

Санкт-Петербургский государственный электротехнический  
университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 4

Изучение шифров DES и Магма

Студент:

Усачева Дарья, группа 1384

Руководитель:

Племянников А.К., доцент каф. ИБ

Санкт-Петербург, 2024

# Цель работы и задачи

**Цель:** Повысить свою компетенцию в области симметричных блочных шифров и в криптографии в целом.

## **Задачи:**

1. Изучить преобразования DES по шаблонной схеме DES Visualisation.
2. Провести исследование DES в режимах работы ECB и CBC.
3. Разработать схему в CcryptTool 2 для экспериментального определения всех версий 3-DES.
4. Изучить преобразования шифра Магма.
5. Провести исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением.

# Изучение преобразований DES

# Ручной расчет

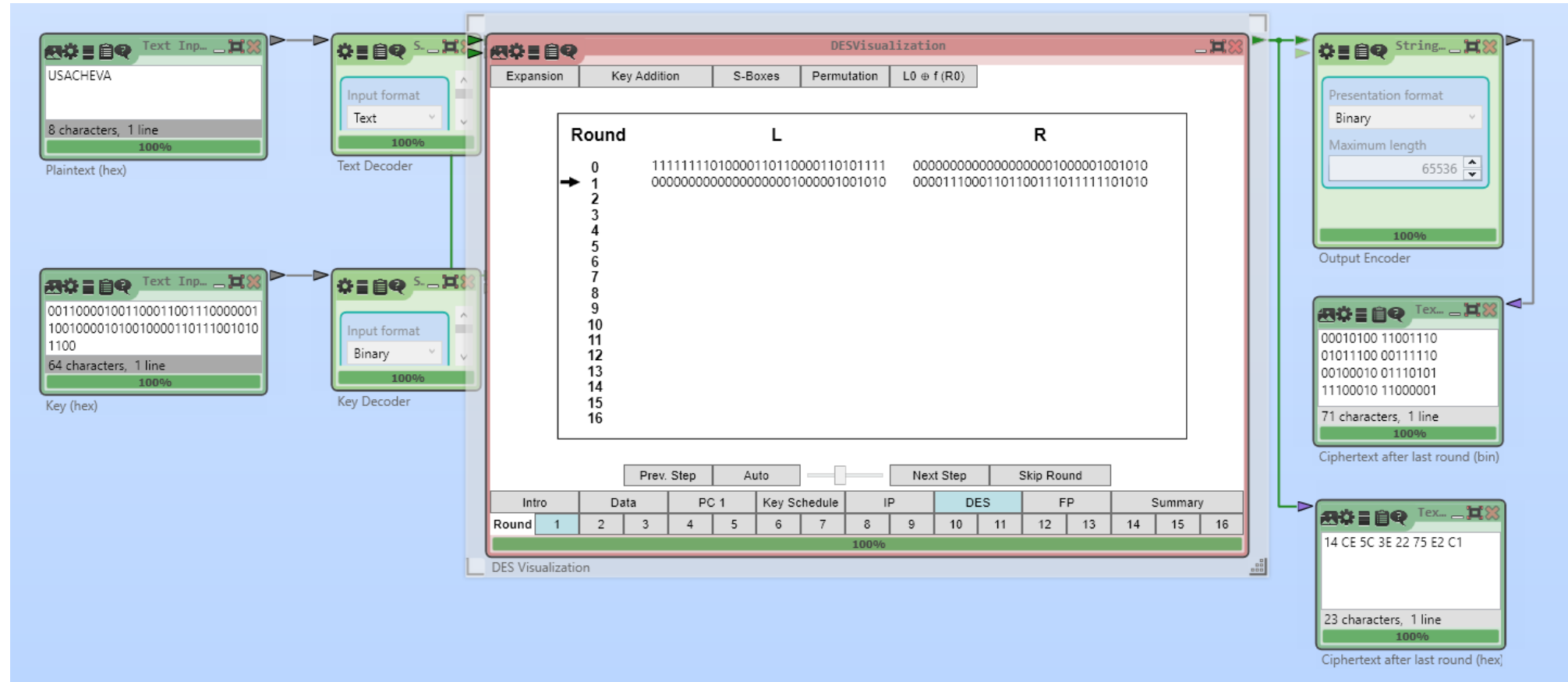
Открытый текст: USACHEVA

Ключ: 138427V (переведен в двоичную сс, в каждый 8 бит записан 0)

[illegible]

