**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Наумов Даниил Дмитриевич**

**Cast 128**Отчет по лабораторной работе №3

(«Криптография»)

студента 2 курса 13 группы

**Преподаватель**

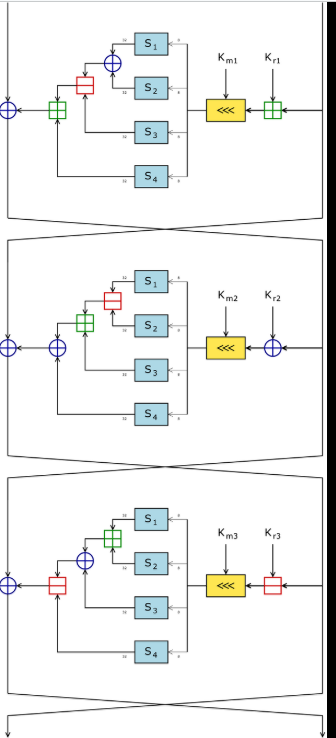
**Ярошеня Ю.В**

**Минск 2018**

Общие сведения  
CAST-128 (или CAST5) в [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) — блочный алгоритм симметричного шифрования на основе [сети Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F), который используется в целом ряде продуктов криптографической защиты, в частности некоторых версиях [PGP](https://ru.wikipedia.org/wiki/PGP) и [GPG](https://ru.wikipedia.org/wiki/GPG) и кроме того одобрен для использования Канадским правительством.

|  |  |  |  |
| --- | --- | --- | --- |
| Размер ключа | Размер блока | Число раундов | Тип |
| 40-128 бит | 64 бит | 12 | сеть Фейстеля |

# Шифрование



# 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.