МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования   
«Гомельский государственный университет имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Отчёт по теме

**«ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ПАРОЛЯ»**

Студент группы МС-22 Яковенко Т.В.

Проверил: ст. преп. Соколов С.И.

Гомель 2022

Цель работы

**Цель работы**

Целью работы является исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

**Задание**

Проведение атаки перебором (bruteforce attack)

1. Создайте запароленный архив, используя программу WinRar, при этом

длина пароля должна составлять от 1 до 8 символов для различных алфавитов:

А) только английские малые буквы;

Б) только английские малые буквы и цифры;

В) английские буквы большого и малого регистра и цифры.

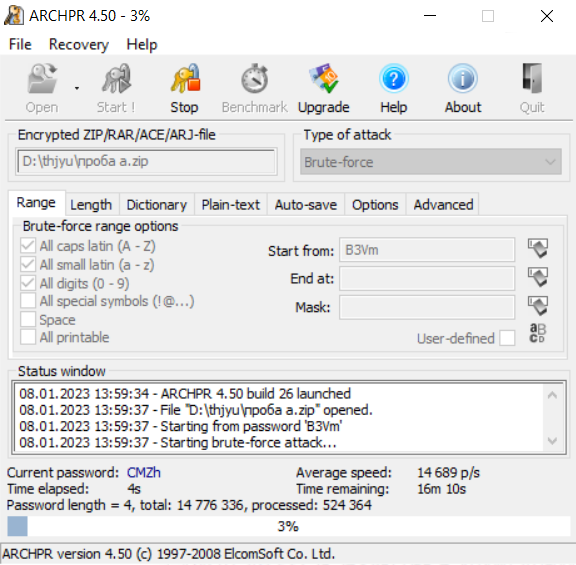
Используя программу для вскрытия паролей произвести атаку на

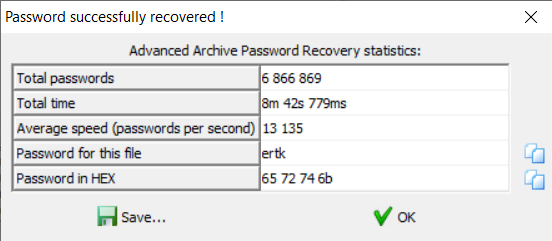
зашифрованный файл. Область перебора – английские буквы большого и малого

регистра и цифры, длина пароля от 1 до 8 символов. Проверить правильность

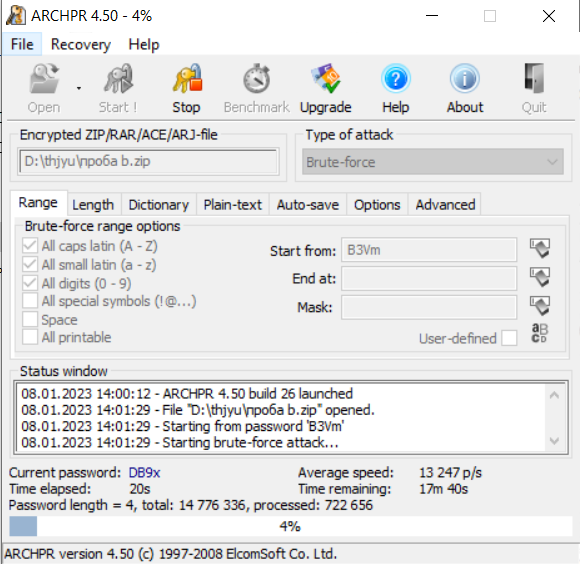
определенного пароля, распаковав файл и ознакомившись с его содержимым.