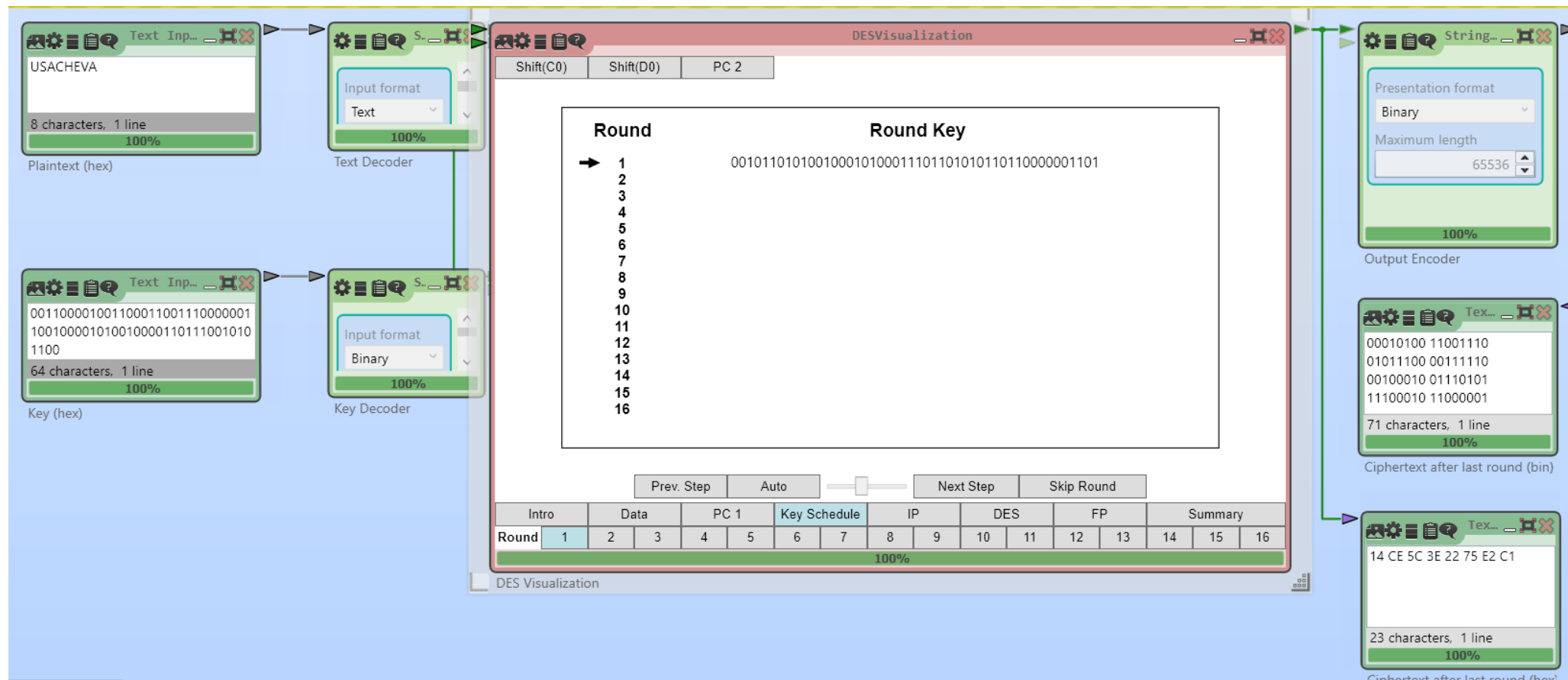
# Результат раунда 1

Результат раунда 1 совпадает с результатом раунда 1 ручного расчета.



