д	Л	Ё	Ж	З	И	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	А	Ё	Ж	З	И
29	Й	К	Е	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Й	К	Е	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
30	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	Т	Т	Д	Е	Ё	Ж	З	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	Т	Т	Д	Е	Ё	Ж	З
31	Л	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Л	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч

$$x_{i+1} = ((x_i + a^2)^{a \mid x_i} + a\ )\ mod\ 32,$$
$$y_{i+1} = ((y_i + b^2)^{b \mid y_i} + b)\ mod\ 32$$

Рисунок 1 – Формулы вычисления координат символов,
mod – операция остатка от деления,
| – побитовое ИЛИ (OR).

Вариант 2

В предполагаемом месте встречи агента был найден ноутбук. В ходе анализа его содержимого была обнаружена таблица символов (таблица 1) и скриншот формулы (рисунок 1).

Экспертами установлено, что в таблице символов скрыт пароль от рабочего стола ноутбука, каждая буква которого находится на определенной позиции, вычисляемой с помощью указанной формулы.

Определите пароль, если известно, что координаты первого символа: $(x_0, y_0) = (8, 3)$, длина пароля – *12* символов, и пароль является осмысленным словом. В ответе укажите сам пароль и значения параметров формулы.

Таблица 1 – Таблица символов

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	О	Ф	У	Т	С	Р	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	О	Ф	У	Т	С	Р
1	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	П	О	Н	М	Л	К	Я	И	З	Ж	Ё	Е	Д	Г	В	Б
2	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	И	Ч	Ц	Х	Ф	У	Т	С	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	И	Ч	Ц	Х	Ф	У	Т	С
3	Р	П	О	Н	М	Л	К	Й	В	З	Ж	Ё	Е	Д	Г	О	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	О
4	Б	А	Я	Ю	Э	Ь	О	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	Б	А	Я	Ю	Э	Ь	О	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т
5	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Т	Д	Г	С	Р	П	О	Н	М	Л	К	Й	И	И	Ж	Ё	Т	Д	Г
6	В	Б	А	Я	П	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	В	Б	А	Я	П	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У
7	Т	С	Р	П	О	Н	М	Л	К	Й	И	Е	Ж	Ё	Е	Д	Т	С	Р	П	З	Н	У	Л	К	Й	И	Е	Ж	Ё	Е	Д
8	Г	В	Я	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	Г	В	Я	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф
9	У	Т	С	Р	П	О	З	М	Л	С	Й	И	З	Ж	Ё	Е	У	Т	С	Р	П	О	Н	М	Л	С	Й	И	З	Ж	Ё	Е
10	И	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	И	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х
11	Ф	У	Т	С	Р	П	О	Р	М	Л	К	Й	И	З	Ж	Ё	Ф	У	Т	С	Р	П	О	Р	А	Л	К	Й	И	З	Ж	Ё
12	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц
13	Х	Ф	У	Т	С	Н	П	О	Н	М	Л	К	Й	И	З	Ж	Х	Ф	У	Т	С	Н	П	О	Н	М	Л	К	Й	И	З	Ж
14	Ё	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Т	Щ	Ш	Ч	Ё	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Т	Щ	Ш	Ч
15	Ц	Х	Ф	В	И	С	Р	П	О	Н	М	Л	К	Й	И	З	Ц	Х	Ф	В	Т	С	Р	П	О	Н	М	Л	К	Й	И	З
16	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	О	Ф	У	Т	С	Р	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	О	Ф	У	Т	С	Р
17	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б
18	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	И	Ч	Ц	Х	Ф	У	Т	С	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	И	Ч	Ц	Х	Ф	У	Т	С
19	Р	П	О	Н	М	Л	К	Й	А	З	Ж	Ё	Е	Д	Г	О	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	О
20	Б	А	Я	Ю	Э	Ь	О	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	Б	А	Я	Ю	Э	Ь	О	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т
21	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Т	Д	Г	С	Р	П	О	Н	М	Л	К	Й	И	Ц	Ж	Ё	Т	Д	Г
22	В	Б	А	Я	П	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	В	Б	А	Я	П	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У
23	Т	С	Р	П	О	Н	М	Л	К	Й	И	Е	Ж	Ё	Е	Д	Т	С	Р	П	И	Н	М	Л	К	Й	И	Е	Ж	Ё	Е	Д
24	Г	В	Я	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	Г	В	Я	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф
25	У	Т	С	Р	П	О	Н	М	Л	С	Й	И	З	Ж	Ё	Е	У	Т	С	Р	П	О	Н	М	Л	С	Й	И	З	Ж	Ё	Е
26	И	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	И	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х
27	Ф	У	Т	С	Р	П	О	Р	М	Л	К	Й	И	З	Ж	Ё	Ф	У	Т	С	Р	П	О	Р	М	Л	К	Й	И	З	Ж	Ё
28	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц
29	Х	Ф	У	Т	С	Н	П	О	Н	М	Л	К	Й	И	З	Ж	Х	Ф	У	Т	С	Н	П	О	Н	М	Л	К	Й	И	З	Ж
30	Ё	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Т	Щ	Ш	Ч	Ё	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Т	Щ	Ш	Ч
31	Ц	Х	Ф	В	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ц	Х	Ф	В	Т	С	Р	П	О	Н	М	Л	К	Й	И	З

