Дана REST служба с API указанным ниже.

Задача - построить эффективный распознаватель режимов шифрования (ECB, CBC).

**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

1. Проверить работоспособность контроллера с помощью метода GET <host>/api/EncryptionModeOracle
2. Получить зашифрованное сообщение с помощью метода POST <host>/api/EncryptionModeOracle/<userId>/<challengeId>/noentropy
3. Определить режим шифрования
4. Проверить верность ответа использовав метод GET <host>/api/EncryptionModeOracle/<userId>/<challengeId>/verify
5. Проверить корреиность программы для <challengeId> = 1..10

### Сдача лр

шаги 1 - 3 этапа тестирования аналогично, но использование метода POST <host>/api/EncryptionModeOracle/<userId>/<challengeId> на шаге 2.  
для 50 различных <challengeId>.

## Описание API

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

### Описание методов

## GET <host>/api/EncryptionModeOracle

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

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

## POST <host>/api/EncryptionModeOracle/<userId>/<challengeId>

Дополняет полученные данные случайными байтами вначале и в конце.

После чего зашифровывает данные на случайном ключе, либо в режиме CBC, либо в ECB.

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

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

Дополняет полученные данные случайными байтами вначале и в конце.

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, какой режим использует метод POST <host>/api/EncryptionModeOracle/<userId>/<challengeId>/noentropy  
в указанном задании. Ответ не кодируется в BASE64. Возвращает "ECB" или "CBC"

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