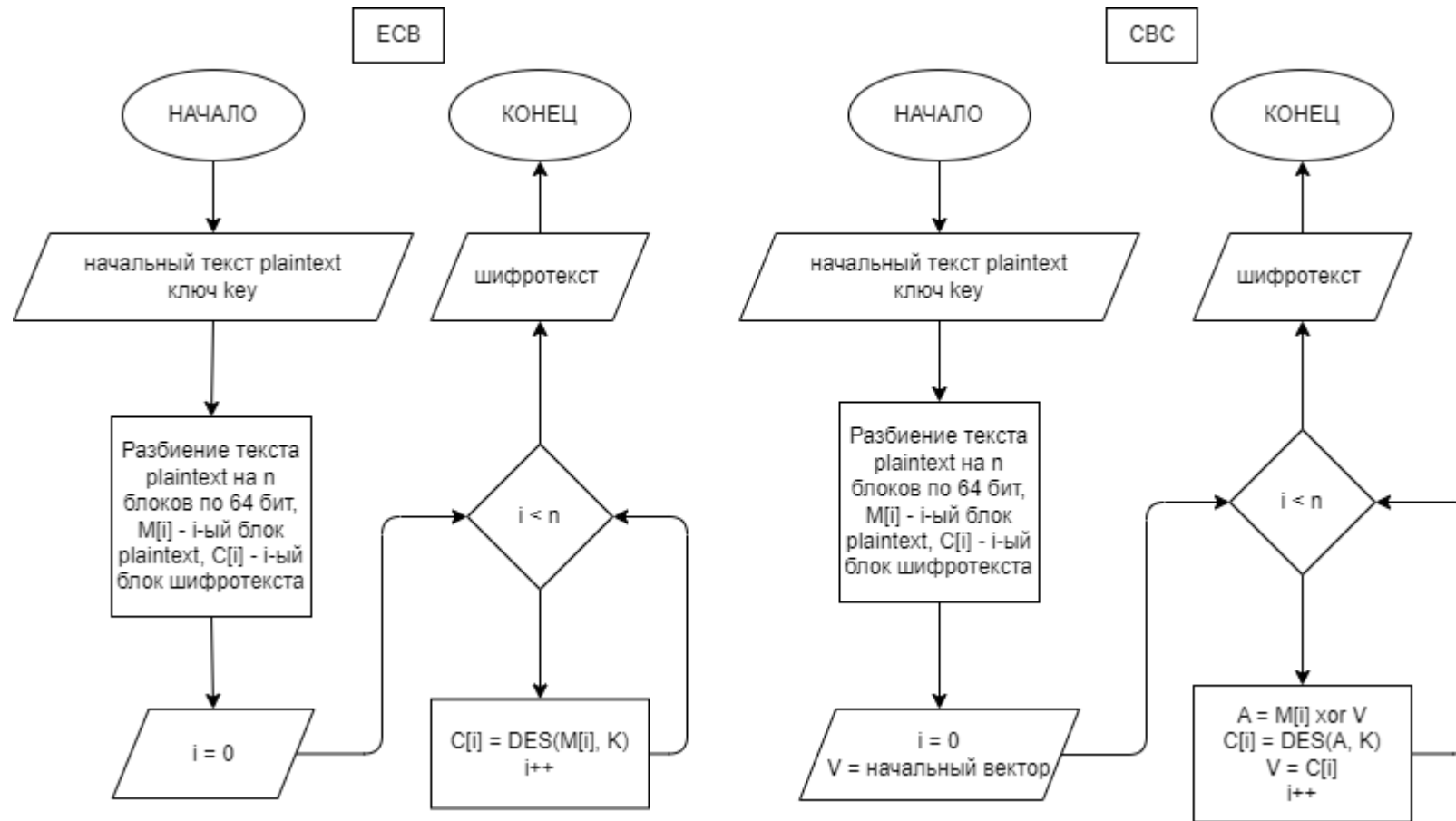
# Ключ раунда 1

Ключ раунда 1 совпадает с результатом ручного расчета ключа 1.



