

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №1**

**В РАМКАХ ДИСЦИПЛИНЫ «МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В КМПЬЮТЕРНЫХ СИСТЕМАХ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Защита информации

1. Доступность
   1. Парольная аутентификация
   2. Смарт-карты (сим-карты, банковские)
2. Целостность
   1. Цифровая подпись
   2. CVS
3. Конфиденциальность
   1. Криптография
   2. Стеганография

Стойкость пароля зависит от

1. Длинны пароля
2. Мощность алфавита (256 максимальная для windows)
3. Срок действия
4. Отсутствие повторяющихся паролей
5. Отсутствие осознанных фраз
6. Количество попыток

В текущем задании мощность 128

Практика

**Задание 1**

Сколько пятибуквенных слов можно построить, используя весь русский алфавит?

1. Определение мощности алфавита (N=33 символа)
2. Длинна слова L=5 символов
3. Первый символ можно выбрать 33 способами
4. Далее перебираем второй символ одним из 33 способов с каждой комбинаций с первой ячейкой
5. Далее перебираем 3 ячейку 33 способами
6. Далее перебираем 4 ячейку 33 способами
7. В завершении перебираем 5 ячейку 33 способами
8. Итоговое кол-во слов = 335

**Задание 2**

Есть алфавит 20 символов. Из них необходимо выбрать 5 и отправить на конкурс.

1. Алфавит N=20 символов
2. Выбор первого символа 1 символ из 20
3. Выбор второго символа 1 символ из 19
4. Выбор второго символа 1 символ из 18
5. Выбор второго символа 1 символ из 17
6. Выбор второго символа 1 символ из 16
7. Возможное число комбинаций 20\*19\*18\*17\*16 = 1 860 480

**Задание 3**

Из 5 букв А,Б,В,Г,Д нужно составить все трехбуквенные слова

1. Мощность алфавита N=5 символов
2. Длинна L=5 символов
3. Выбор первой буквы 1 символ из 5
4. Выбор второй буквы 1 символ из 5
5. Выбор третьей буквы 1 символ из 5
6. Полное кол-во = 5\*5\*5=53

**Задание 3**

Сколько можно получит пятибуквенных слов в алфавите А, Б, В, Г, Д

1. Мощность алфавита N=5 символов
2. Длинна L=5 символов
3. Выбор первой буквы 1 символ из 5
4. Выбор второй буквы 1 символ из 4
5. Выбор третьей буквы 1 символ из 3
6. Выбор четвертой буквы 1 символ из 2
7. Выбор пятой буквы 1 символ из 1
8. Кол-во = 5\*4\*3\*2\*1=5!

**Задание 4**

Пусть пароль содержит в себе 5 символов, каждый символ может встречаться в пароле только один раз, латинский строчной алфавит (26). Злоумышленнику требуется на подбор одного пароля 30 секунд.

1. Мощность алфавита N=26 символов
2. Длинна L=5 символов
3. Выбор первой буквы 1 символов из 26
4. Выбор второй буквы 1 символов из 25
5. Выбор третьей буквы 1 символов из 24
6. Выбор четвертой буквы 1 символов из 23
7. Выбор пятой буквы 1 символов из 22
8. Общее число паролей 26\*25\*24\*23\*22=7 893 600 комбинаций
9. Общее время 236 800 000 секунд ~7.5 лет

**Задание 5**

Длинна пароля 5 символов, мощность алфавита 128 символов, мощность 48.3Гфлопс (48 300 флопс)

1. Мощность алфавита N=128 символов
2. Длинна L=5 символов
3. Выбор первой буквы 1 символ из 128
4. Выбор второй буквы 1 символ из 128
5. Выбор третьей буквы 1 символ из 128
6. Выбор четвертой буквы 1 символ из 128
7. Выбор пятой буквы 1 символ из 128
8. Общее кол-во паролей 1285 комбинаций
9. Время подбора = 1285:48300 ~ 8,23 дня

**Задание 6**

Количество сочетаний в таблице АСКИ = 2256

Перевести слово в двоичный код

Текст =11110010 11100101 11101010 11110001 11110010

Огонь=11101110 11100011 11101110 11101101 11111100

Сложить слова в двоичной системе

00011100 0000110 00000100 00011100 00001110

Перевести слова в десятичную систему

Текст=242 229 234 241 242

Огонь=238 227 238 237 252

Сложить полученные слова

224 200 216 222 238

**Теория**

Множество целых чисел Z

Множество действительных чисел M

Множество простых чисел (начало 2) P

НОД наименьший общий делитель

НОК наименьшее общее кратное (ищется через разложение)

**Задание 7**

Алфавит кириллица (33 символа), мощность 3.1 тфлопс, длина пароля 8 символов, каждый символ встречается 1 раз.

Найти: время подбора пароля

Количество возможных вариантов пароля 33\*32\*31\*30\*29\*28\*27\*26= 559 809 169 920 вариантов

Мощность 3.1 тфлопс = 3 100 000 000 000 флопс (операций в секунду)

Врем подбора пароля 559 809 169 920\3 100 000 000 000 ≈ 0.18 сек