**Методы проектирования, используемые при создании проекта:**

При проектировании и разработке Приложения Шифрования DES/XOR можно выделить следующие этапы работы:

**I этап. Постановка задачи:**

На этом этапе формируется задание по созданию Приложения шифрования текстовой информации. В нем подробно описывается состав программы, назначение и цели ее создания, а также перечисляется, какие виды работ предполагается осуществлять в программе (отбор, дополнение, изменение данных, вводили вывод и тд.).

Для разработки данного приложения был использован структурный метод проектиирования.

Характеристика и методология структурного проектирования использованные в данном проекте:

* нисходящее проектирование,
* кодирование и тестирование программ;
* модульное программирование;
* структурное проектирование (программирование) и др.

В зависимости от объекта структурирования различают:

функционально-ориентированные методы — последовательное разложение задачи или целостной проблемы на отдельные, достаточно простые составляющие, обладающие функциональной определенностью;

**II этап. Методы структурирования данных**.

Для функционально-ориентированных методов в первую очередь учитываются заданные функции обработки данных, в соответствии с которыми определяется состав и логика работы (алгоритмы) отдельных компонентов программного продукта. С изменением содержания функций обработки, их состава, соответствующего им информационного входа и вы­хода требуется перепроектирование программного продукта. Основной упор в структурном подходе делается на моделирование процессов обработки данных. Для методов структурирования данных осуществляется анализ, структурирование и создание моделей данных, применительно к которым устанавливается необходимый состав функций и процедур обработки. Программные продукты тесно связаны со структурой обрабатываемых данных, изменение которой отражается на логике обработки (алгоритмах) и обязательно требует перепроектирования программного продукта.

.

Структурный подход и как он используется:

• диаграммы потоков данных (информационно-технологические схемы) — показывают процессы и информационные потоки между ними с учетом "событий", инициирующих процессы обработки;

• интегрированную структуру данных предметной области (инфологическая модель, ER-диаграммы);

•диаграммы декомпозиции — структура и декомпозиция целей, функций управления, приложений;

• структурные схемы — архитектура программного продукта в виде иерархии взаимо­ связанных программных модулей с идентификацией связей между ними, детальная логика обработки данных программных модулей (блок-схемы). Для полного представления о программном продукте необходима также текстовая ин­формация описательного характера.

**III этап. На чем основывался выбор алгоритма шифрования.**

Для шифрования данных в текстовом виде было использовано 2 вида алгоритма шифрования с не заданным ключом шифрования(XOR) и заданным заранее количеством бит ключ(DES). Особенности данного приложения в том, что des и xor на прямую связаны математическими формулами и самой концепцией ключей.

Немного о XOR:

Особенность XOR в том, что одной и той же функцией можно как зашифровать данные, так и расшифровать их. Это простой метод шифрации данных, который может быть взломан достаточно быстро при наличии достаточно большого зашифрованного текста, или большого словаря паролей. Тем не менее это уже можно применять для небольшой первоначально защиты данных.

Немного о Des:

DES (Data Encryption Standard) — симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных. DES разработан фирмой IBM и утвержден правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бит и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит(в преобразовании учавствуют раундовые ключи по 48 бит). Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов.

**IV этап. Выбор способов представления информации и программного инструментария.**

После создания модели необходимо, в зависимости от выбранного программного продукта, определить форму представления информации.

Для работы с программой для пользователя предоставлен интерфейс:

* Оконное приложение

В моём решении (программе) данные представлены в сугубо текстовом представлении, но формат файла может определить сам пользователь.

**V этап. Создание компьютерной модели объекта.**

В процессе создания компьютерной модели можно выделить некоторые стадии, типичные для любого приложения:

**Стадия 1**. Запуск программного средства в котором будет написан код.

**Стадия 2.** Создание интерфейса программы.

Создавая интерфейс программы шифрования нужно использовать простые решения с простым и отзывчивым интерфейсом.

**Стадия 3.** Описание или памятка для пользователя.

Нужно учитывать, что некоторые алгоритмы шифрования бывают с ограничением на ввод символов или Бит. Для того, чтобы приложение работало корректно в руках пользователя нужно дать ему понять как с ней работать и указать либо в самой форме приложения информацию об использовании, либо сделать вывод окна с перечнем правил.

**VI этап. Работа с готовой программой шифрования.**

Работа с программой включает в себя следующие действия:

* поиск необходимых сведений для шифрования;
* сортировка данных;
* отбор данных;
* вывод на печать;
* Шифрования/Дешифровка
* изменение и дополнение данных.
* Удаление данных из файла с зашифровкой или дешифровкой и тд.

Источники:

1. <https://studizba.com/lectures/10-informatika-i-programmirovanie/323-lekcii-po-informatike-i-programmirovaniyu/4303-metodologiya-proektirovaniya-programmnyh-produktov.html>
2. <https://ru.bmstu.wiki/DES_%28Data_Encryption_Standard%29>
3. <https://evileg.com/ru/post/271/>