# **Исследование DES в режимах работы ECB и CBC**

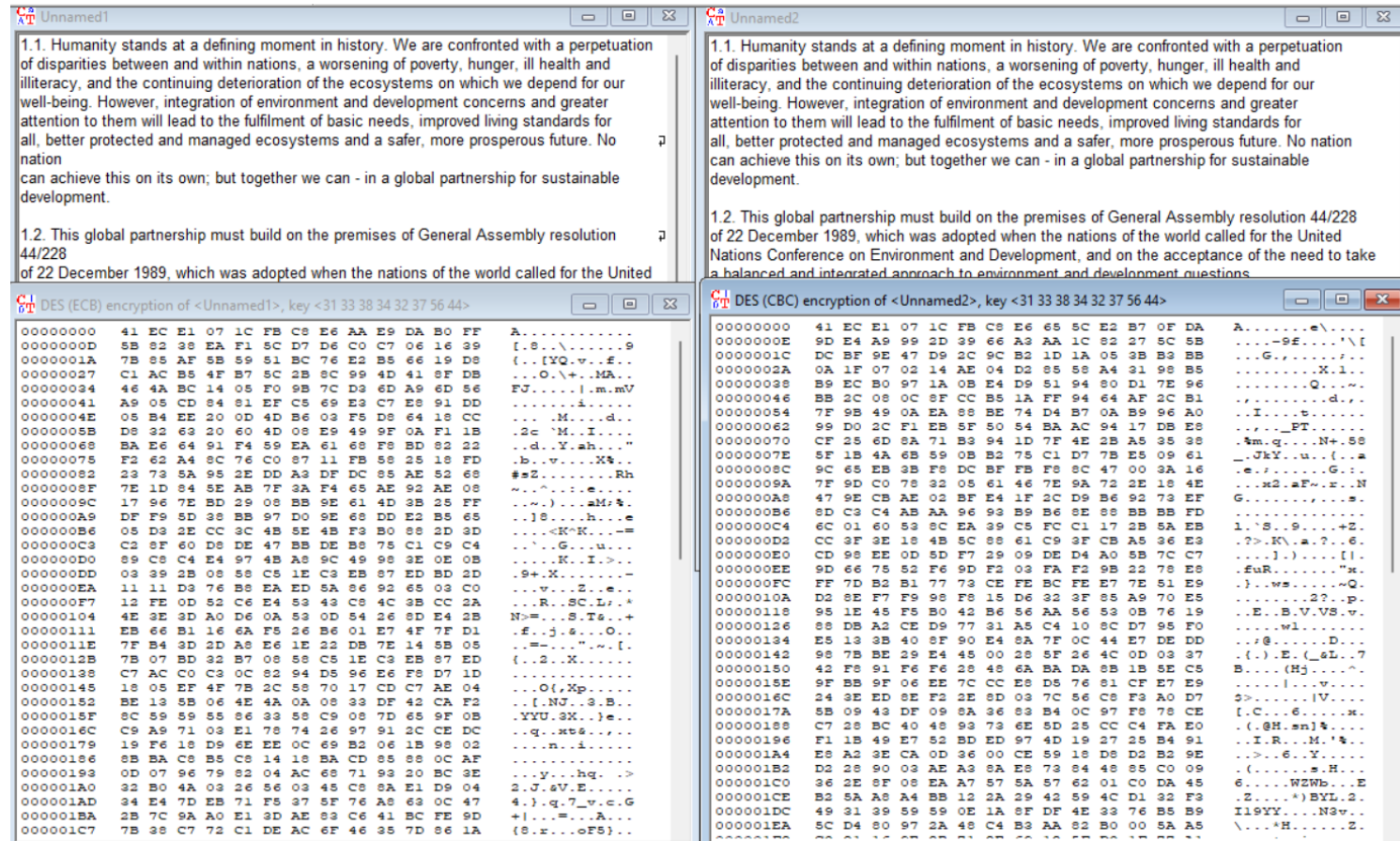
# Схемы алгоритмов работы DES в режимах ECB и CBC





