**ОТЧЁТ**

**ПО КРИПТОГРАФИИ**

**«Алгоритм шифрования RDES»**

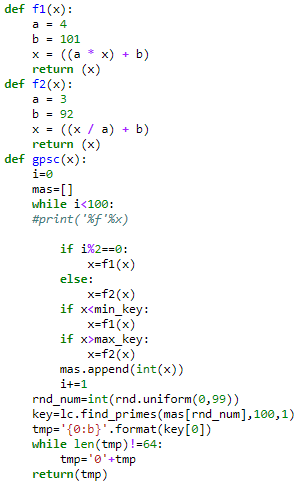
Выполнил студент группы 448

Гусев Ю.С.

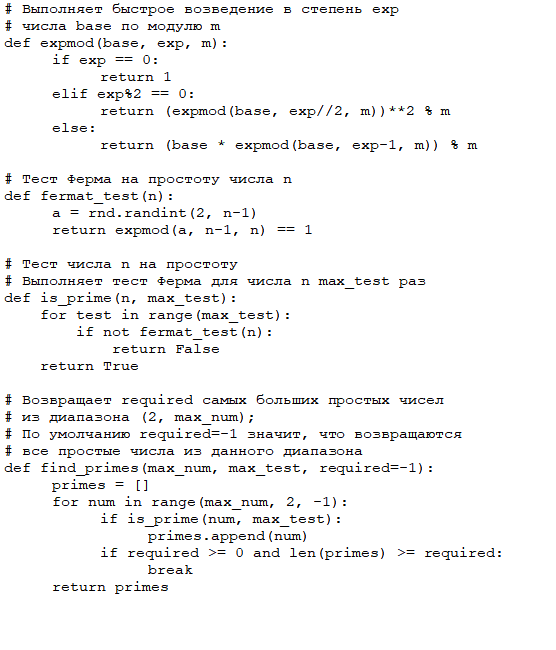
Нижний Новгород

16.12.2018

**Генератор случайных чисел**



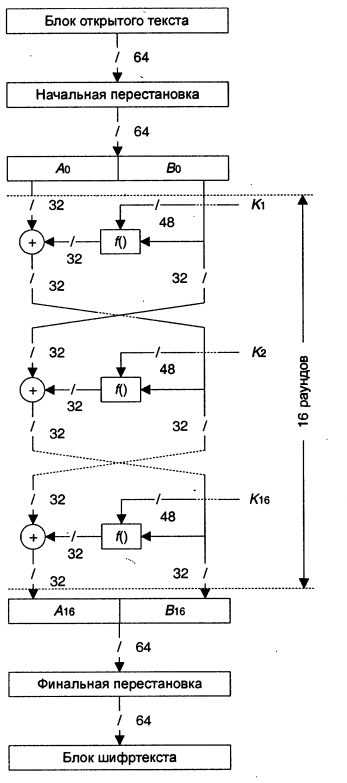
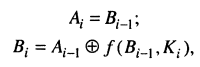
Функция получает на вход число и выдает последовательность псевдослучайных чисел, из которой потом случайным образом выбирается одно из чисел. Затем выбирается ближайшее к нему простое число по следующему алгоритму:



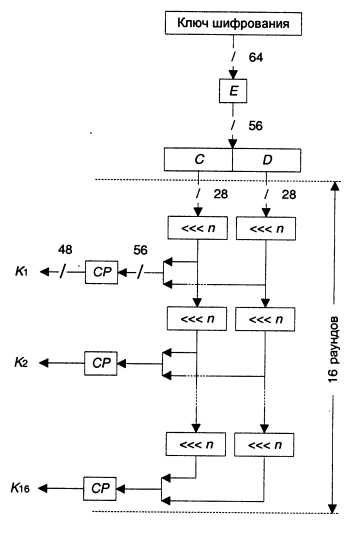
Тест Ферма на простоту числа проводится 100 раз, для достижения оптимальной точности определения простоты числа.

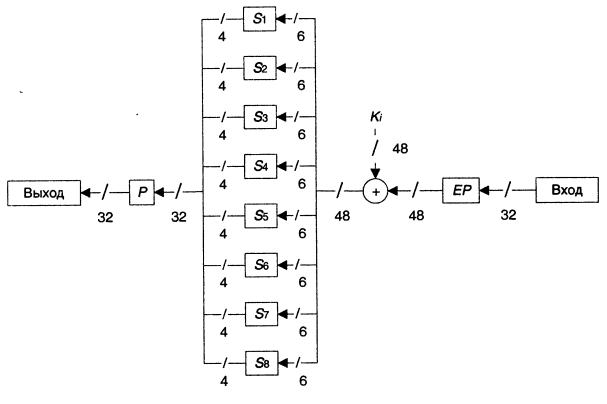
**Алгоритм RDES**

Структура алгоритма DES представлена на рисунке ниже (1). Входной текст разбивается на 64-битные блоки, к которым применяется алгоритм.

Начальная перестановка выполняется с использование таблицы перестановки 1. (все таблицы перестановки указаны в приложении). Далее выполняются 16 раундов преобразований, которые можно описать формулой 

После применяется финальная перестановка и на выходе получается зашифрованный текст. Структура функции f() представлена на рисунке ниже (2). Перестановки EP,S и P в приложении. Так как ключ изначально один, а раундов 16, то применяется процедура расширения ключа (3).





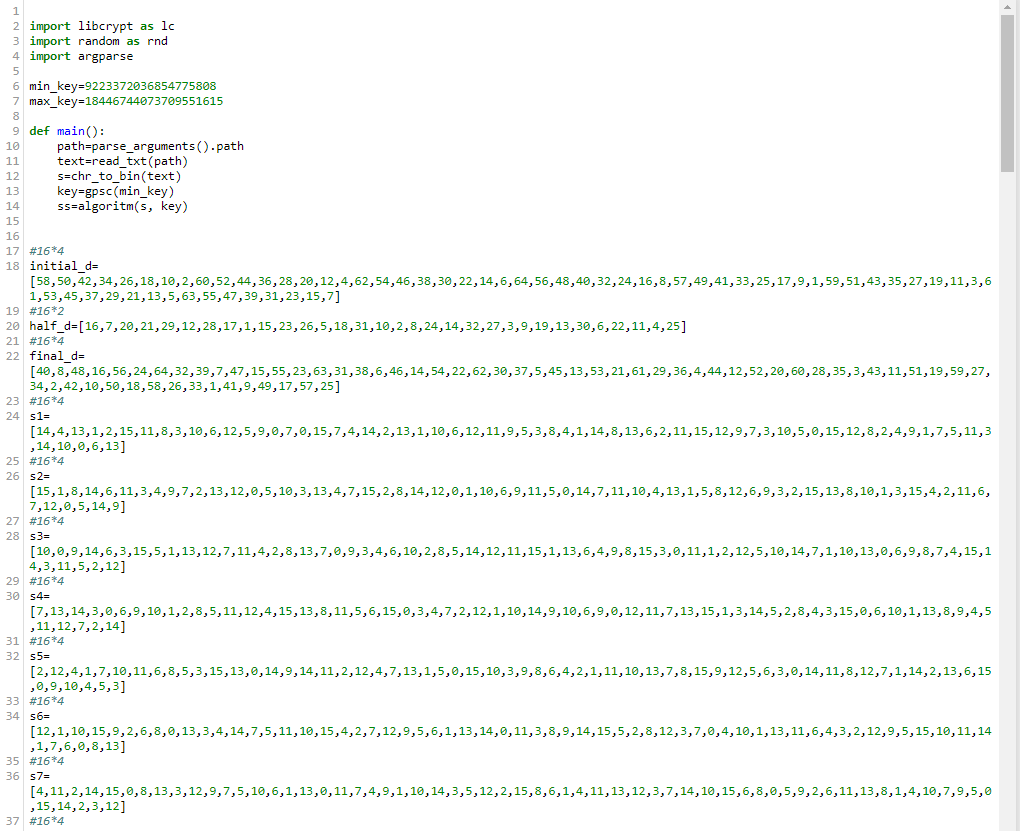
Дешифрование происходит путем применения алгоритма шифрования к шифрованному тексту, но с использованием ключей раундов в обратном порядке.