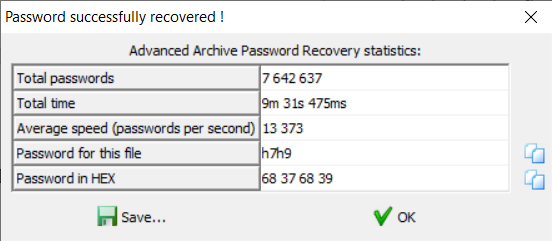
А)



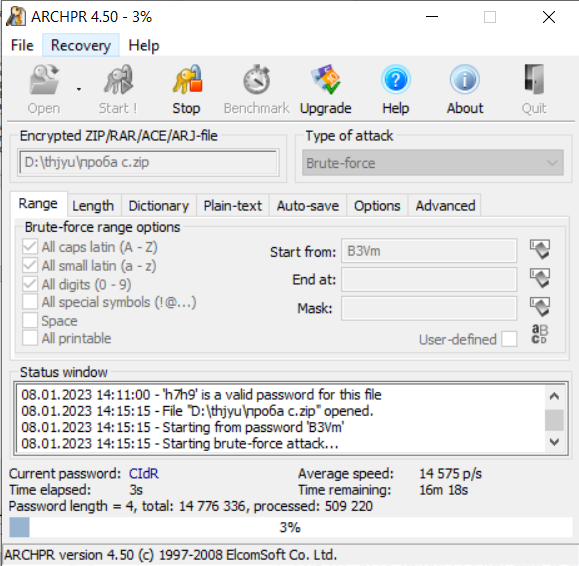


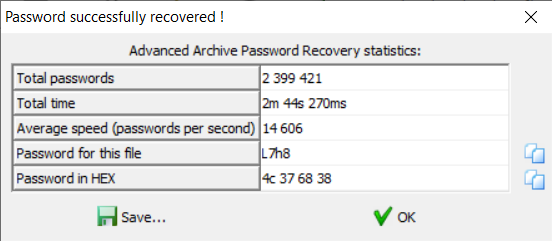
Б)





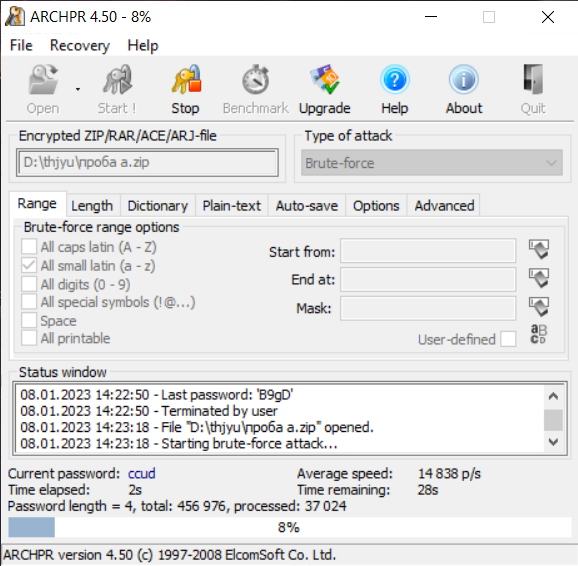
В)

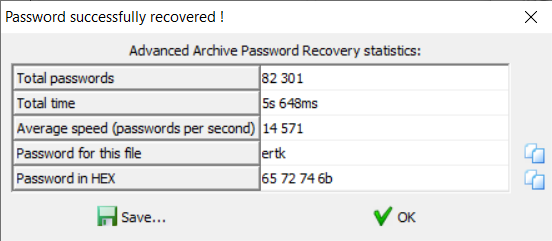




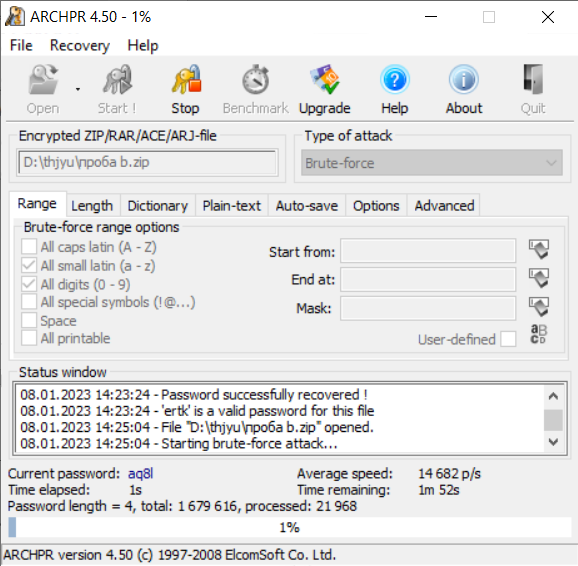
2. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время