# Результаты шифрования текста

Результаты шифрования текста на английском языке (не менее 1000 символов), полученные с помощью DES в режиме работы ECB и CBC. Ключ: 31 33 38 34 32 37 56 44



The image displays two side-by-side windows of a text editor, each showing the encryption of a sample text using DES. The left window is titled "DES (ECB) encryption of <Unnamed1>, key <31 33 38 34 32 37 56 44>" and the right window is titled "DES (CBC) encryption of <Unnamed2>, key <31 33 38 34 32 37 56 44>". Both windows show the original text and the resulting ciphertext in hexadecimal and ASCII.

Original text (visible in both windows):

1.1. Humanity stands at a defining moment in history. We are confronted with a perpetuation of disparities between and within nations, a worsening of poverty, hunger, ill health and illiteracy, and the continuing deterioration of the ecosystems on which we depend for our well-being. However, integration of environment and development concerns and greater attention to them will lead to the fulfilment of basic needs, improved living standards for all, better protected and managed ecosystems and a safer, more prosperous future. No nation can achieve this on its own; but together we can - in a global partnership for sustainable development.

1.2. This global partnership must build on the premises of General Assembly resolution 44/228 of 22 December 1989, which was adopted when the nations of the world called for the United Nations Conference on Environment and Development, and on the acceptance of the need to take a balanced and integrated approach to environment and development questions.

The left window shows the ECB encryption result, and the right window shows the CBC encryption result. The ciphertext is displayed in hexadecimal and ASCII format.

# Оценка времени атаки грубой силой

Была проведена оценка времени выполнения атаки грубой силой для шифротекста длины 1009

## ЕСВ

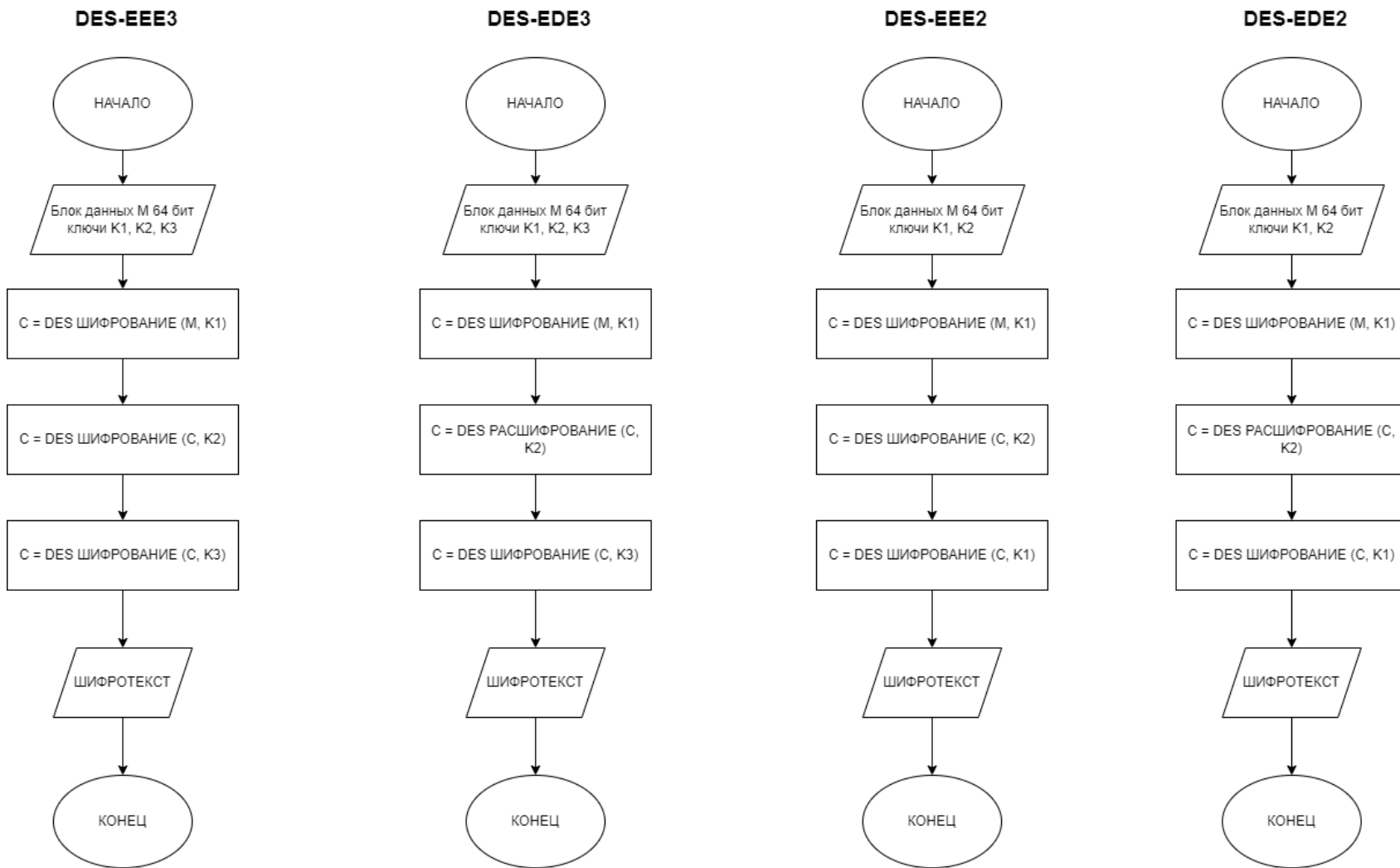
Кол-во известных байт ключа	Ожидаемое время выполнения
2	1.1 года
4	26 минут
6	<1 секунды

