**ЛАБОРАТОРНА РОБОТА 5**

**СПОСОБИ ШИФРУВАННЯ ІНФОРМАЦІЇ**

***Мета роботи:*** дослідити способи побудови різних типів шифрів.

**Вхідні дані**

Матушевич Ярослав Євгенович

1 листопада 1997 року

10 номер в групі

Повідомлення M = ‘MATUSHEVYCH YAROSLAV’

Нехай

Тоді

Відкритий ключ – взаємно простий з

Розв’язуємо цілочисельне рівняння

Закритий ключ

Отже, відкритий ключ

Закритий ключ

Реалізуємо в MATLAB

Степінь з покроковим розрахунком залишку, щоб запобігти переповненню

function res = pow\_modulo(x, n, m)

%x - base of power

%n - power

%m - modulo

res = 1;

for i = 1:n

res = mod(res\*x, m);

end

end

Основний модуль

%RSA

M = 'MATUSHEVYCH YAROSLAV'; %message

p = 17;

q = 31;

n = p\*q;

phi = (p-1)\*(q-1);

e = 7;

d = 343;

alph = 'A':'Z';

Map(alph(1:26)) = 1:26;

MNUM = Map(M); %message to numbers

disp('Original message in numbers');

disp(MNUM);

N = size(MNUM,2);

%encryption

E = zeros(1,N);

for i = 1:N

E(i) = pow\_modulo(MNUM(i),e,n);

end

disp('Encrypted');

disp(E);

%decryption

D = zeros(1,N);

for i = 1:N

D(i) = pow\_modulo(E(i),d,n);

end

disp('Decrypted');

disp(D);

Результат виконання

>> RSA

Original message in numbers

13 1 20 21 19 8 5 22 25 3 8 0 25 1 18 15 19 12 1 22

Encrypted

208 1 266 166 162 219 129 486 304 79 219 0 304 1 443 178 162 24 1 486

Decrypted

13 1 20 21 19 8 5 22 25 3 8 0 25 1 18 15 19 12 1 22

***Висновки***

Було проведено дослідження шифрування і дешифрування з алгоритмом RSA.

Знайдено пару відкритий-закритий ключ для обраних .

Розроблено додаток в MATLAB, з урахуванням можливостей переповнення для великих степеней. Отримано правильний результат.