***Тема***: шифрование с открытым ключом.

***Задание на лабораторную работу:***

1. Программно реализовать алгоритм шифрования/дешифрования RSA.

***Сроки выполнения:*** 24/09/2021-8/10/2021.

***Среда реализации***: любая.

***Методические указания:***

Алгоритм шифрования RSA.

1. Выбираются два различных случайных простых числа p и q.
2. Вычисляется их произведение n=p⋅q, которое называется *модулем*.
3. Вычисляется значение функции Эйлера от числа n:

φ(n)=(p−1)⋅(q−1).

1. Выбирается целое число e (1<e<φ(n), взаимно простое со значением функции  φ(n)φ(n). Обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи. Число e называется открытой экспонентой.
2. Вычисляется число d, удовлетворяющее сравнению:

d⋅e≡1(modφ(n)).

Число d называется секретной экспонентой.

1. Пара {e,n} публикуется в качестве открытого ключа RSA.
2. Пара {d,n} играет роль закрытого ключа RSA и держится в секрете.
3. Для шифрования сообщения m необходимо выполнить

m=(cd)mod n

1. Для шифрования сообщения m необходимо выполнить

c=(me)mod n

1. Пример шифрования RSA–
   1. <https://www.e-nigma.ru/stat/rsa/>
   2. <http://infoprotect.net/varia/algoritm_shifrovaniya_rsa_primer>