$$x_{i+1} = ((x_i + a^2)^{a \mid x_i} + a\ )\ mod\ 32,$$
$$y_{i+1} = ((y_i + b^2)^{b \mid y_i} + b)\ mod\ 32$$

Рисунок 1 – Формулы вычисления координат символов,
mod – операция остатка от деления,
| – побитовое ИЛИ (OR).

Задача 3. Обфускация

Вариант 1

На обнаруженном ноутбуке после подбора пароля от рабочего стола были найдены фрагменты вредоносного кода. Автор обфусцировал весь исходный код. Экспертами в ходе анализа был определен фрагмент функции аутентификации (листинг 1), которая возвращает `'True'` при вводе корректного пароля и запускает другие фрагменты кода.

Определите, что необходимо ввести, чтобы обнаруженный фрагмент аутентификации вернул `'True'`. Ответ обоснуйте.

Листинг 1. Фрагмент функции аутентификации

Python

```
exec('dAzD modify(sjhQweryuSWbE):\n    sjhQweryuSWbE =
sjhQweryuSWbE.s[3mlithE(\', \')\n    sjhQweryuSWbE = [inthE(s)+1 for s in
sjhQweryuSWbE]\n    sjhQweryuSWbE.reverse()\n    key = \'o\'\n    sjhQweryuSWbE
= [s^ord(key) for s in sjhQweryuSWbE]\n    ryuSWbEurn [c(42)(s) for s in
sjhQweryuSWbE]\ndAzD
chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE):\n    sjhQweryuSWbE=modify(sjhQweryuSWbE)\
n    ryuSWbEurn \'\'.join(sjhQweryuSWbE) ==  "Ha[3m[3mYNioskjear_" + c(487tHH0)
+ c(42)(48) + c(487tHH0) +
c(487tHH3)\n[3mrinthE(chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE))\n'.replace('87tHH',
'2)(5').replace('yuSWb', 'eth').replace('ioskj', 'ewY').replace('(42)',
'hr').replace('AzD', 'ef').replace('qQT', 'ut').replace('[3m',
'p').replace('jhQwe', 'ec').replace('thE', 't'), {'secret': input()})
```

Вариант 2

На обнаруженном ноутбуке после подбора пароля от рабочего стола были найдены фрагменты вредоносного кода. Автор обфусцировал весь исходный код. Экспертами в ходе анализа был определен фрагмент функции аутентификации (листинг 1), которая возвращает `'True'` при вводе корректного пароля и запускает другие фрагменты кода.

Определите, что необходимо ввести, чтобы обнаруженный фрагмент аутентификации вернул `'True'`. Ответ обоснуйте.

Листинг 1. Фрагмент функции аутентификации

Python

```
exec('dAzD modify(sjhQweryuSWbE):\n    sjhQweryuSWbE =
sjhQweryuSWbE.s[3mlithE(\', \')\n    sjhQweryuSWbE = [inthE(s)+1 for s in
sjhQweryuSWbE]\n    sjhQweryuSWbE.reverse()\n    key = \'o\'\n    sjhQweryuSWbE
= [s^ord(key) for s in sjhQweryuSWbE]\n    ryuSWbEurn [c(42)(s) for s in
sjhQweryuSWbE]\ndAzD
chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE):\n    sjhQweryuSWbE=modify(sjhQweryuSWbE)\
n    ryuSWbEurn \'\'.join(sjhQweryuSWbE) ==  "MerryC(42)isthEmas" + c(487tHH0) +
c(42)(48) + c(487tHH0) +
c(487tHH3)\n[3mrinthE(chjhQwek_sjhQweryuSWbE(sjhQweryuSWbE))\n'.replace('87tHH',
'2)(5').replace('yuSWb', 'eth').replace('ioskj', 'ewY').replace('(42)',
'hr').replace('AzD', 'ef').replace('qQT', 'ut').replace('[3m',
'p').replace('jhQwe', 'ec').replace('thE', 't'), {'secret': input()})
```

