## Практическая работа №4 - Асимметричный алгоритм шифрования

**Цель работы:**

Исследование структуры асимметричных алгоритмов шифрования: *RSA, DSA, Схема Эль-Гамаля, ГОСТ Р 34.10-2001*.

**Задание:**

- реализовать один из существующих асимметричных алгоритмов шифрования: *RSA, DSA, Схема Эль-Гамаля, ГОСТ Р 34.10-2001*;

- реализовать разработанный алгоритм на любом языке программирования.

**Методика выполнения Практической работы**

Студентами рассматриваются один из алгоритмов симметричного шифрования. Изучается алгоритм работы выбранного алгоритма шифрования и после чего, реализуется на каком либо языке программирования.

**Дополнительная информация к выполнению Практической работы**

Примером асимметричного алгоритма шифрования может являться схема Эль Гамаля. Схема шифрования Эль Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность схемы Эль Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

В настоящее время наиболее перспективными системами криптографической защиты являются системы с открытым ключом. В таких системах для шифрования сообщения используется закрытый ключ, а для расшифрования – открытый.

Открытый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровывание данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует секретный ключ, который не может быть определён из открытого ключа.

При использовании алгоритма шифрования Эль Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***М***. В реальных схемах шифрования необходимо использовать в качестве модуля n большое простое число, имеющее в двоичном представлении длину ***512… 1024 бит***.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения ***k***, причём это значение должно выбираться случайным образом. Если нарушитель раскроет значение ***k***, повторно используемое отправителем, то может раскрыть и секретный ключ ***x*** отправителя. Ниже приведен алгоритм шифрования данных по схеме Эль Гамаля. [5,6]

Шаг 1. Определение открытого “*y*” и секретного “*x*” ключей

Шаг 1.1. Выбор значения секретного ключа *x, x < p*

Шаг 1.2. Выбор двух взаимно простых больших чисел *p* и *q*, *q < p*

Шаг 1.3. Определение значения открытого ключа *y* из выражения:*y = qx (mod p)*

Шаг 2. Алгоритм шифрования сообщения M

Шаг 2.1. Выбор случайного числа *k*, удовлетворяющего условию:

*0* ≤ *k < p-1* и *НОД (k,p-1) = 1*

Шаг 2.2. Определение значения *a* из выражения: *a = qk(mod p)*

Шаг 2.3. Определение значения *b* из выражения: *b = yk M (mod p)*

Шаг 2.4. Криптограмма *C,* состоящая из *a и b,* отправляется получателю.

Шаг 2.5. Получатель расшифровывает криптограмму с помощью выражения*:*

*M ax = b (mod p)*

На рис. 4 представлен результат работы алгоритма шифрования по схеме Эль-Гамаля.

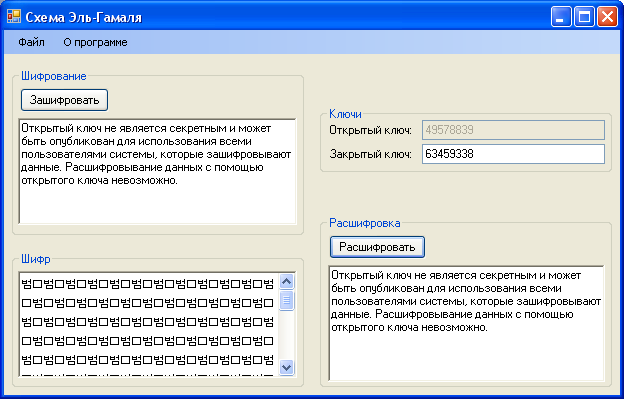
****

Рис. 4. Форма Алгоритм шифрования Схема Эль-Гамаля

**Требования к предъявляемой работе:**

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

- Полная реализация выбранного алгоритма.

- Запрещено использование любых сторонних библиотек.