**Министерство образования Республики Беларусь**

**Белорусский национальный технический университет**

**Факультет Информационных Технологий и Робототехники**

**Программное обеспечение информационных систем и технологий**

**Отчет**

**по лабораторным работам**

**по курсу «Основы защиты информации (с модулем основ управления интеллектуальной собственностью)»**

Выполнил: студент гр. 10702319 Опарина В. Р

Сачкова Е. Д.

Сугак Н. С.

Проверил: Барышев А. А.

Минск 2023

**ЛАБОРАТОРНАЯ РАБОТА №1**

Задания

1. Определить время перебора всех паролей. Алфавит состоит из n=26 символов. Длина пароля символов k=12. Скорость перебора s=13 паролей в секунду. После каждого из m=3 неправильно введенных паролей идет пауза в v=2 секунд.

Количество вариантов: С=n^k =26^12= 95 428 956 661 682 176

Время перебора всех паролей t= C/s=95 428 956 661 682 176/13 = =7 340 688 973 975 552 секунд≈122 344 816 232 925,867 минут ≈2 039 080 270 548,764часов≈84 961 677 939,5 дня.

После каждого из m=3 неправильно введенных паролей идет пауза в v=2 секунд. Получаем время перебора всех паролей T=t\*v/m= =7 340 688 973 975 552\*2/3= 4 893 792 649 317 034,67 секунд = =81 563 210 821 950,5 минут = 1 359 386 847 032,5 часов = 56 641 118 626,4 дней

Титог = t+T=84 961 677 939,5+56 641 118 626,4=141 602 796 565,9 дней = =387 952 867 лет

1. Определить минимальную длину пароля, алфавит которого состоит из n=26 символов, время перебора которого было не меньше t=120 лет. Скорость перебора s=13 паролей в секунду.

Длина пароля рассчитывается: k=logn C= lg C.

Определим количество вариантов C= t \* s=120лет\*13 паролей в сек. = =49 196 160 000 вариантов

Таким образом, получаем длину пароля: k=lg (49 196 160 000) = 10,69.

Значит минимальная длина пароля 11 символов

1. Определить количество символов алфавита, пароль состоит из k=6 символов, время перебора которого было не меньше t=120 лет. Скорость перебора s=13 паролей в секунду.

Длина пароля рассчитывается: k=logn C

Определим количество вариантов C= t \* s=120лет\*13 паролей в сек. = =49 196 160 000 вариантов

6= logn 49 196 160 000

n^6=49 196 160 000

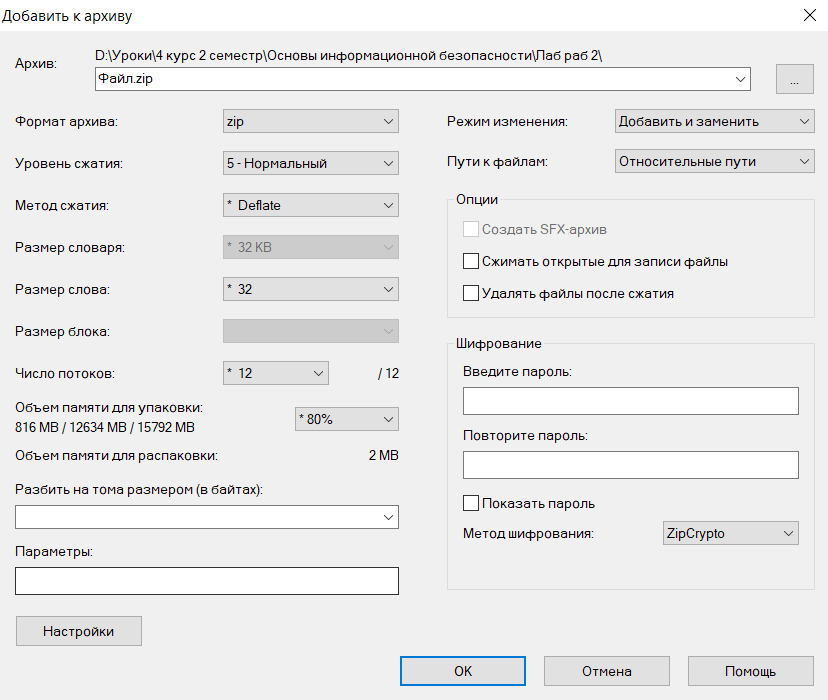
n=60,5 символов

Значит в алфавите 61 символ.

**ЛАБОРАТОРНАЯ РАБОТА №2**

Исходный файл







Время на подбор пароля, состоящего из 3 цифр 1,5 минуты

**ЛАБОРАТОРНАЯ РАБОТА №3**

1. Шифр Цезаря

Сдвиг – 1



Сачкова – Тбшлпгб

1. Лозунговый шифр

Слово-лозунг – физика

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| ф | и | з | к | а | б | в | г | д | е | ё | ж | й | л | м | н | о | п | р | м | с | у | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

Сачкова – Рфчжнзф

1. Полибианский квадрат



Сачкова – 41 11 51 26 34 13 11

1. Шифр Playfair

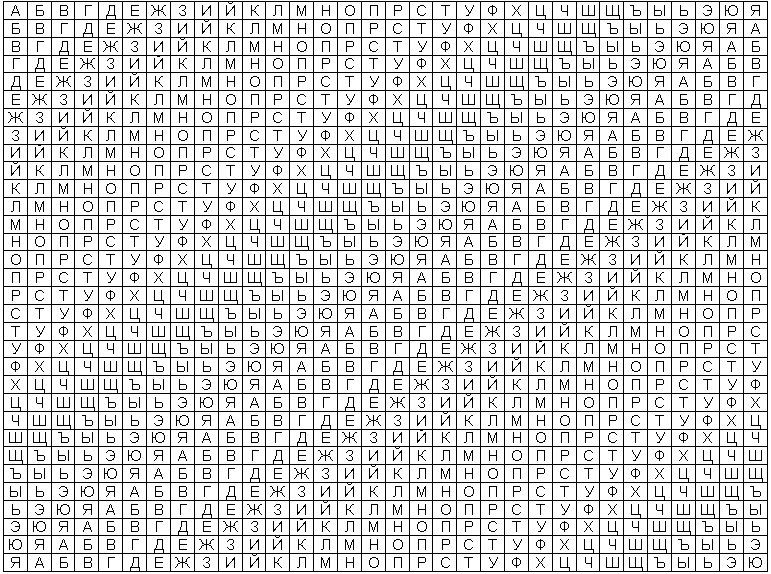
Слово – физика, вспомогательный символ - я

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ф | и | з | к | а | б |
| в | г | д | е | ё | ж |
| й | л | м | н | о | п |
| р | с | т | у | х | ц |
| ч | ш | щ | ъ | ы | ь |
| э | ю | я | - | 1 | 2 |

Сачкова – са чк ов ая – их фъ йё з1

1. Шифра Виженера

Слово – физика



Сачкова - ёияущвф