**11 класс**

**1. Парольная комбинация**

Для входа в систему используется пароль, состоящий из трёх шестизначных чисел, расположенных следующим образом:

хххххх-хххххх-хххххх

Известно, что пароль состоит из *3-х неповторяющихся простых чисел* в диапазоне от 100 000 до 100 300. При этом *последняя цифра первого числа равна первой цифре второго числа, а последняя цифра второго числа равна первой цифре третьего числа*.

Пример:

ххххх3-3хххх7-7ххххх

Задержка между попытками входа в систему равна 1 секунде. За какое максимальное количество времени (в секундах) можно гарантированно получить пароль, если на ввод пароля время не тратится?

**2. Мессенджер**

В компании для общения между сотрудниками используется мессенджер собственной разработки, который передает сообщения в зашифрованном виде. Шифрование производится с использованием метода «двоичного гаммирования» или путем выполнения операции «побитового исключающего ИЛИ» между байтами сообщения и ключа. Для каждого сотрудника ежедневно генерируется новый ключ по следующей формуле

К = (Ф1\*И1 + Ф2И2 + … +ФNИN) div C,

где Ф1,Ф2,…,ФN – код букв дополненной фамилии в соответствии с таблицей ASCII (регистр учитывается),

И1,И2,…,ИN – код букв дополненного имени в соответствии с таблицей ASCII (регистр учитывается),

N – максимум из длин фамилии и имени сотрудника,

C – сумма всех цифр текущей даты в формате ДД-ММ-ГГГГ,

div – операция целочисленного деления (целая часть от деления).

Если длина фамилии меньше длины имени, то фамилия дополняется путем дозаписи в конец циклического повторения букв фамилии, пока её длина не сравняется с длиной имени. Аналогично с именем, если его длина меньше длины фамилии.

Например, для сотрудника с ФИО 'Ivanov Petr' 5 марта 2023 ключ будет вычисляться следующим образом:

1. Выравнивание длин имени и фамилии – имя дополняется двумя дополнительными символами:

Ivanov – 73 118 97 110 111 118

PetrPe – 80 101 116 114 80 101

1. Вычисление суммы цифр даты:

C = 0 + 5 + 0 + 3 + 2 + 0 + 2 +3 = 15

1. Вычисление ключа:

K = (73\*80+118\*101+97\*116+110\*114+111\*80+118\*101) div 15 =

= 415610 = 103C16 = 0001 0000 0011 11002.

Далее байты текстового сообщения складывается по модулю 2 с байтами, полученными циклическим повторением последовательности байтов вычисленного ключа.

Руководитель отдела разработки дал поручения своим сотрудникам в течение дня 21 февраля 2023 года написать в чат название аэропорта, откуда им удобнее вылетать в командировку: VKO или DME. Проанализируйте полученный им зашифрованный поток сообщений из мессенджера и определите:

1) кто не выполнил поручение руководителя?

2) за какой аэропорт проголосовало большинство сотрудников?

*К задаче прилагается:*

*«list\_v1.txt»* – список сотрудников;

*«cypher\_v1.txt»* – зашифрованный текст переписки в мессенджере.

1. **Web-сайт**

Олег создал сайт, в котором спрятал IP-адрес своего секретного сервера в формате xxx.xxx.xxx.xxx (xxx – число от 0 до 255). На сайте Олег оставил подсказки. Определите IP-адрес секретного сервера Олега.

*К задаче прилагается:*

*папка «3\_задача» – папка с содержимым сайта*

1. **Вирус**

Имеется система, представляющая собой файл-серверную архитектуру, состоящую из 1 файл-сервера и 6 ПК. На файл-сервере хранится 30 файлов-приложений (file1.exe, file2.exe, …, fileN.exe). Известно, что один из файлов заражён вредоносным кодом, который после попадания на клиентское устройство выводит его из строя через 1 час. Каждый ПК может копировать с файл-сервера любое количество файлов.

За какое минимальное количество часов можно точно определить зараженный файл. Ответ обоснуйте.

1. Сетевая стеганография

Агенты одной спецслужбы общаются по открытому каналу связи с помощью сетевых пакетов. Известно, что для передачи текстовых сообщений они используют значения некоторых полей заголовков пакетов.

Администратору удалось перехватить фрагмент передаваемых данных. Изучите его и извлеките передаваемое сообщение. Ответ обоснуйте.

*К задаче прилагается:*

«packets\_v1.cap» – дамп сетевого трафика со скрытым текстовым сообщением.