**Отчёт по лабораторной работе №1**

**1. Общее описание алгоритма**

Алгоритм **«Магма»** (ранее известный как ГОСТ 28147-89) — блочный симметричный алгоритм шифрования, предназначенный для защиты информации в соответствии с российскими криптографическими стандартами.

* **Длина блока:** 64 бита (8 байт)
* **Длина ключа:** 256 бит (32 байта), разбит на 8 32-битных подключей
* **Количество раундов:** 32 раунда. Первые 31 с итеративным использованием ключей; 32-й — финальный раунд
* Режим OFB (Output Feedback) представляет собой один из стандартных режимов работы блочных шифров, в котором блочный алгоритм преобразуется в потоковый. Это достигается путём итеративного применения шифра к вектору инициализации (IV) и использованию полученного результата как псевдослучайного потока, с которым затем осуществляется операция XOR по открытому тексту.

**2. Криптографические свойства и стойкость**

* **Тип конструкции:** Фейстел-сеть
* **S-блоки:** 8 статичных таблиц подстановок (SBOX), определённых государственным стандартом
* **Циклический сдвиг:** на 11 бит после каждой S-блочной подстановки
* **Стойкость к линейному и дифференциальному криптоанализу:** обеспечивается за счёт нелинейных преобразований (S-блоков) и фейстель-структуры
* **Максимальная стойкость против полного перебора:**  
  22562^{256}2256 операций для полного перебора ключа — соответствует современному требованию КС3

Не смотря на возраст алгоритма, **Магма** остаётся устойчивым при условии использования безопасных ключей и корректных параметров режима (IV, S-блоки). Однако на международной арене уступает современным алгоритмам (AES, Camellia) по скорости и универсальности.

**3. Вычислительная сложность**

**Временная:**

* На один блок: 32 раунда × операции S-блоков, сложения и сдвигов
* Общая сложность: O(N), где N — количество блоков

**По памяти:**

* Константные таблицы SBOX: 8×16 байт
* Хранение ключа: 256 бит
* Оценка RAM при обработке 500 МБ файла ≈ 2.5 ГБ (включая все структуры, паддинг и кэш)

**4. Программная реализация**

* Реализован блочный шифр «Магма» в **режиме OFB (Output Feedback)** по ГОСТ 34.13-2018.
* Программа:
  + Считывает файлы input1mb.txt, input100mb.txt, input500mb.txt
  + Шифрует и расшифровывает каждый из них, используя случайный IV и мастер-ключ
  + Дополняет данные до блока (паддинг) по ГОСТ
  + Сохраняет зашифрованные и расшифрованные данные в директории encrypted/ и decrypted/
  + Ведёт журнал действий в logs/magma\_ofb.log с правами 0600
  + Проводит **производительный тест**: 10⁶ блоков со сменой ключа каждые 10, 100, 1000 блоков
  + Показывает нагрузку на **CPU и RAM** во время операций
  + После каждого этапа — **очищает ключи** (рандомизация + зануление)

**5. Скорость выполнения тестов**

**5.1 Шифрование/расшифрование файлов:**

| **Файл** | **Шифрование (с)** | **Расшифровка (с)** | **CPU (%)** | **RAM (KB)** |
| --- | --- | --- | --- | --- |
| input1mb.txt | 0.0288 | 0.0286 | 99.97 | 8288 |
| input100mb.txt | 2.926 | 2.854 | 99.99 | 520228 |
| input500mb.txt | 14.485 | 14.244 | 99.99 | 2596788 |

**5.2 Шифрование/расшифрование 10⁶ блоков (8 МБ) со сменой ключа:**

| **Интервал смены ключа** | **Шифрование (с)** | **Расшифровка (с)** | **CPU (%)** | **RAM (KB)** |
| --- | --- | --- | --- | --- |
| Каждые 10 блоков | 0.2177 | 0.2197 | 100.0 | 36904 |
| Каждые 100 блоков | 0.2150 | 0.2179 | 100.0 | 36904 |
| Каждые 1000 блоков | 0.2167 | 0.2139 | 100.0 | 36904 |

**6. Описание тестового стенда**

* **ОС:** Ubuntu 22.04.4 LTS (WSL2 на Windows 11)
* **Архитектура:** x86\_64
* **Процессор:** Intel Core i5-12400H
* **ОЗУ:** 32 ГБ
* **Компилятор:** g++ 11.4

**7. Нагрузка на ЦП и ОЗУ**

* **CPU:** Загруженность одного ядра достигала 100%. Программа корректно измеряет потреблённое процессорное время по getrusage, делит его на wall-time и выводит процент.
* **RAM:** Использование оперативной памяти увеличивается пропорционально объёму обрабатываемого файла.  
  На 500 МБ зашифрованного файла использовано ≈ 2.6 ГБ памяти, включая кэш и все буферы.