Отчет по ЛР 3 «Криптосистема RSA»

Индюков Станислав 5ПИ

2 Вариант

Дано:

p	684391453787369
q	938396705691661
e	24537234425391565353136925689 9
X1	184712154522842417799563173273
Y2	44720486418380146363820886811 6

Вычислить:

1. Личный ключ *d* заданных *p, q* и *e*.
2. Для заданного сообщения *X1*, зашифрованное сообщение Y1, используя открытый ключ *e*.
3. Сообщение *Y1*, используя личный ключ d, сравнить результат с исходным сообщением *X1*.
4. Для заданного шифртекста *Y2*, исходный открытый текст *X2*, используя личный ключ *d*.

Ход работы:

Разработанная программа имеет следующий набор команд (рис. 1).

```
> help

    gen {p} {q} {e}           - gets private key   - p (prime), q (prime), e (public key)
    encr {x} {e} {n | p q}    - encrypts message   - x (int), e (public key), n (module) | p q (primes)
    decr {x} {d} {n | p q}    - encrypts message   - x (int), d (private key), n (module) | p q (primes)

    help - list of commands
    exit - exit
```

Рис. 1 – Набор команд

1. По заданным *p*, *q* и *e* вычисляем *d*. Полученный ключ, так же представлен на рисунке 2: 6053861662624766125227754551 79

```
> gen 684391453787369 938396705691661 24537234425391565353136925689960538616626247661252277545517 9
>
```

Рис. 2 – Личный ключ

2. По заданному *X1* вычислим *Y1*.
   Результат (рис. 3): 120595678337547166852120120039

```
> encr 184712154522842417799563173273 24537234425391565353136925689960538616626247661252277545517 9 684391453787369 938396705691661
120595678337547166852120120039
>
```

Рис. 3 – Шифротекст 1

3. Обратно вычислим *X1*, по *Y1* при помощи личного ключа.
   Результат (рис. 4): 184712154522842417799563173273
   Заметим, что результат совпадает с *X1*, что свидетельствует о правильной реализации алгоритма шифрования.

```
> decr 120595678337547166852120120039 60538616626247661252277545517 9 684391453787369 938396705691661
184712154522842417799563173273
>
```

Рис. 4 – Расшифровка *Y1*

4. Используя личный ключ, вычислим *X2* из *Y2*.
   Результат (рис. 5): 22229472790034336755103030065 4.

```
> decr 44720486418380146363820886811660538616626247661252277545517 9 684391453787369 938396705691661
22229472790034336755103030065 4
>
```

Рис. 5 – Расшифровка *Y2*