Encryption API

Time: 1h30

Requirements

Create an application that will expose REST APIs that allow encrypting and decrypting the content passed a payload. The API end points are:

Encryption

- Request:
  - POST /encrypt
- Payload:
  - data: [{
    text: “Message to encrypt.”
    }, {
    text: “Second message to encrypt.”
    }]
- Response:
  - data: [{
    encrypted: “…”
    }, {
    encrypted: “…”
    }]

You can chose the encryption algorythm of your choice. Some popular ones are:

- AES
- DES
- Blowfish

The encrypted data should be of type String. If the encryption generates an array of bytes, you can convert them using Base-64 encoding.

Decryption

- Request:
  - POST /decrypt
- Payload:
  - data: [{
    encrypted: “…”
    }, {
    encrypted: “…”
    }]
- Response:
  - data: [{
    text: “Message to encrypt.”
    }, {
    text: “Second message to encrypt.”
    }]

Marking criteria

What you'll be evaluated on:

- Functionality: the code compiles, runs, and satisfies the given requirements
- SOLID principles
- Code cleanliness and readability
- Unit test coverage
- Integration test coverage
- Documentation:
  - Useful comments in the code
  - README file that explains how to run your code

Tools and language

You can use your own laptop or use the provided ones.

You can use internet (Google, StackOverflow, technet…) but be mindful to not copy code as-is. Create your own structure.

You can ask for help to the Agoda staff, in particular if you are stuck in getting started.

Tips

- Focus on the class design, interfaces of functionality first.
- Once it's done then work on implementation, input parsing, serving result
- Try using meaningful names for classes, variables, methods, etc.
- Edge cases handling is a plus.
- If in doubt, please ask for clarification.