**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Введение в профессиональную деятельность»

**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ**

«**Методы обеспечения целостности информации**»

**Выполнил:**

студент группы N3151

Мочеков Семён Сергеевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*



(подпись)

**Проверил:**

Таранов Сергей Владимирович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Санкт-Петербург

2023 г.

**Цель работы:**

Познакомиться с методами обеспечения целостности информации

**Задачи:**

* Выполнить задачи из теории кодирования
* Ознакомиться с работой хэш-функции md5
* Ознакомиться с использование цифровых подписей с помощью GnuPG и Kleopatra

**Задание 1.**

Исходное сообщение поделим на порождающий многочлен, которому соответствует двоичная запись. Результатом будет контрольная сумма, служащая для проверки ошибок при передаче данных. Не обнаруживаемые ошибки при получении контрольной суммы дают такой же результат, как и исходное сообщение, т.е дают ту же контрольную сумму. В таком случае факт ошибки не отличим от факта сохранения исходного сообщения.

*Вариант 0.*

Сообщение 1 = 11010110110 -> Контр. сумма = 1110000 <- Ошибка = 100011011100

Сообщение 2 = 10101101101 -> Контр. сумма = 1000011 <- Ошибка = 100000110010

*Вариант 2.*

Сообщение 1 = 101010101010 – > Контр. Сумма = 11110100 <- Ошибка = 1000001100111

Сообщение 1 = 100000111110 – > Контр. Сумма = 11100111 <- Ошибка = 1000010010101

*Вариант 1.*

На основе проверочной матрицы получим порождающую k\*n:

| 1 0 0 1 1 1 |

| 0 1 0 1 1 0 |

| 0 0 1 0 1 1 |

Т.к длина исходного сообщения k = 3, а длина закодированного n = 6, всему набору 2k сообщений: 000, 001, 010, 100, 011, 101, 110, 111 сгенерируем по порождающей матрице кодовое пространство:

000000, 001011, 010110, 100111, 011101, 101100, 110001, 111010

Не обнаруживаемые ошибки возможно получить комбинациями векторов кодового пространства, ведь результатом будет так же элемент пространства, что маскирует факт ошибки:

110001 = 100111 + 010110

001011 = 100111 + 101100

010110 = 011101 + 001011

**Задание 2.**

*(2.1)*

*Изображение выглядит как Шрифт, текст, зеленый, Графика

Автоматически созданное описание(2.2)*

*Изображение выглядит как текст, снимок экрана, Шрифт, логотип

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание(2.3)*

*(2.4)*

**1)**

4d c9 68 ff 0e e3 5c 20 95 72 d4 77 7b 72 15 87

d3 6f a7 b2 1b dc 56 b7 4a 3d c0 78 3e 7b 95 18

af bf a2[00]a8 28 4b f3 6e 8e 4b 55 b3 5f 42 75

93 d8 49 67 6d a0 d1[55]5d 83 60 fb 5f 07 fe a2

**2)**

4d c9 68 ff 0e e3 5c 20 95 72 d4 77 7b 72 15 87

d3 6f a7 b2 1b dc 56 b7 4a 3d c0 78 3e 7b 95 18

af bf a2[02]a8 28 4b f3 6e 8e 4b 55 b3 5f 42 75

93 d8 49 67 6d a0 d1[d5]5d 83 60 fb 5f 07 fe a2

**Результат**: 008ee33a9d58b51cfeb425b0959121c9

**Задание 3.**

Изображение выглядит как текст, снимок экрана, линия, Шрифт

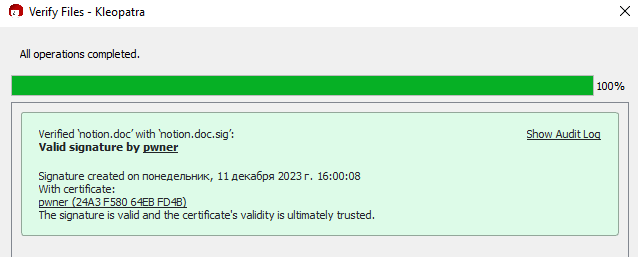
Автоматически созданное описаниеГенерация ключей:

Изображение выглядит как текст, Цвет электрик, снимок экрана, логотип

Автоматически созданное описаниеЭкспорт:

**Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание**Файл notion.doc:



Импортированная подпись:

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описаниеФайл одногруппника:

**Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание**