“Введение в криптографию” 2019-2020 г.о.

Формирование оценок:

Ниже описан список вариантов, по каждому из которых можно получить 1 балл. Предполагается, что 2 балла каждый студент имеет автоматически (то есть выполнение хотя бы одного из нижеперечисленных пунктов позволит вам получить 3).

Теоретический экзамен:

Теоретический экзамен будет состоять из билета и дополнительных заданий/вопросов.

Билет будет состоять из 2 теоретических вопросов. Вопросы будут из разных разделов, например: один вопрос по симметричной криптографии, другой по хеш-функциям.

Сдача вопроса из билета подразумевает оценку вашего понимания этого вопроса, поэтому при подготовке можно пользоваться любыми материалами.

Дополнительные вопросы/задачи будут по сложности похожи на те, которые разбирались на лекциях. Дополнительных вопросов/задач будет не менее 2.

Варианты получения баллов:

Каждый вариант позволит получить 1 балл. Дополнительную информацию для пунктов 4-7 необходимо указывать тут.

1. Теоретический экзамен. Вопрос из билета №1.
2. Теоретический экзамен. Вопрос из билета №2.
3. Теоретический экзамен. Ответ на дополнительные вопросы/решение простых задач.
4. Реализация одного из стандартов симметричного шифрования Магма/Кузнечик. Ссылка на ГОСТ 34.12-2015.

   При выборе этого пункта необходимо указать, что именно собираетесь реализовывать Кузнечик или Магму.
5. Дополнительно к предыдущему пункту, реализация одного из режимов шифрования Ссылка на ГОСТ 34.13-2015.

   При выборе этого пункта необходимо указать, какой именно режим шифрования собираетесь использовать (смотрите соответствие режимов тому, что проходили на лекции, в пояснении к пунктам 4 и 5).
6. Взлом шифра простой замены.

   При выборе этого пункта необходимо указать язык, для которого будете осуществлять взлом (смотрите пояснения к пункту 6)
7. Устный доклад в декабре на одной из пар. Тематика докладов: криптоанализ, атаки на современные криптографические алгоритмы и примитивы. Продолжительность доклада: 10-20 минут.

   При выборе этого пункта достаточно указать “+”.

Пояснение к пунктам 4 и 5

Ваша программа должна проходить тесты, указанные в ГОСТе.

Также должна существовать возможность передать программе на вход отличные от примеров в стандартах ключ, открытый текст.

Как вариант, может быть реализована обработка аргументов командной строки, через которые передаются пути к файлам, где хранится ключ, открытый текст, куда должен быть записан выходной текст, желаемый режим шифрования или дешифрования. Пример использования для C/C++:

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

Опции, для которых должна быть возможность задать их извне:

- `-e` – произвести шифрование.
- `-d` – произвести дешифрование.
- `-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.

Соответствие режимов из стандарта 34.13-2015 с теми, что проходили на лекции:

`ecb` – пункт 5.1

`ctr` – пункт 5.2

`ofb` – пункт 5.3

`cbc` – пункт 5.4

`cfb` – пункт 5.5

`mac` – пункт 5.6

Пояснение к пункту 6

Алгоритм должен реализовывать взлом произвольного шифра простой замены. Алгоритм должен состоять из 2 независимых этапов:

- Сбор статистики для взлома. На вход поступает открытый текст (несколько сотен символов, например, несколько глав “Война и мир” Л.Н.Толстого)

- Взлом шифра простой замены. На вход поступает шифртекст (несколько десятков символов, например, зашифрованный абзац из главы “Война и мир” Л.Н.Толстого, которая **не** использовалась для сбора статистики на первом этапе).

Для проверки первого и второго этапов будут использованы части одной и той же книги. На выбор взлом может быть сделан для английского и/или русского языков.

Сдача практических заданий

Сдача практических заданий до экзамена осуществляется или очно, или посредством посылки готового решения на почту iteryokhina@cs.msu.ru. На экзамене сдача осуществляется очно.

До экзамена желательно уточнить у меня, смогу ли я запустить вашу программу у себя (так как не накладывалось ограничений на языки программирования), или прийти со своим ноутбуком.

По всем вопросам/опечаткам/предложениям писать в tg:@irtery или на почту iteryokhina@cs.msu.ru