**ВАЖНО!** Перед данной работы рекомендуется выполнить  
[лабораторную на распознание режимов шифрования.](https://github.com/CryptoCourse/CryptoLabs/blob/master/docs/labEncryptionModeDist.md)

Дана REST служба с API указанным ниже.

Служба шифрует указанный пользователем открытый текст, следующим образом:

E(k, random\_padding || user\_data || target\_data||)

random\_padding - случайное дополнение, фиксированное для пары <userId>, <challengeId>

user\_data - данные пользователя (из post запроса)

target\_data - целевые данные, фиксированные для пары <userId>, <challengeId>.

Задача - расшифровать target\_data.

**ВАЖНО!** Все передаваемые сообщения должны быть предварительно закодированы с помощью BASE64.

Полученные сообщения так же должны быть декодированы из BASE64 в указанный тип.

**ВАЖНО!** Все строки кодируется с использование кодировки ASCII.

т.е. передача строки для лр выглядит следующим образом:  
строка -> (asсii) -> массив байт -> (base64) -> строка -> json

## Ход работы.

### Тестирование

<userId> = имя аккаунта на GitHub (или фамилия студента)

<challengeId> = 1, 2, 3, 4, 5

1. Проверить работоспособность контроллера с помощью метода GET <host>/api/EcbDecryption
2. Получить зашифрованное сообщение с помощью метода POST <host>/api/EcbDecryption/<userId>/<challengeId>/noentropy
3. Определить режим шифрования  
   3.1 Если режим шифрования CBC, перейти к следующему <challengeId>.
4. Используя метод POST <host>/api/EcbDecryption/<userId>/<challengeId>/noentropy получить необходимые шифртексты.
5. Расшифровать target\_data
6. Проверить верность ответа использовав метод GET <host>/api/EcbDecryption/<userId>/<challengeId>/verify
7. Проверить корректность программы для <challengeId> = 1..10

### Сдача лр

шаги 1 - 7 этапа тестирования аналогично, но для 15 различных <challengeId>.

## Описание API

Rest запросы, в заголовке выстален Content-Type: application/json; charset=utf-8.

### Описание методов

## GET <host>/api/EcbDecryption

Проверка работоспособности контроллера. Возвращает operating. Ответ не кодируется в BASE64.

|  |  |
| --- | --- |
| Параметр | Описание |
| <host> | имя хоста веб службы |

## POST <host>/api/EcbDecryption/<userId>/<challengeId>/noentropy

Дополняет полученные данные случайными байтами в начале и в конце. Способ дополнения описан в начале лабораторной.

После чего зашифровывает данные на фиксированном для задания ключе, либо в режиме CBC, либо в ECB.

|  |  |
| --- | --- |
| Параметр | Описание |
| <host> | имя хоста веб службы |
| <userId> | идентификатор студента |
| <challengeId> | идентификатор задания |

## GET <host>/api/EncryptionModeOracle/<userId>/<challengeId>/verify

Возвращает target\_data для указанного задания

|  |  |
| --- | --- |
| Параметр | Описание |
| <host> | имя хоста веб службы |
| <userId> | идентификатор студента |
| <challengeId> | идентификатор задания |