Задание № 2 по практикуму на ЭВМ.

Реализация шифра Магма

Описание:

http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf
http://wwwold.tc26.ru/standard/gost/GOST_R_3413-2015.pdf

В данном задании требуется написать реализацию шифра Магма ГОСТ Р 34.12-2015 п.5 с режимами работы согласно ГОСТ Р 34.13-2015. Необходимо использовать процедуру дополнения исходных данных ГОСТ Р 34.13-2015 п. 4.1.2 для режимов ECB, CBC и CFB (п.5.1, 5.4, 5.5), ГОСТ Р 34.13-2015 п. 4.1.3 для режима MAC (п.5.6).

Поведение программы должно полностью управляться аргументами командной строки, в связи с чем вам потребуется реализовать полноценную обработку передаваемых параметров.

Описание флагов:

```
magma [-h|--help]
magma [--ecb|--ctr|--ofb|--cbc|--cfb] {-e|-d} -k <key file> [options]
magma --mac -k <key file> [options]
```

- `-h | --help` – вывести описание флагов в `stdout`.
- режимы работы, по умолчанию используется режим `ECB`:

  `--ecb` – ГОСТ Р 34.13-2015, пункт 5.1

  `--ctr` – ГОСТ Р 34.13-2015, пункт 5.2

  `--ofb` – ГОСТ Р 34.13-2015, пункт 5.3

  `--cbc` – ГОСТ Р 34.13-2015, пункт 5.4

  `--cfb` – ГОСТ Р 34.13-2015, пункт 5.5

  `--mac` – ГОСТ Р 34.13-2015, пункт 5.6
- `-e` – произвести зашифрование.
- `-d` – произвести расшифрование.
- `-k <key file>` – файл с бинарным ключом.
- `[options]`:

  `-i <input file>` – входной файл. По умолчанию читать с `stdin` до `EOF`;

  `-o <output file>` – выходной файл. По умолчанию выводить в `stdout`;

  `-v <iv file>` – файл с бинарным значением `IV`. Используется с режимами CTR (32 бита), OFB, CBC, CFB ($64z$ бита, $z \in \mathbb{N}$). По умолчанию `IV=0` минимально допустимой длины.
- `[описание дополнительно реализованных флагов]`

Примеры использования:

```
magma --mac -k file.key -i file.in -o file.out
magma --ctr -e -i path/to/file/to/ecrypt -o path/to/encrypted/file \
       -k path/to/key/file -v path/to/iv/file
```

Требования к функциональности:

1. Аргументы командной строки могут передаваться в произвольном порядке.
2. Если переданы неправильные аргументы, вывести сообщение об ошибке (желательно с указанием проблемного аргумента) и напечатать help в `stderr`.
3. Печатать сообщение об ошибке в случае некорректных размеров ключа, `IV` или шифротекста.
4. Если вы реализуете дополнительную печать, она должна включаться отдельным флагом, с выводом в `stderr`.
5. Все ошибки печатаются в `stderr`.

Требования к коду:

1. Программа должна быть написана на языке C/C++.
2. Код не должен быть скопирован у другого студента.
3. Стремиться к тому, чтобы каждая функция в коде не превышала 25 строк.
4. Стремиться к тому, чтобы каждая строка в коде не превышала 80 символов.
5. Функции и переменные должны иметь осмысленные имена.
6. Компиляция производится gcc версии 4.9+ (лучше 8.1+), с флагами -Wall -O2.
7. Реализация должна быть кроссплатформенной.
8. В архиве с программой должен быть Makefile.

Формат приема заданий:

1. Задания отсылаются на почту is.cmc.2018@yandex.ru.
2. Тема письма в формате “Задание_1_|номер задачи|_Ф_И_О” для задания 1.
3. Тема письма в формате “Задание_|номер|_Ф_И_О” для заданий 2,3.
4. В случае наличия замечаний/ошибок аспирант отправляет комментарий. Процесс повторяется до тех пор, пока аспирант не сообщит, что замечаний больше нет.

5. После устранения всех замечаний, назначается встреча в рамках пары для обсуждения деталей реализации, после чего выставляется оценка, согласно пункту “Формирование оценок”.

Сроки выдачи заданий:

- Задание 1: 3 сентября.
- Задание 2: 1 октября.
- Задание 3: ориентировочно, 1 ноября.

Формирование оценок:

- Оценка по заданию выставляется после очной встречи и обсуждения деталей реализации задания.
- Очная встреча назначается после устранения всех замечаний по заданию.
- Каждое задание оценивается в 5 баллов.
- Общая оценка вычисляется как среднее по 3 заданиям.
- Предварительная оценка на момент очной встречи по заданию определяется следующим образом:
  - Устранение всех замечаний в срок 5 недель с момента выдачи задания без учета времени проверки – **5**.
  - Устранение всех замечаний в срок (5, 6] недель с момента выдачи задания без учета времени проверки – **4**.
  - Отправка задания и устранение всех замечаний вне сроков описанных выше – **3**.
  - Невыполнение задания, наличие неустраненных замечаний к зачету – **2**.
- Пояснение фразы *“с момента выдачи задания без учета времени проверки”*:

  Время выделенное на выполнение вами задания не зависит от того, как долго мы его будем проверять.

  То есть, если вы сдадите задание через неделю после его выдачи, а мы будем его проверять 3 недели и после этого вышлем замечания, у вас все еще будет 4 недели на их исправление. Это относится ко всем заданиям, не только ко второму.
- Оценка по заданию по итогам очной встречи может быть изменена, исходя из субъективной оценки аспиранта о выполнении задания студентом, как в меньшую, так и в большую сторону.

Срок выполнения второго задания увеличен на неделю.

Задать вопросы, получить актуальную и оперативную информацию можно в Telegram-чате: https://t.me/joinchat/DpzKQxJXQ_xZAYlYyaYoPQ.