**Программное решение.**

1. **Описания алгоритмов шифрования.**

Шифрование — обратимое преобразование информации в целях сокрытия от [неавторизованных](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) лиц, с предоставлением, в это же время, [авторизованным](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) пользователям доступа к ней.

Главным образом, шифрование служит задачей соблюдения [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) передаваемой информации. Важной особенностью любого алгоритма шифрования является использование [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма**.**

1. **Особенности алгоритмов шифрования «симметричный и ассиметричный ключ шифрования»**

**Ключ шифрования**— это секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности. Количество информации в ключе измеряется в битах: чем больше битов в ключе, тем надежней зашифрована информация.

Ключи шифрования бывают симметричными и ассиметричными.

**ассиметричный шифр -** используется два ключа: один для шифрования, открытый (он передается по открытому каналу), другой для расшифровки (так называемый, закрытый ключ).

**Симметричный шифр** - обычно строится на основании ряда блоков с математическими функциями преобразования, ассиметричный — на математических задачах. Тот же RSA создан на задаче возведения в степень с последующим вычислением модуля. В результате алгоритмы симметричного шифрования модифицировать просто, а ассиметричного — практически невозможно

**Программное использование:**

Области применения у обоих типов шифрования разные, поэтому при выборе нужно соотносить возможности алгоритмов с поставленными задачами. Может быть, использовать гибридные решения.

Следует учитывать и практическую целесообразность. Допустим, если ваша программа предназначена только для персонального пользования, вряд ли будет рациональным использовать ассиметричный подход. Лучший вариант здесь — мощный симметричный алгоритм.

Характеристика:

Название / статус DES (Data Encryption Standard).

Федеральный стандарт шифрования США в 1977-2001 годах.

Время / место разработки

Создан в 1972-1975 годы в исследовательской лаборатории корпорации IBM. В качестве федерального стандарта США принят в 1977 году. В декабре 2001 года утратил свой статус в связи с введением в действие нового стандарта.

Авторы: Группа под руководством д-ра. У.Тачмена.

Архитектура: Классическая сбалансированная сеть Файстеля с начальной и конечной битовыми перестановками общего вида.

Параметры:

pазмер блока, бит 64

pазмер ключа, бит 56 (64, 8 из которых служат для контроля четности)

число раундов 16

pазмер ключевого элемента, бит 48

число ключевых элементов 16 (равно числу раундов)

Патент Не запатентован.

Особенности Широкое использование битовых перестановок в DES делает алгоритм неудобным для программных реализаций на универсальных процессорах, а сами такие реализции крайне неэффективными. По сравнению с Российским стандартом шифрования DES содержит вдвое меньше раундов, однако его оптимальная реализация для процессоров линии Intel x86 уступает реализации Российского стандарта по скорости в 3-5 раз в зависимости от марки процессора, эта разница увеличивается от младших моделей к старшим. Кроме того, по единодушному мнению криптографов начальная и конечная битовые перестановки являются не более чем "украшениями" алгоритма т.е. бесполезны с криптографической точки зрения, а размера ключа в 56 бит явно недостаточно для обеспечения приемлемой стойкости, что регулярно демонстрируется успехами во вскрытии шифровок DES путем подбора ключа методом прямого перебора с помощью распределенной сети или спецпроцессора.

Источники:

1. Оутус - .<https://otus.ru/nest/post/726/>

2.Вики -<https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5>

3. Описание алгоритма DES на странице ИС США <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

4. описание режимов шифрования DES на странице ИС США <http://www.itl.nist.gov/fipspubs/fip81.htm>

5. различные реализации (FTP) ftp://ftp.funet.fi/pub/crypt/cryptography/libs/des/