Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра ИПиЭ

Дисциплина: Криптографические технологии

Отчет

по Лабораторной работе №5

на тему «Исследование методов идентификация и аутентификация пользователя. Протоколы рукопожатия и идентификации типа запрос-ответ»

Студент гр. 910902 Шпак В.А.

Проверил Давыдович К.И.

Минск 2022

Цель работы: научиться определять время перебора всех паролей, минимальную длину пароля, а также подобрать пароль для архива с помощью специальной программы.

Ход работы:

Задание 1.

Вариант 5.

1. Определить время перебора всех паролей с параметрами.

n = 59 – количество символов алфавита

k = 5 – длина пароля

s = 200 – скорость перебора пароля в секунду

m = 0 – неправильно введенные пароли

v =0 – пауза

Количество вариантов: $C = 59^5$

Время перебора всех паролей:

t = C/s = 3 574 621с = 59 577 мин = 993 ч = 41 день.

Время перебора всех паролей:

T = t*0 = 0

$T_{итог}$ = t + T = 41 день.

2. Определить минимальную длину пароля

n = 59 - количество символов алфавита

t = 50 – время перебора

s = 200 – скорость перебора

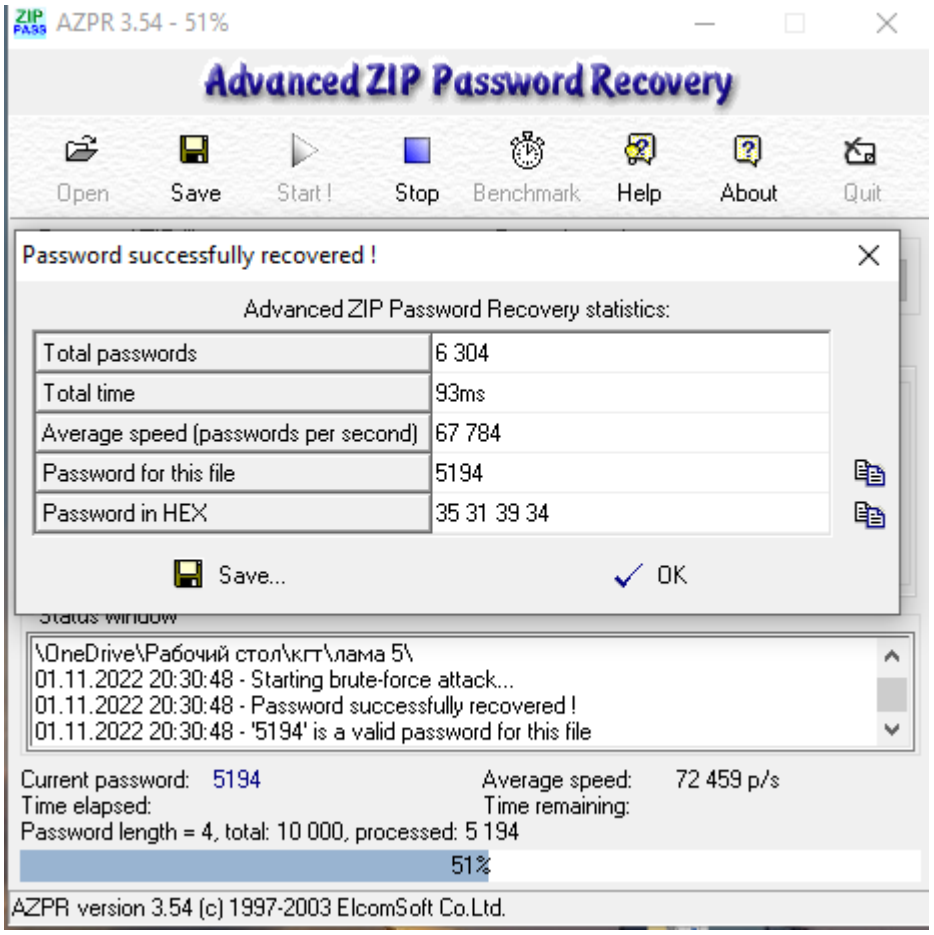
Количество вариантов: $C = t * s = 50*200 = 10\ 000 = 3.15*10^{10}$