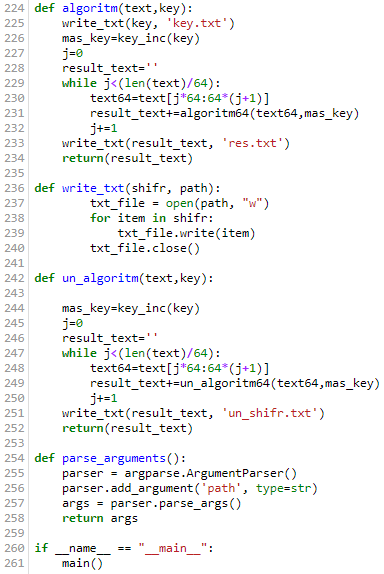
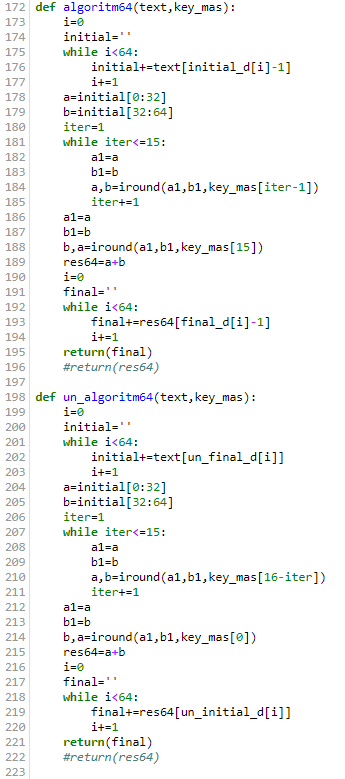
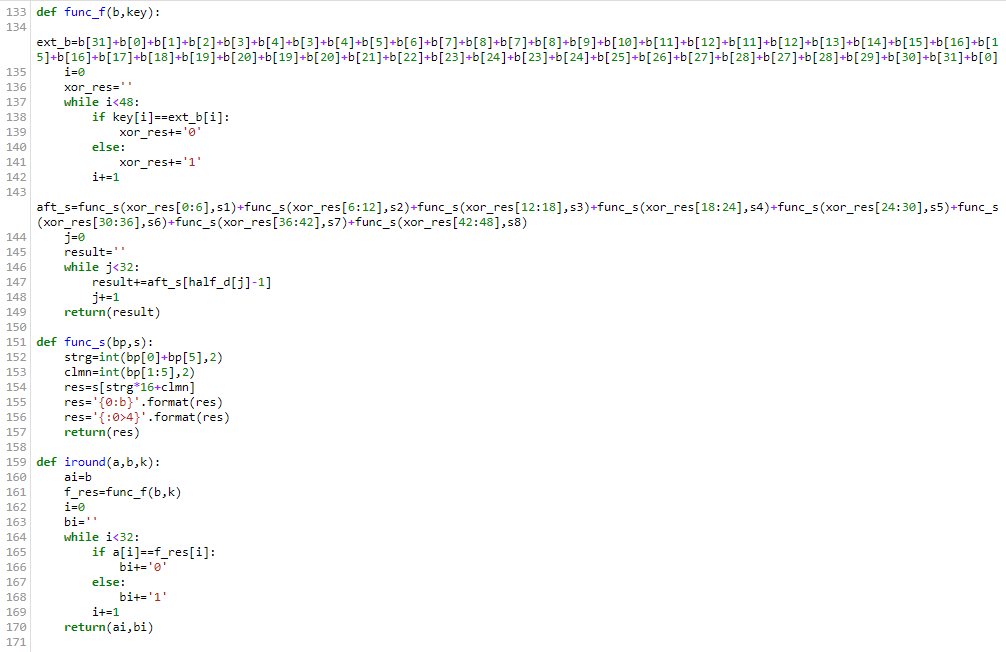
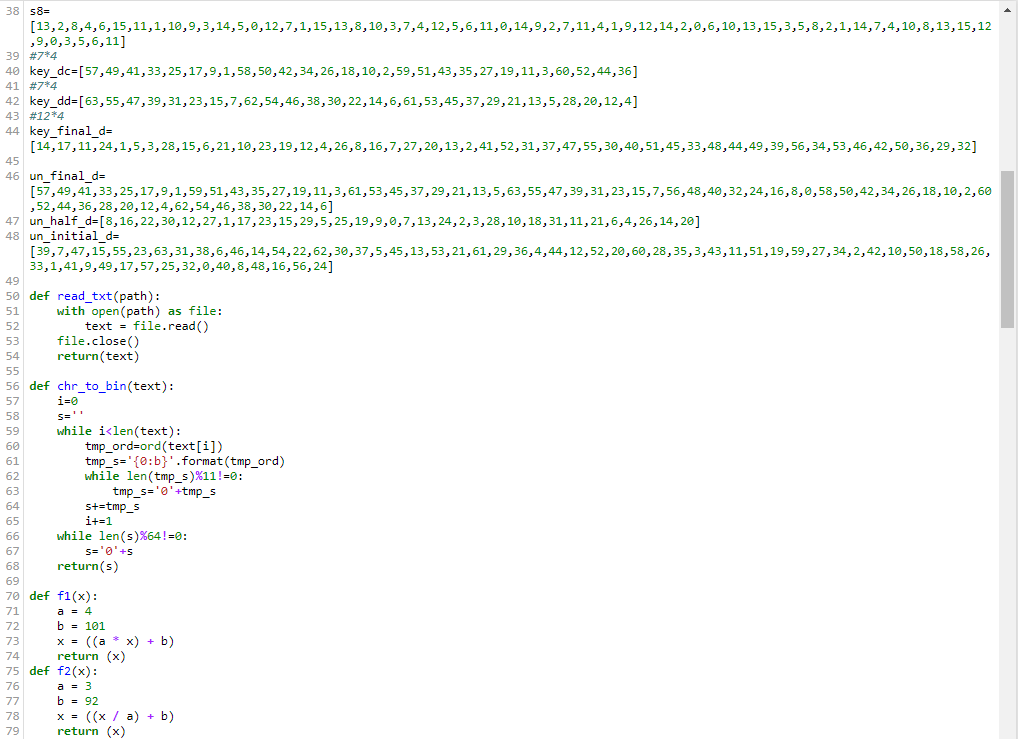
Randomize DES отличается от обычного DES тем, что вносятся элементы случайности в перестановку блоков текста во время раундов преобразования в зависимости от значений битов ключа. Например, в моем случае перестановка блоков происходит в том случае, если первый бит текущего ключа имеет значение единицы.

