Отчет по ЛР 3 «Криптосистема RSA»

Индюков Станислав 5ПИ

2 Вариант

Дано:

|  |  |
| --- | --- |
| p | 684391453787369 |
| q | 938396705691661 |
| e | 245372344253915653531369256899 |
| X1 | 184712154522842417799563173273 |
| Y2 | 447204864183801463638208868116 |

Вычислить:

1. Личный ключ *d* заданных *p*, *q* и *e*.
2. Для заданного сообщения *X1*, зашифрованное сообщение Y1, используя открытый ключ *e*.
3. Cообщение *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).

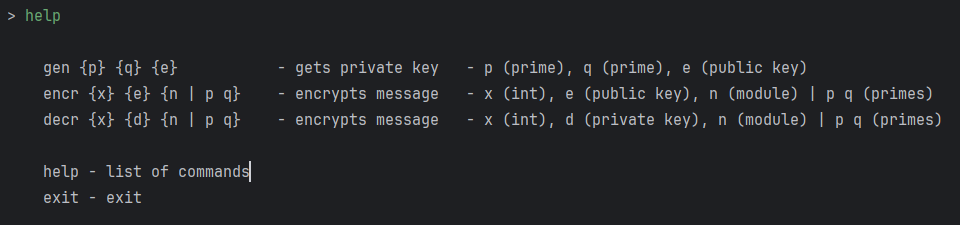


Рис. 1 – Набор команд

1. По заданным *p*, *q* и *e* вычисляем *d*. Полученный ключ, так же представлен на рисунке 2: 605386166262476612522775455179

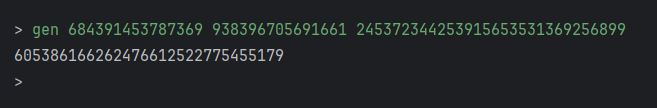


Рис. 2 – Личный ключ

1. По заданному *X1* вычислим *Y1*.

Результат (рис. 3): 120595678337547166852120120039

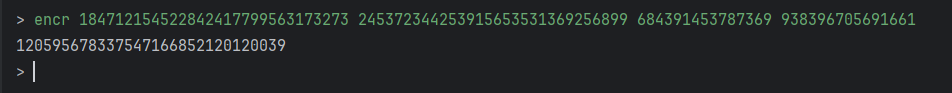


Рис. 3 – Шифротекст 1

1. 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.

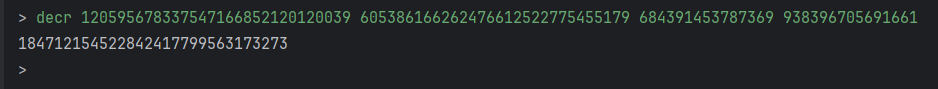


Рис. 4 – Расшифровка *Y1*

1. Используя личный ключ, вычислим *X2* из *Y2.*

Результат (рис. 5): 222294727900343367551030300654.

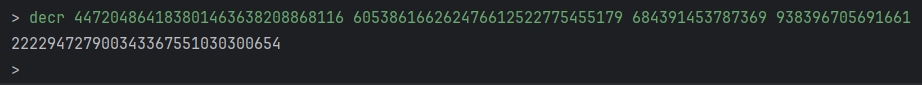


Рис. 5 – Расшифровка *Y2*