**Лабораторная работа 1**

Выполнить статистический анализ свободных русскоязычного и англоязычного текстов (по вариантам):

* организованного текста
* сжатого файла
* соответствующих шифртекстов, созданных одной из программ симметричного шифрования.

Произвести сравнительный анализ статистик. Для экспресс-анализа использовать посимвольные гистограммы, автокорреляционную функцию, статистические тесты.

**Лабораторная работа 2**

Реализовать симметричный криптоалгоритм на основе простого гаммирования. Гаммирование осуществлять на основе алгоритма Макларена-Марсальи на основе двух конгруентных датчиков. Конгруэнтные ДСЧ создать на основе рекомендаций в книге Дональда Кнута и встроенного ГСЧ. Предоставить возможность сохранения гаммы в отдельный файл. Провести экспресс-анализ.

**Лабораторная работа 3**

Разработать программу генерации симметричных ключей с помощью алгоритма Диффи-Хеллмана для расчётов применять алгоритм ускоренного возведения в степень.

**Лабораторная работа 4**

Разработать программу шифрования и дешифрования основанную на асимметричном алгоритме RSA. Разработанную программу для стандартных типов данных (unsigned \_\_int64) расширить для целых чисел произвольной длины.

**Лабораторная работа 5**

Разработать программу для вычисления циклических избыточных кодов. Для всех многочленов от 0x00000000 до 0xffffffff вычислить 8-битовый остаток от деления на заданный в варианте 9-разрядный делитель (порождающий многочлен). Построить гистограмму распределения остатков. Модернизировать программу для определения пригодности многочлена-делителя для вычисления CRC, на основании повторяемости остатков при расстоянии между многочленами-делимыми в 1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | P | № | P | № | P | № | P | № | P |
| 1 | 341 | 8 | 346 | 15 | 295 | 22 | 378 | 29 | 398 |
| 2 | 384 | 9 | 467 | 16 | 261 | 23 | 426 | 30 | 320 |
| 3 | 259 | 10 | 430 | 17 | 462 | 24 | 339 |  |  |
| 4 | 337 | 11 | 469 | 18 | 310 | 25 | 416 |  |  |
| 5 | 367 | 12 | 410 | 19 | 257 | 26 | 424 |  |  |
| 6 | 489 | 13 | 503 | 20 | 367 | 27 | 348 |  |  |
| 7 | 502 | 14 | 362 | 21 | 403 | 28 | 359 |  |  |

**Лабораторная работа 6**

Реализуйте один из трёх алгоритмов криптографического хеширования (0 - sha1, 1 - md5, 2 - ГОСТ Р 34.11-94) в зависимости от остатка при делении номера варианта в поле GF(3).

**Лабораторная работа 7**

Разработайте приложение которое разбивает файл из первой лабораторной работы на блоки длинной 1000 байт, затем в первом блоке M требуется рассчитать хеш основываясь на реализацию созданную в предыдущей работе.

Подберите такое значение Nonce, что бы hash(M + Nonce) начинался с 0 (старший бит). Учитывайте, что length(M + Nonce + hash(M + Nonce))=1024. Оцените время работы вашего приложения.

**Домашняя работа**

Разработать и описать в виде SDP новую или модернизируемую ИТ-услугу. По возможности требуется описать SLA.