## СВС

Кол-во известных байт	Ожидаемое время выполнения
2	1.8 года
4	41 минут
6	<1 секунды

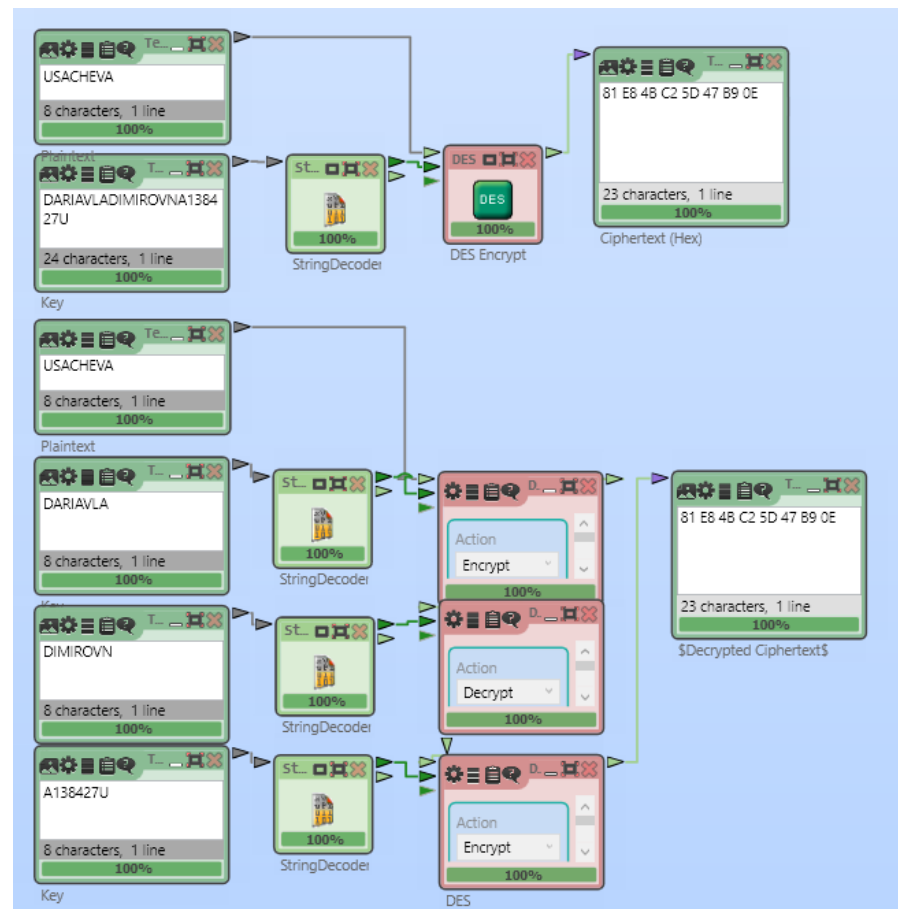
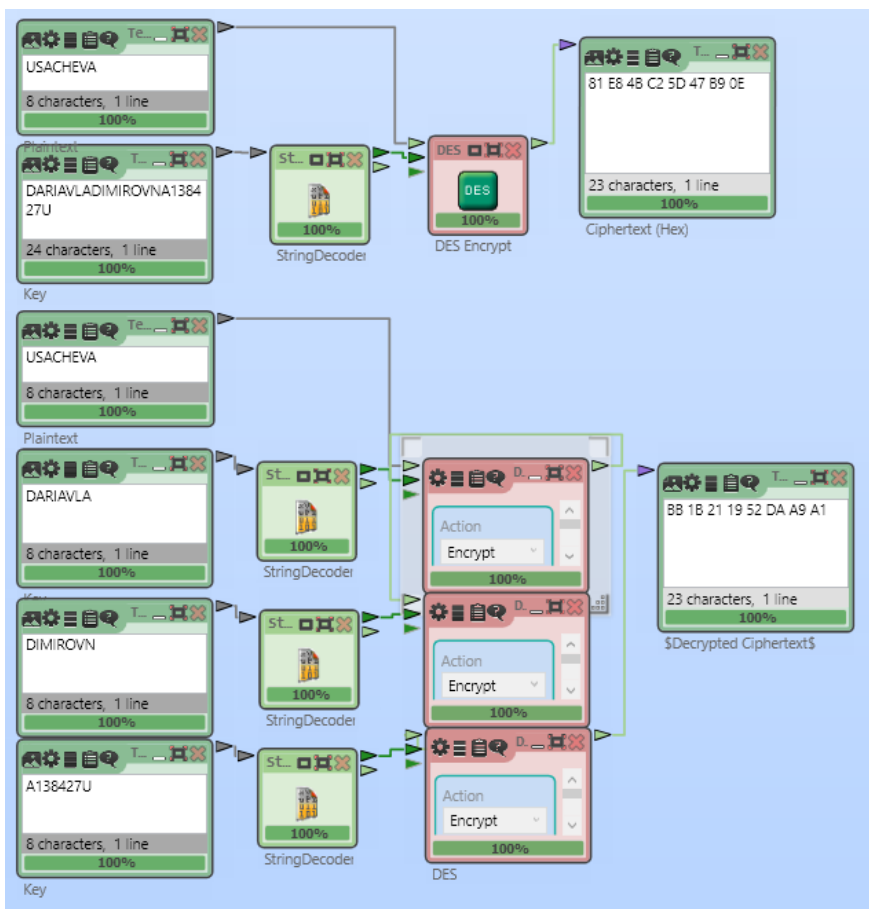
# **Разработка схемы в CrypTool 2 для экспериментального определения всех версий 3-DES**

