## Задание

Дана REST служба с API указанным ниже.

Задача - детерминировано дешифровать пин-код из шифртекста.

Пин-код длины не более 5, состоит из цифр. Строковое представление пин-кода кодируется с помощью ASCII, дополняется до  
длины 16 байт нулями и шифруется.

**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/IvIsTime
2. Получить зашифрованный пин-код с помощью метода GET <host>/api/EncryptionModeOracle/<userId>/<challengeId>/encryptedpin
3. Получить пин-код, используя метод POST <host>/api/EncryptionModeOracle/<userId>/<challengeId>/noentropy
4. Проверить пин-код, используя метод GET <host>/api/IvIsTime/<userId>/<challengeId>/validate

### Сдача лр

шаги 1 - 3 этапа тестирования аналогично для 20 различных <challengeId>.

## Описание API

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

### Описание методов

## GET <host>/api/IvIsTime

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

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

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

Зашифровывает данные в режиме CBC на фиксированном для задания для задания ключе.

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

## GET <host>/api/IvIsTime/<userId>/<challengeId>/encryptedpin

Возвращает зашифрованный пин код, на фиксированном для задания ключе

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

## GET <host>/api/IvIsTime/time

текущее время в формате unix time (секунды), используется в качестве IV.

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

## GET <host>/api/IvIsTime/<userId>/<challengeId>/validate

Возвращает пин-код, используемый в задании.

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