## Практическая работа №2 - Алгоритм шифрования с ключом

**Цель работы:**

Анализ существующих простейших алгоритмов шифрования с ключом.

**Задание:**

- разработать собственный алгоритм шифрования и дешифрования данных с ключом;

- разработать форму содержащую: 3 текстовых поля, кнопку «Шифровать», кнопку «Расшифровать», текстовое поле «Ключ» для шифрации, текстовое поле «Ключ» для дешифрации;

- реализовать разработанный алгоритм на любом языке программирования.

**Методика выполнения Практической работы**

Студентами рассматриваются существующие простые алгоритмы шифрования с ключом. В результате просмотра и анализа источников литературы формируются принципы работы алгоритмов шифрования.

**Основные теоретические положения**

Все криптоалгоритмы с ключом делятся на симметричные и асимметричные. В симметричных криптоалгоритмах ключи, используемые на передающей и приемной сторонах, полностью идентичны. Такой ключ несет в себе всю информацию о засекречивании сообщения и поэтому не должен быть известен никому, кроме двух участвующих в разговоре сторон. Поэтому в отношении ключа симметричных систем часто применяется термин секретный ключ, а сами подобные системы называются шифрами на секретном ключе.

Симметричное шифрование можно применять как при отправке сообщений между двумя пользователями, разделенными большим расстоянием, так и при отправке “посланий” одним и тем же человеком самому себе, но во времени. Примером подобных отправлений является шифр файлов на жестких дисках и сменных носителях с тем, чтобы другие пользователи тех же ЭВМ не могли считать информацию в отсутствие владельца.

В асимметричном шифровании, для шифрования сообщения применяется один ключ, а для дешифрования другой. Ниже на рис. 1 показана схема передачи информации абонентом А абоненту В.

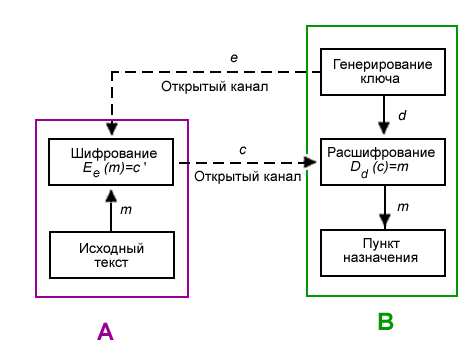


Рис. 1. Шифрование с открытым ключом

1. Абонент B выбирает пару (*e*,*d*) и шлёт ключ шифрования *e* (открытый ключ) абоненту A по открытому каналу, а ключ расшифрования *d* (закрытый ключ) защищён и секретен (он не должен передаваться по открытому каналу, либо его подлинность должна быть гарантирована некоторым сертифицирующим органом).
2. Чтобы послать сообщение *m* абоненту B, абонент A применяет функцию шифрования, определённую открытым ключом *e: Ee(m) = c, c* — полученный шифротекст.
3. Абонент B расшифровывает шифротекст *c*, применяя обратное преобразование *Dd*, однозначно определённое значением *d*.[2]

**Требования к предъявляемой работе:**

- Программа шифрования должны быть наделена понятным и удобным пользовательским интерфейсом.

- Алгоритм шифрования в обязательном порядке должен использовать математические и- или побитовые функции.

- Разработанный алгоритм должен приводить к полной утрате всех статистических закономерностей исходного сообщения.

- Максимально возможная длина ключа шифрования 100 символов. Минимальная 1 длина ключа 1 символ.