Длина пароля: $k = \lg C = \lg(3.15*10^{10}) = 10.5$

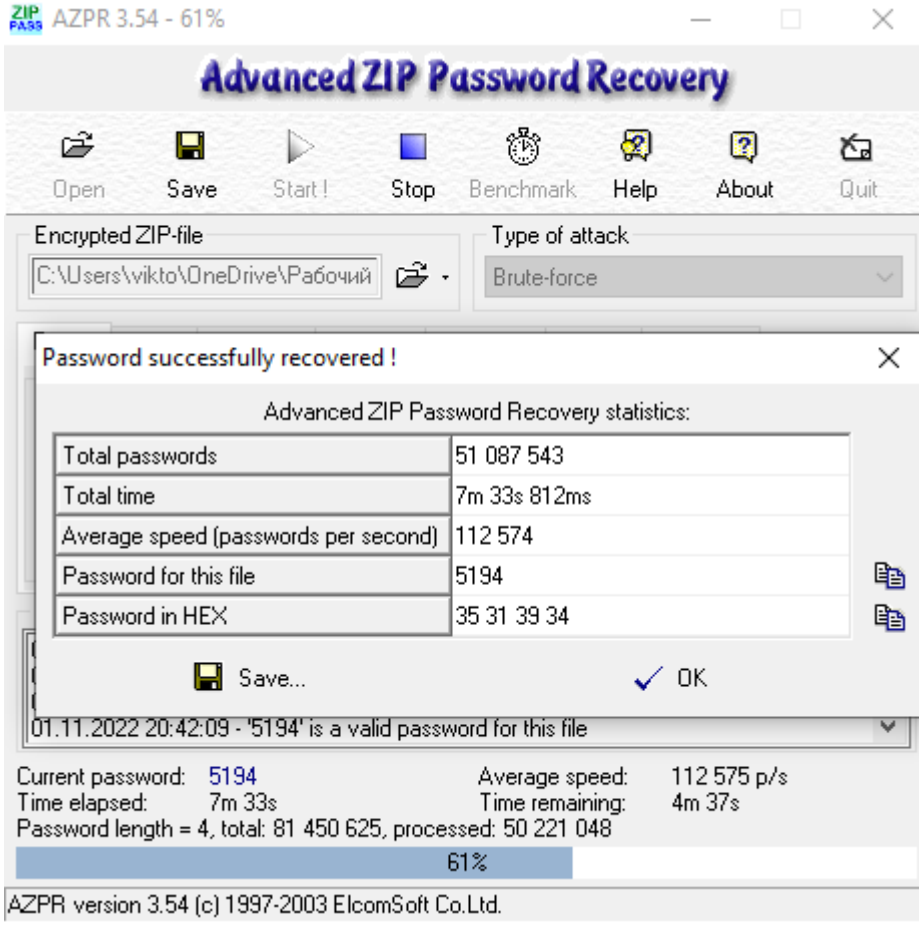
Длина пароля должна быть не менее 11 символов.

Задание 2.

Все цифры, длина 1-4

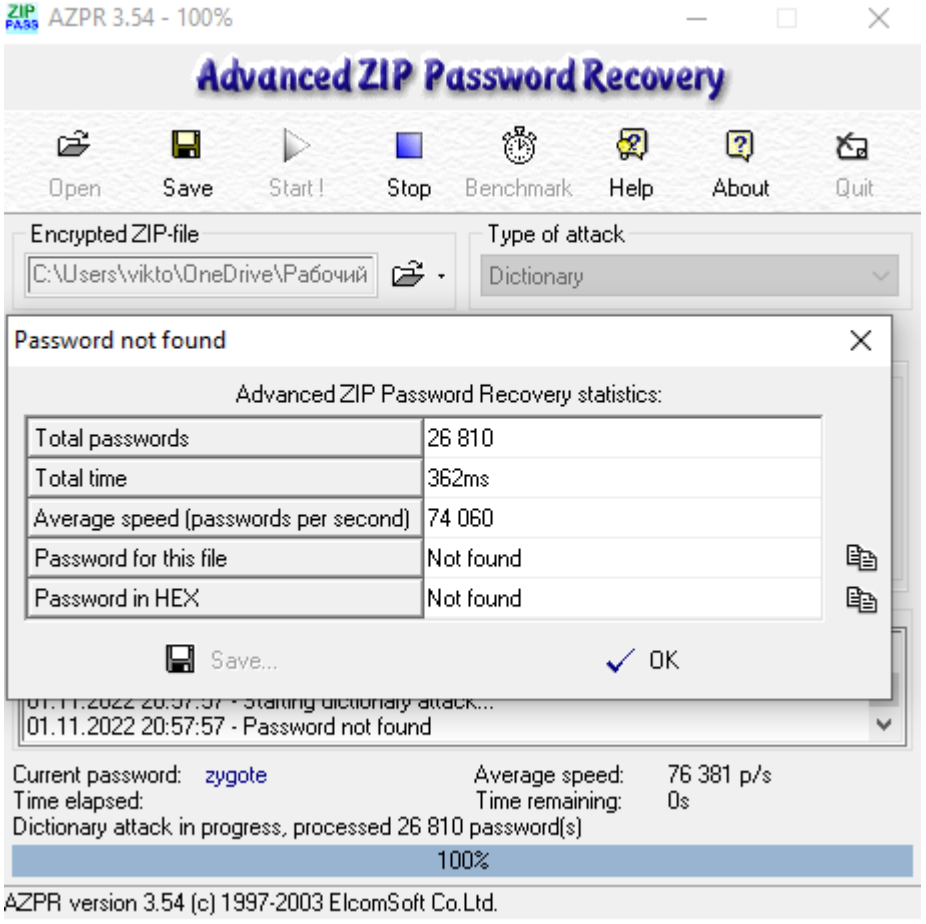


Все печатаемые.



Перебор по маске.

Перебор по словарю.



Вывод: таким образом, в ходе лабораторной работы мы научились определять время перебора всех паролей, минимальную длину пароля, а также подобрали пароль для архива с помощью специальной программы.