Задача 4. Тайное послание

Вариант 1

После успешного прохождения аутентификации и запуска специальной программы на ноутбуке был обнаружен скрытый раздел, на котором хранились файлы с историей переписки. Установлено, что в тексте переписки спрятан адрес следующей цели атаки хакеров. У команды аналитиков есть подозрение, что использовался метод, связанный с количеством пробелов в каждом абзаце.

Помогите найти закономерность в сообщении и расшифровать данные, указывающие на следующую цель хакеров. В ответе укажите следующую цель хакеров, решение обоснуйте.

К задаче прилагается:
файл «*message_v1.txt*»

Вариант 2

После успешного прохождения аутентификации и запуска специальной программы на ноутбуке был обнаружен скрытый раздел, на котором хранились файлы с историей переписки. Установлено, что в тексте переписки спрятан адрес следующей цели атаки хакеров. У команды аналитиков есть подозрение, что использовался метод, связанный с количеством пробелов в каждом абзаце.

Помогите найти закономерность в сообщении и расшифровать данные, указывающие на следующую цель хакеров. В ответе укажите следующую цель хакеров, решение обоснуйте.

К задаче прилагается:
файл «*message_v2.txt*»

Задача 5. Система защиты

Вариант 1

После получения информации о возможной компьютерной атаке, в компании решили установить и настроить систему защиты от DDoS-атак. Система анализирует журналы активности пользователей и вычисляет количество запросов от уникальных пользователей на каждый ресурс в единицу времени. Журналы содержат информацию о попытках доступа к серверу, включая время обращения, IP-адрес источника, IP-адрес назначения. Если количество одновременных подключений разных пользователей превышает пороговое значение для конкретного ресурса, выдается предупреждение о возможной DDoS-атаке.

Перед запуском системы необходимо её настроить (обучить) на корректном трафике. Для этих целей был подготовлен журнал запросов от сотрудников компании за определенный период времени ко всем внутренним информационным ресурсам компании.

Администраторам требуется настроить систему защиты для следующих информационных ресурсов:

– web-сервер (IP-адрес: 172.17.148.17),
– почтовый сервер (IP-адрес: 172.17.148.18).

Определите, какое максимальное количество одновременных подключений разных пользователей в минуту необходимо установить в системе защиты для указанных ресурсов, чтобы она корректно работала и не выдавала ложных предупреждений. Разработчики рекомендуют устанавливать пороговое значение на *20%* больше максимально возможного числа подключений в единицу времени.

В ответе укажите ресурс и пороговое значение (количество подключений в единицу времени), а также обоснование выбранного значения.

К задаче прилагается:
файл «*log_v1.log*» – журнал посещений

Вариант 2

После получения информации о возможной компьютерной атаке, в компании решили установить и настроить систему защиты от DDoS-атак. Система анализирует журналы активности пользователей и вычисляет количество запросов от уникальных пользователей на каждый ресурс в единицу времени. Журналы содержат информацию о попытках доступа к серверу, включая время обращения, IP-адрес источника, IP-адрес назначения. Если количество одновременных подключений разных пользователей превышает пороговое значение для конкретного ресурса, выдается предупреждение о возможной DDoS-атаке.

Перед запуском системы необходимо её настроить (обучить) на корректном трафике. Для этих целей был подготовлен журнал запросов от сотрудников компании за определенный период времени ко всем внутренним информационным ресурсам компании.

Администраторам требуется настроить систему защиты для следующих информационных ресурсов:

– web-сервер (IP-адрес: 192.168.214.14),
– почтовый сервер (IP-адрес: 192.168.214.16).

Определите, какое максимальное количество одновременных подключений разных пользователей в минуту необходимо установить в системе защиты для указанных ресурсов, чтобы она корректно работала и не выдавала ложных предупреждений. Разработчики рекомендуют устанавливать пороговое значение на *20%* больше максимально возможного числа подключений в единицу времени.

В ответе укажите ресурс и пороговое значение (количество подключений в единицу времени), а также обоснование выбранного значения.

К задаче прилагается:
файл «*log_v2.log*» – журнал посещений