В теоретической части пользователь знакомится с информацией необходимой для понимания методов шифрования/дешифрования данных, получая доступ к следующим разделам по средству ответа на поставленные вопрос и имея возможность проверяя свой прогресс по мере ознакомления.

В практической части имеется возможность ввода текста (алфавита), выбора ключа и манипуляция с шифрованием/дешифрования представленного алфавита.

На втором этапе определены основные составляющие предметной области исходя из анализа приложений-аналогов, произведённого выше.

Теоретическая часть приложения:

* User (Пользователь): содержит информацию о пользователях приложения;
* Lesson (Урок): представляет урок по криптографии данных. Содержит материалы урока;
* Quiz (Тест): содержит вопросы и ответы для проверки знаний пользователей;
* UserProgress (Прогресс пользователя): связывает пользователя и урок, отслеживает прогресс пользователя в изучении курса.

Связи между элементами предметной области:

* User имеет отношение "имеет" к UserProgress;
* UserProgress имеет отношение "относится к" к Lesson;
* Lesson имеет отношение "содержит" к Quiz.

Практическая часть приложения:

* CryptographicSystem (Криптографическая система): представляет центральный компонент криптографической системы;
* KeyManagement (Управление ключами): отвечает за создание и управление криптографическими ключами;
* EncryptionAlgorithm (Алгоритм шифрования): содержит математические методы шифрования и дешифрования;
* DecryptionAlgorithm (Алгоритм дешифрования): осуществляет обратное преобразование зашифрованных данных;
* Message (Сообщение): представляет данные, которые требуется зашифровать или дешифровать.

Связи между классами:

* CryptographicSystem связан с KeyManagement, EncryptionAlgorithm и DecryptionAlgorithm;
* KeyManagement генерирует криптографические ключи и предоставляет их EncryptionAlgorithm и DecryptionAlgorithm;
* EncryptionAlgorithm и DecryptionAlgorithm используют ключи и обрабатывают Message.

+-----------------+ +----------------+ +-------------+

| User | | Lesson | | Quiz |

+-----------------+ +----------------+ +-------------+

| - userID | | - lessonID | | - quizID |

| - username | | - lessonTitle | | - questions |

| - email | | - content | | - answers |

| - passwordHash | | - concepts | +-------------+

+-----------------+ +----------------+

| | 1..\* | 1..\*

| |

| |

v v

+-----------------+ +----------------+

| UserProgress | | Cryptographic |

+-----------------+ | Concept |

| - progressID | +----------------+

| - userID | | - conceptID |

| - lessonID | | - conceptTitle |

| - completed | | - description |

+---------------------+

| CryptographicSystem |

+---------------------+

| - keyManagement |

| - encryptionAlg |

| - decryptionAlg |

+---------------------+

| | |

| | |

v v v

+----------------+ +----------------+

| KeyManagement | | EncryptionAlg |

+----------------+ +----------------+

| - generateKeys | | - encrypt |

| - provideKey | | - decrypt |

+----------------+ +----------------+

| |

v v

+----------------+ +----------------+

| Message | | DecryptionAlg |

+----------------+ +----------------+

| - data | | - decrypt |

+----------------+ +----------------+

<https://habr.com/ru/articles/721790/>