# Схемы алгоритмов работы 3-DES в различных режимах



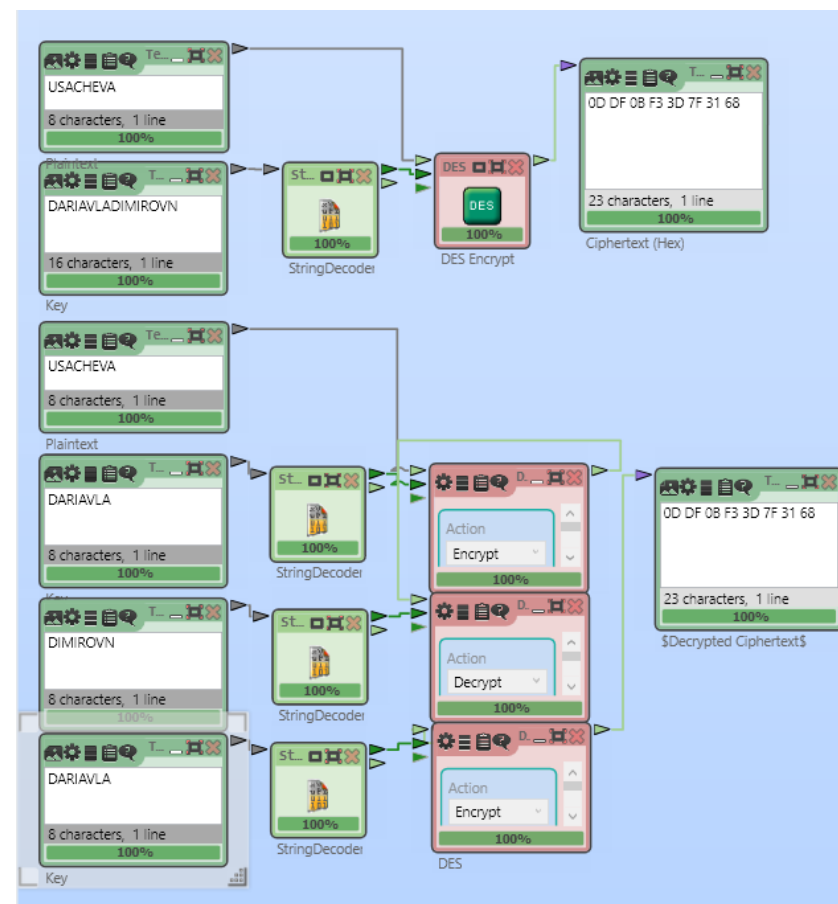
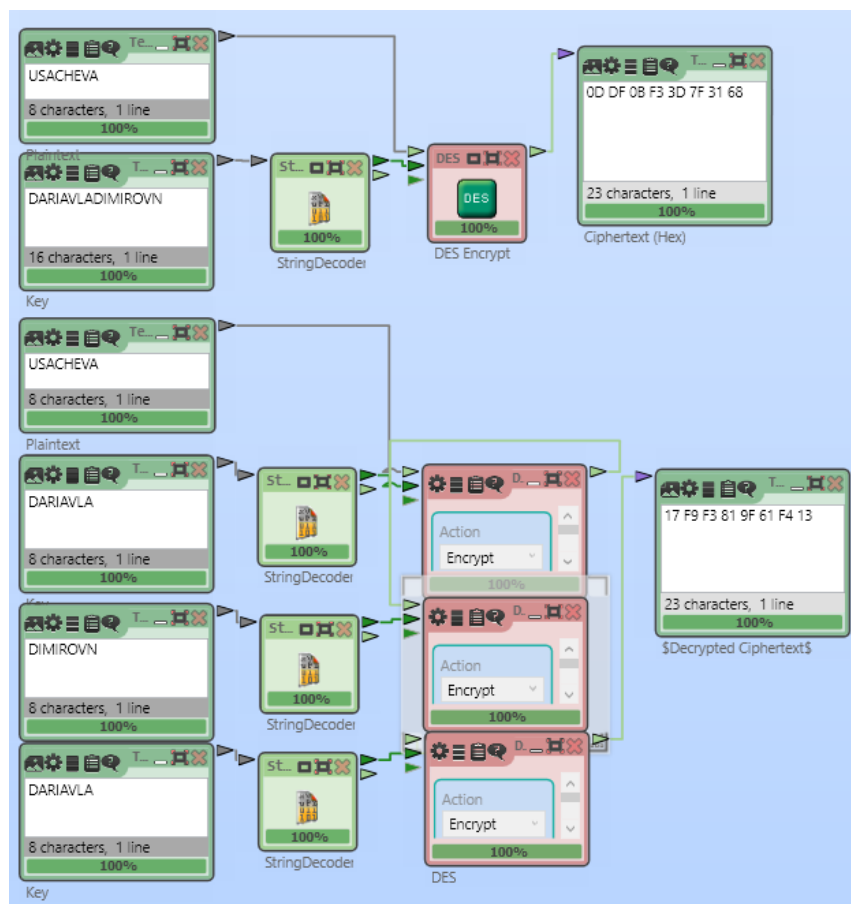
# Определение версий 3-DES, реализованных в Cryptool 2

Зашифруем текст алгоритмом 3-DES и вручную в режимах EEE3 и EDE3. Как видим, результаты шифрования совпали для EDE3, что означает, что Cryptool 2 использует его.



# Определение версий 3-DES, реализованных в Cryptool 2

Зашифруем текст алгоритмом 3-DES и вручную в режимах EEE2 и EDE2. Как видим, результаты шифрования совпали для EDE2, что означает, что Cryptool 2 использует его.