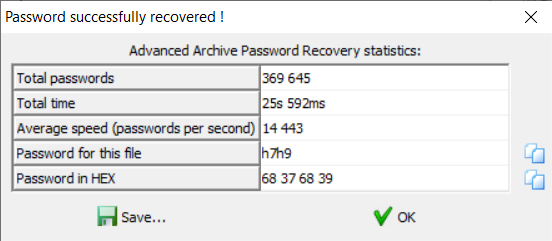
A)





Б)





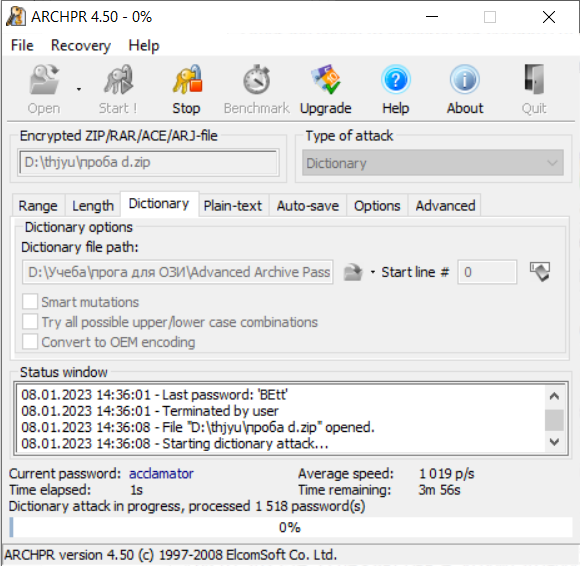
По результатам наших взломов мы видим, что при уточнении диапазона пароля мы получаем результата на много быстрее.

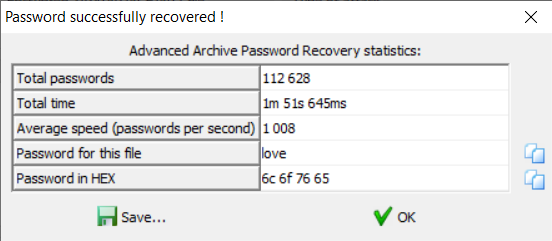
3. Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

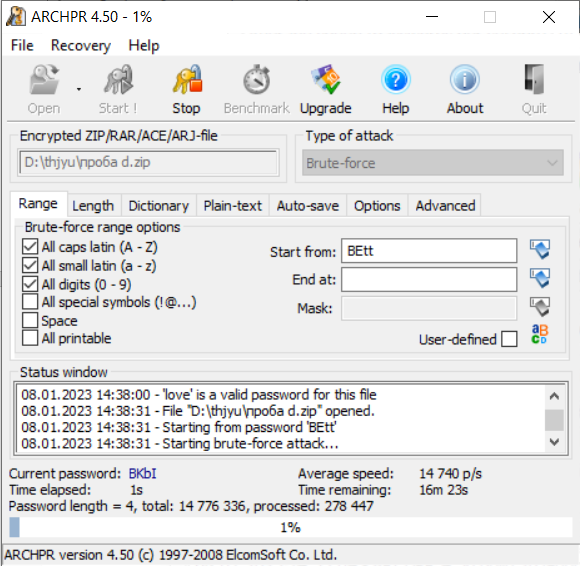
2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

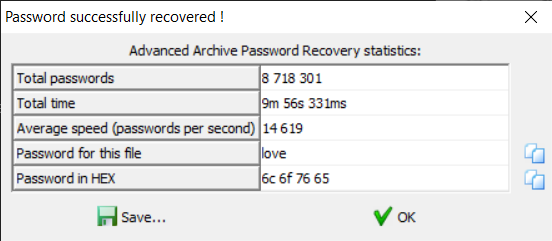
3.1





3.2





На этом примере видно, что с помощью словаря мы подобрали пароль намного быстрее чем через перебор

**Вывод**

В ходе лабораторной работы исследовали защиты с применением пароля, а также исследовали методов противодействия атакам на пароль. При взломе увидели эффективность различных паролей. познакомились с различными способами взлома пароля, проверили их эффективность.