**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Ястребова Вероника**

**СТБ 34.101.31-2007**Отчет по лабораторной работе №3

(«Криптография»)

студентки 2 курса 13 группы

**Преподаватель**

**Ярошеня Ю.В**

**Минск 2018**

Оглавление

[Общие сведения 2](#_Toc515565365)

[Шифрование 2](#_Toc515565366)

[Программа 4](#_Toc515565367)

[Тестирование 5](#_Toc515565368)

[Вывод 6](#_Toc515565369)

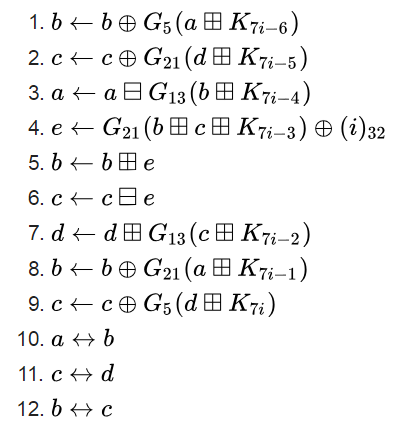
Общие сведения  
BelT — государственный [стандарт](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) [симметричного](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и контроля целостности Республики Беларусь. Полное название стандарта — СТБ 34.101.31-2007 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности». Принят в качестве предварительного стандарта в 2007 году. Введен в действие в качестве окончательного стандарта в 2011 году.

|  |  |  |  |
| --- | --- | --- | --- |
| Размер ключа | Размер блока | Число раундов | Тип |
| 256 бит | 128 бит | 8 | комбинация сети Фейстеля и подстановки Лэя-Мэсси |

# Шифрование

Входные данные для шифрования подготавливаются следующим образом:

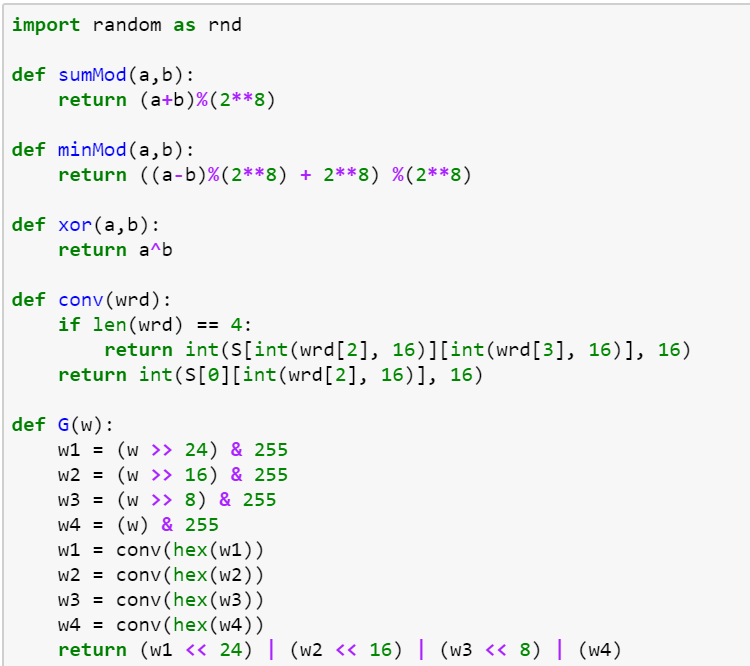
* Входное 128-битное слово записывается в виде Х=Х1||X2||X3||X4, Xi – 32-битное слово.
* Ключ записывается в виде 
* Для зашифрования слова {\displaystyle X}Х на ключе {\displaystyle \theta } необходимо выполнить следующие шаги:

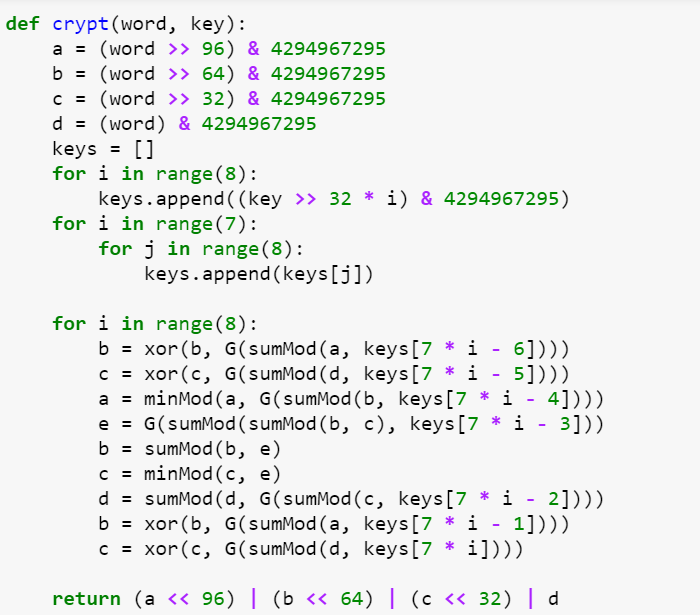
1. Установить в дополнительные переменные 
2. для i от 1 до 8 выполнить: 
3. Установить Y = b||d||a||c
4. Возвратить Y

Переменные a, b, c, d, e — 32-битные слова. Преобразование  ставит в соответствие 32-битному слову u = u1||u2||u3||u4 (ui – 8-битное слово) 32-битное слово.

Подстановка {\displaystyle H:{\{0,1\}}^{8}\rightarrow {\{0,1\}}^{8}}H : {0,1}8 -> {0,1}8 задается фиксированной таблицей (S — блок).

# Программа





# Тестирование

Цель теста : определить, является ли последовательность случайной на самом деле.

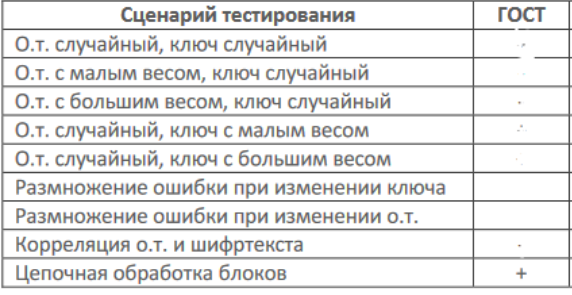
На вход в тест поступает размер блока и шифр-текст.

На выходе – число(**p-value)**

Если **p-value** < 0.01, то тест не пройден, последовательность не является случайной.

* случайный ключ, случайный текст : p-value = 0.27633928292912
* случайный ключ, сильный текст, нулей 3 : 0.41223
* случайный ключ, слабый текст, 0 единиц : 0 случайный ключ, слабый текст, 1 единица : 3.892e-123
* корреляция открытого текста и шифр-текста - 0.13471

# Вывод



На основании проведенного тестирования с использованием 4 сценариев генерирования шифртекстов можно сделать вывод, что криптосистема СТБ 34.101.31-2007 неустойчива в случае атак с открытым текстом с очень малым весом Хэмминга и случайном ключе.