# **Изучение преобразований шифра Магма**

# Ручной расчет

## Открытый текст: USACHEVA

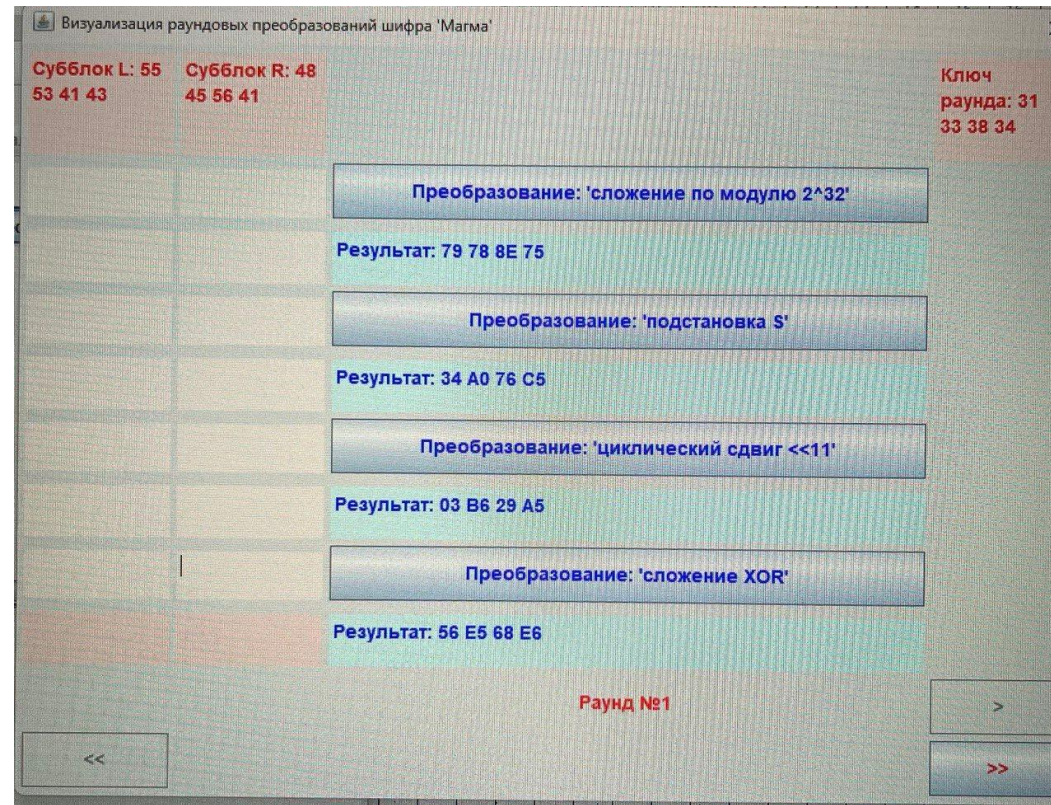
Ключ: 138427DARIAVLADIMIRONVA23102002K

[illegible]



# Результат раунда 1

Результат выполнения раунда 1 совпадает с результатом раунда 1 ручного расчета.

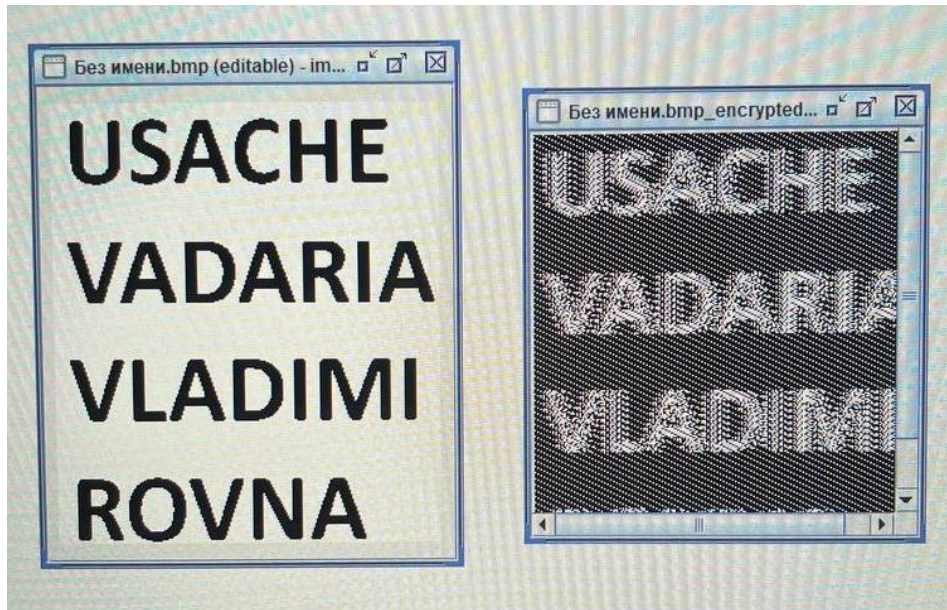


**Исследование шифра Магма в  
режимах работы простой замены  
и простой замены с зацеплением**

# Результаты шифровки

Была создана картинка в формате bmp и зашифрована с помощью шифра Магма в режиме простой замены(ЕСВ) и в режиме простой замены с зацеплением(СВС). Как можно заметить, изображение, полученное с помощью режима СВС, менее читаемо.

ЕСВ



СВС





# Заключение

1. Изучены преобразования DES по шаблонной схеме DES Visualisation.

Выполнено ручное преобразование первого раунда и рассчитан раундовый ключ. Результаты программных и ручных вычислений совпали.

2. Проведены исследования DES в режимах работы ECB и CBC.

Выполнено сравнение скорости дешифрования в различных режимах работы. CBC продемонстрировал большую устойчивость по сравнению с режимом ECB. Установлено, что режим ECB, благодаря параллельности вычислений, работает быстрее, чем режим CBC.

3. Разработана схема в CrypTool 2 для экспериментального определения всех версий 3-DES.

Выяснено, что CrypTool 2 реализует шифр 3-DES по схеме EDE3 и EDE2.

4. Изучены преобразования шифра Магма.

Выполнено ручное преобразование первого раунда. Результаты программных и ручных вычислений совпали.

5. Проведено исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением.

Режим простой замены продемонстрировал, что одинаковые блоки исходных данных шифруются в одинаковые блоки, что сохраняет структуру данных и может облегчить сжатие, но при этом снижает безопасность. В режиме замены с зацеплением данные преобразуются в псевдослучайный шум, что значительно повышает их стойкость к анализу, однако делает сжатие практически невозможным.