БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

ОТЧЕТ ПО КРИПТОГРАФИЧЕСКИМ МЕТОДАМ

студента 2 курса 13 группы

Лабораторная работа №3

Вариант 11

Преподаватель

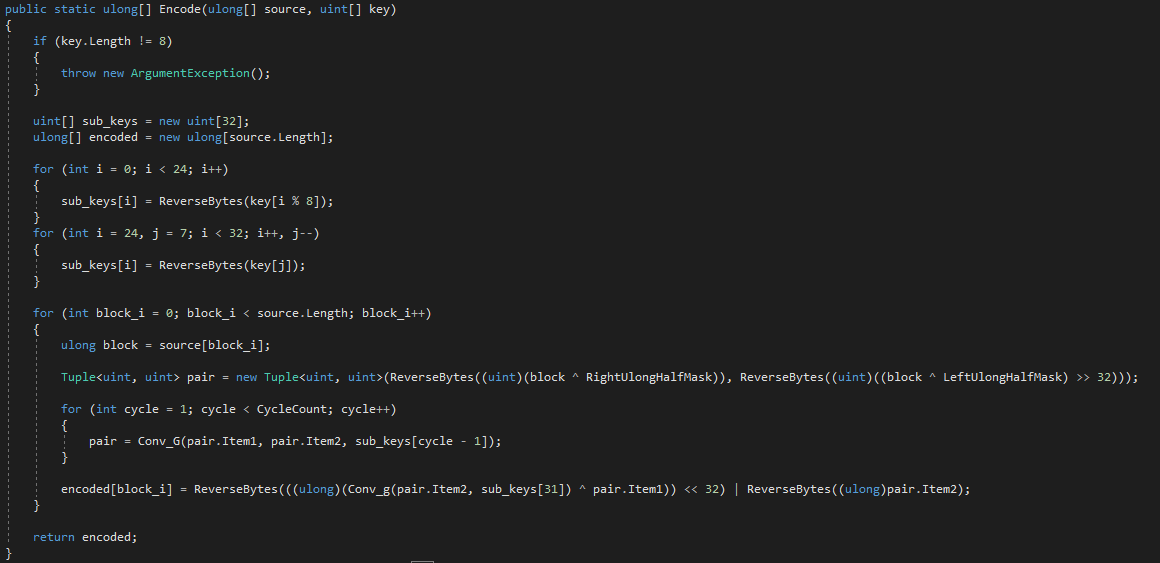
Ярошеня Ю.С.

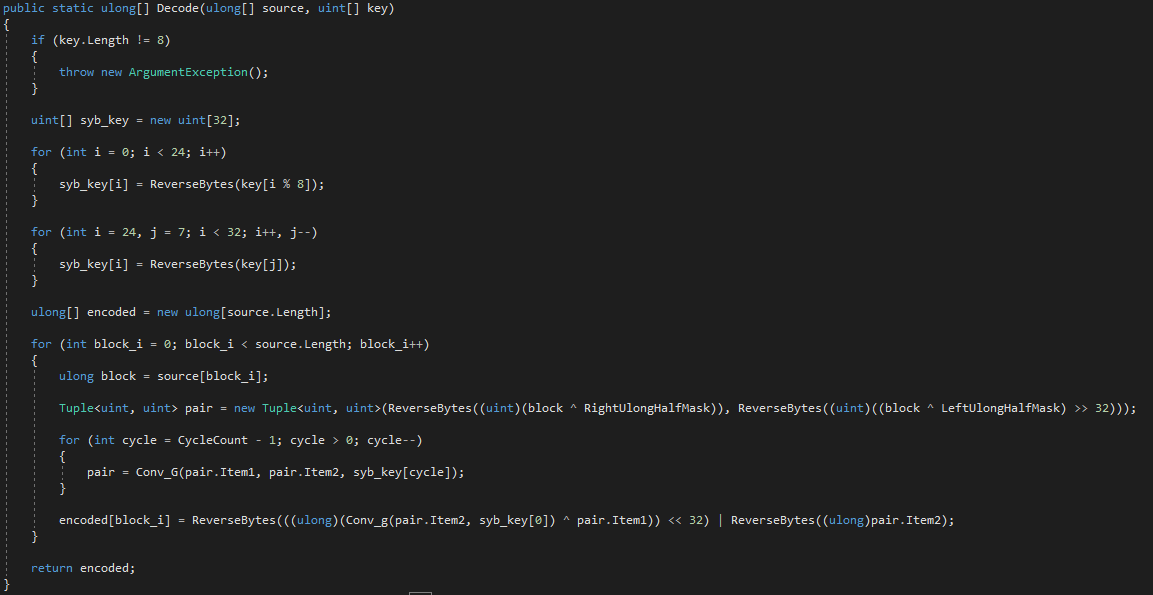
Минск 2020

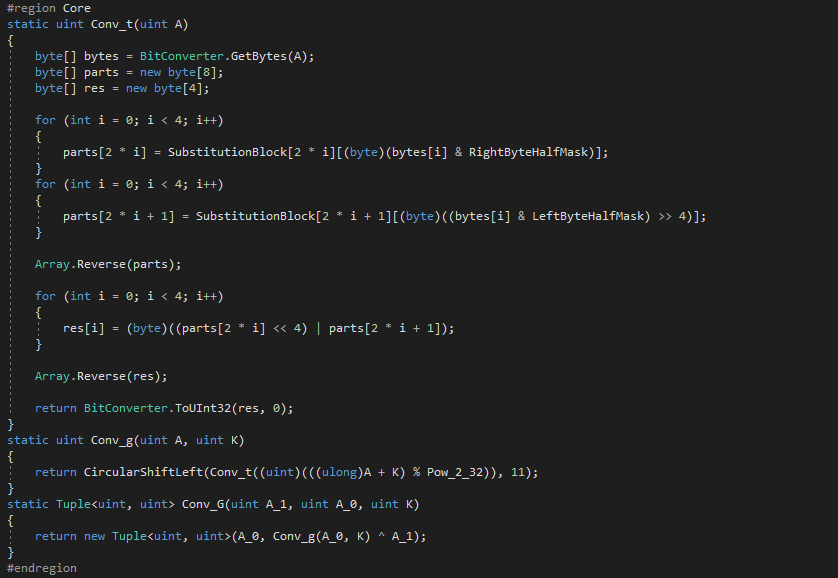
Криптосистема

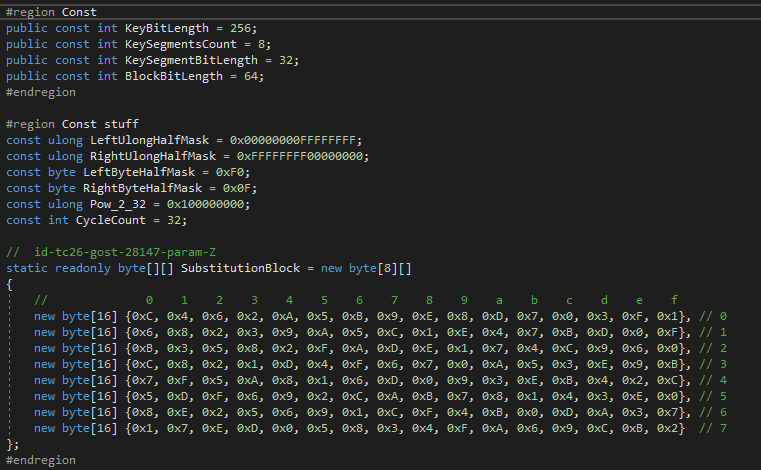
У меня была система ГОСТ 28147-89, я реализовал её современный вариант “Магма”.

Реализация:





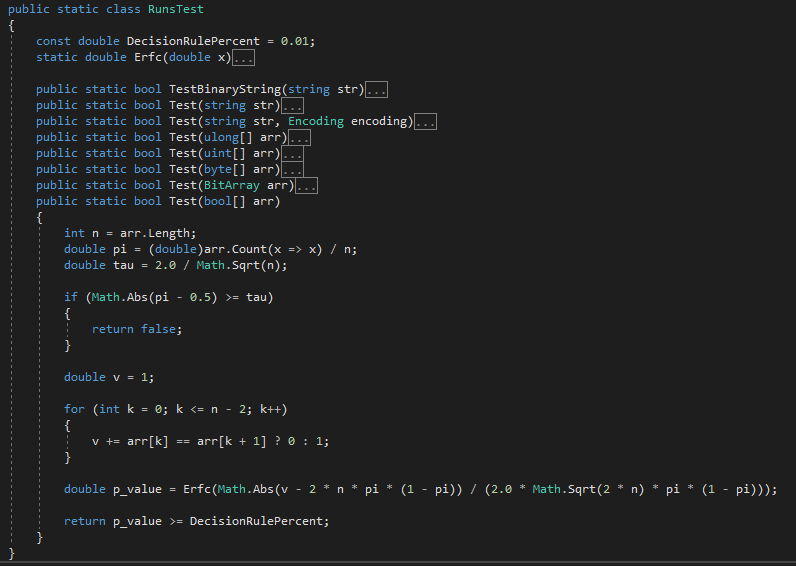




Тест

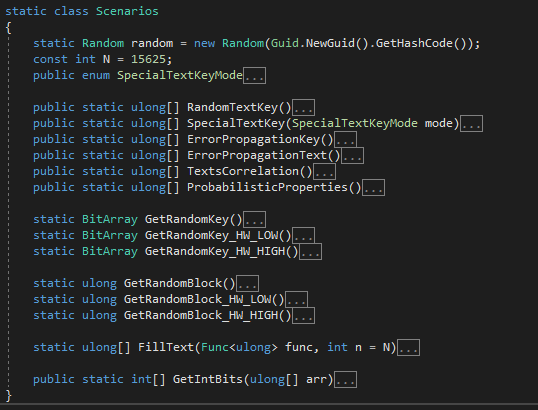
У меня был Runs test

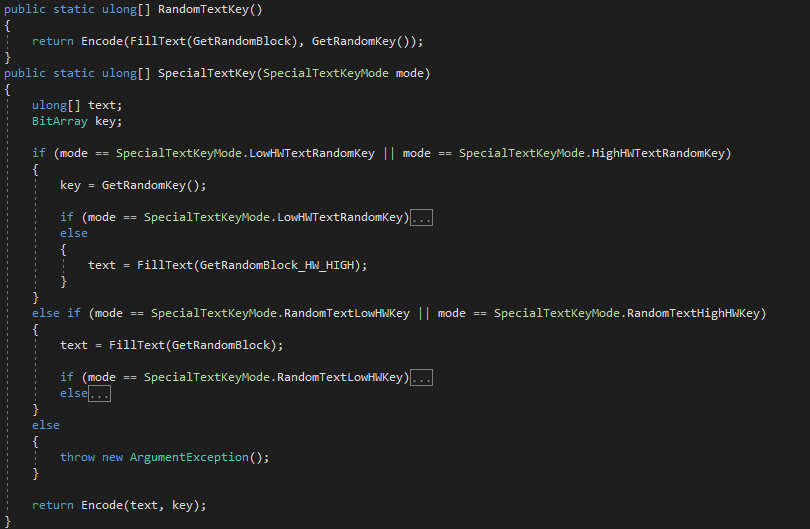
Реализация:

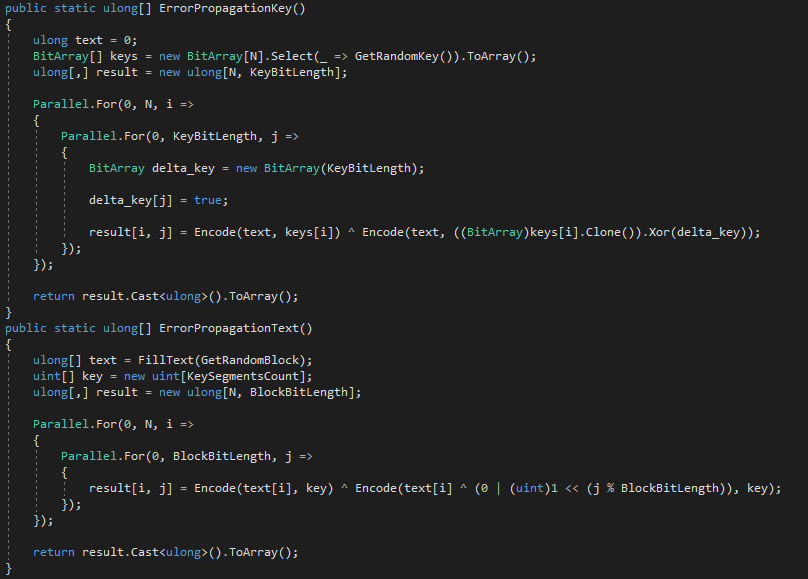


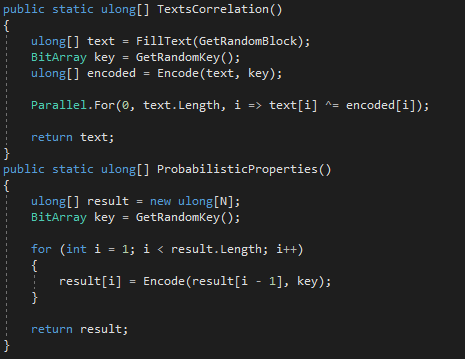
Сценарии

Реализация:



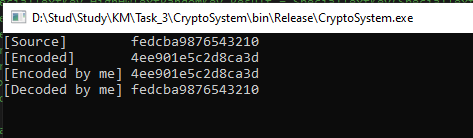




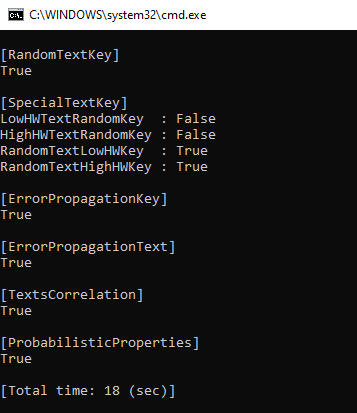


Тестирование

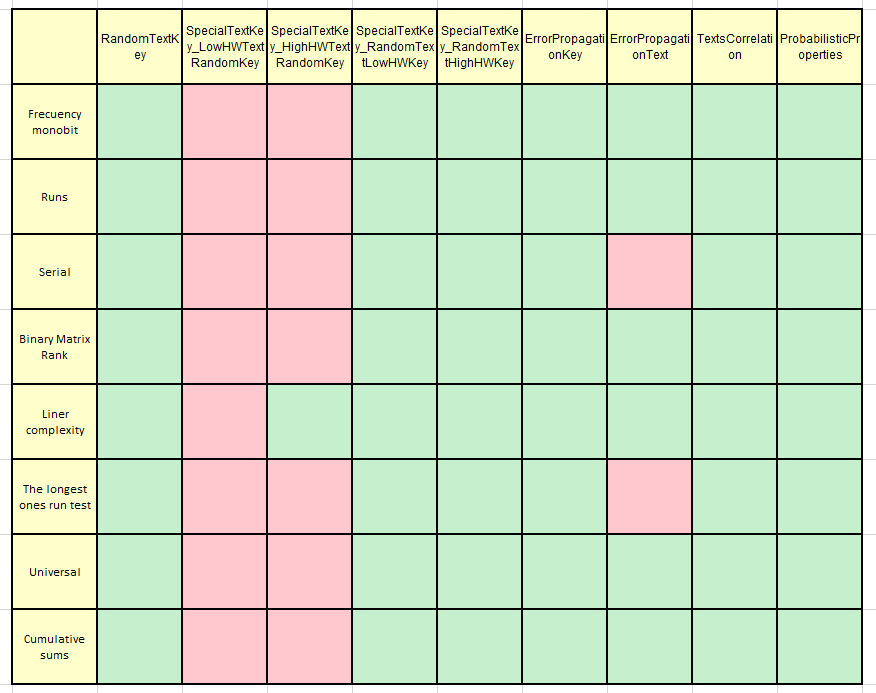
Проверка работоспособности шифра:



Проверка сценариев моим тестом:



Прогон сценариев по всем тестам:



Можно заметить, что сценарии со специальным выбором текста (малый/большой вес Хэмминга) в результате не проходят большинство тестов. Это может говорить о том что шифр довольно плохо отображает последовательности одинаковых бит на последовательность равномерно-распределенных бит.