Данный алгоритм работает с 64-битным ключом.

**Текст программы.**

Шифратор





Дешифратор:



На вход программе подается текст:

«Я, Гусев Юрий Сергеевич, дата рождения 03.04.1997, место рождения г. Нижний Новгород, страна РФ, проживающий по адресу: город Нижний Новгород, ул. Мончегорская, д. 16а/3. Сдаю зачет по криптографии.»

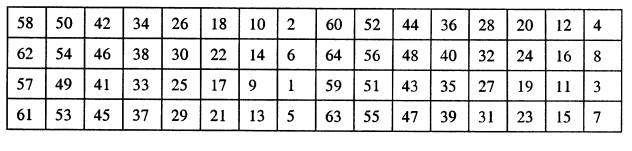
Результатом работы шифратора являются файл с зашифрованным текстом в двоичном виде и файл с ключом в двоичном представлении.

Дешифратор принимает на вход файл с зашифрованным текстом, а файл с ключом ему заранее известен. После выполнения он создает файл с расшифрованным текстом.

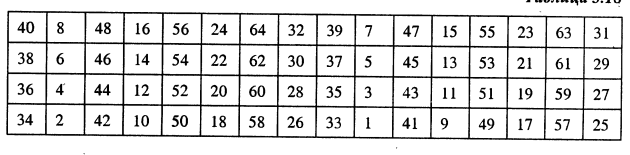
**Вывод:** мною была изучена литература с описанием алгоритма шифрования DES и его модификаций, был разработан алгоритм, реализующий успешное шифрование и настолько же успешное дешифрование.

**Приложение.**

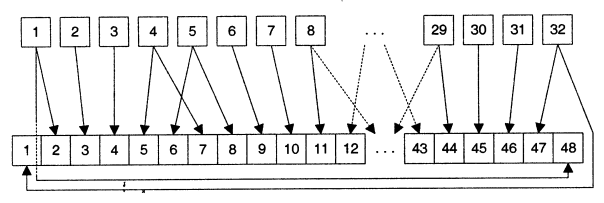
Начальная перестановка



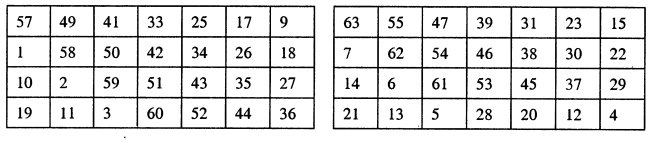
Финальная перестановка:



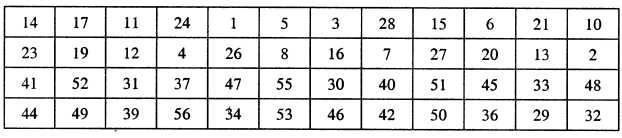
Расширяющая перестановка EP:



Перестановки С и D для ключа:



Сжимающая перестановка:



Перестановки S для ключей:

