РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ RSA В СИСТЕМЕ WOLFRAM MATHEMATICA

Юхновская О.В.,
молодой ученый ПСФ, УО «БНТУ», г. Минск, Республика Беларусь

Ключевые слова. Шифрование информации, простые числа, компьютерная система Wolfram Mathematica.

Keywords. Encryption of information, ordinary numbers, Wolfram Mathematica computer system.

Вопрос сохранности данных не утрачивает свою актуальность. Важным аспектом этого вопроса является разработка алгоритмов шифрования, которые трудно взломать из-за их вычислительной сложности. Суть шифрования заключается в следующем: сначала происходит переход данных через серию математических операций, которые генерируют альтернативную форму этих данных, затем получатель преобразует эту форму в исходную.

Безопасность шифрования заключается в способности алгоритма генерировать зашифрованный текст, который нелегко преобразовать в исходный. Криптографическая функция в основном зависит от значения ключа, необходимого как для шифрования, так и для дешифрования.

Двумя широко используемыми методами шифрования являются шифрование с симметричным ключом и шифрование с открытым ключом. При шифровании с симметричным ключом и отправитель, и получатель используют один и тот же ключ, необходимый для шифрования данных [1]. На сегодняшний день разработаны различные алгоритмы для описания криптографии с симметричным ключом, такие как AES, DES, 3DES, Blowfish и другие. Недостатком таких методов являет недостаточный уровень безопасности, поскольку отправитель и получатель используют один и тот же ключ (закрытый ключ) через незащищенные каналы [2]. Это может привести к легкому обнаружению ключей шифрования и дешифрования.

Криптография с асимметричным ключом известна как криптография с открытым ключом. В шифровании с открытым ключом используются два разных, но математически связанных ключа. В этом случае обеспечивается лучшая аутентификация. Существуют различные алгоритмы для реализации этого механизма шифрования. Это RSA, Diffie-Hellman, ECC (криптография на эллиптических кривых) и алгоритм цифровой подписи [3].

Криптография на эллиптических кривых (ECC) является одним из эффективных криптографических алгоритмов с асимметричным ключом, который зависит от того, что отправитель использует ключ, отличный от закрытого ключа получателя, и каждая сторона генерирует открытый и секретный ключ отдельно после согласования параметров области эллиптической кривой [4, 5].

Шифрование на основе RSA с большим модулем и, соответственно, большим ключом, позволяет также надежно сохранять данные.

Материал и методы. В качестве компьютерной системы для организации процесса автоматизации процесса реализации алгоритма шифрования выбрана система Wolfram Mathematica.

Результаты и их обсуждение. Рассмотрим реализацию алгоритма шифрования в системе Wolfram Mathematica.

Система позволяет работать с большим объемом данных и быстро их обрабатывать [6].

В начале подключаем кодировщик данных с помощью следующей команды:

```
enc=NetEncoder["UTF8"].
```

Вывод набора первых последовательных простых чисел может быть получен с помощью следующей команды:

```
Table[Prime[n],{n,20}].
```

Выбираем два простых числа из списка p=59, q= 61. Находим их произведение max=pq. Вычисляем функцию Эйлера fi=(p-1)(q-1). В этом случае ее значение для данных чисел равно 3480.

Выбираем простое его не превосходящее: pub=1223.

Находим обратное ему число по модулю: priv=ModularInverse[1223,3480].

Зашифруем следующее сообщение:

t=enc["The square on the hypotenuse is equal to the sum of the squares on the other two sides"]

Числовая запись его выглядит следующим образом:

{85,105,102,33,116,114,118,98,115,102,33,112,111,33,117,105,102,33,105,122,113,112,117,102,111,118,116,102,33,106,116,33,102,114,118,98,109,33,117,112,33,117,105,102,33,116,118,110,33,112,103,33,117,105,102,33,116,114,118,98,115,102,116,33,112,111,33,117,105,102,33,112,117,105,102,115,33,117,120,112,33,116,106,101,102,116}

Шифруем его следующим образом согласно алгоритму RSA:

For[i=1,i<=Length[t2],i++,t2[[i]]=Nest[Mod[# t[[i]],max]&,t[[i]],pub-1]]

Функция Nest позволяет применить одну и ту же функцию конечное число раз.

Получатель может расшифровать данные следующим образом:

For[i=1,i<=Length[t2],i++,t3[[i]]=Nest[Mod[# t2[[i]],max]&,t2[[i]],priv-1]].

Заключение. Процесс шифрования является очень важным вопросов в задачах прикладной информатики, он позволяет обеспечить сохранность данных и упростить процесс ее дешифровки.

1. Khan, M.A. A new hybrid technique for data encryption / M.A. Khan, K.K. Mishra, N. Santhi, J. Jayakumari // Global Conference on Communication Technologies 23– 24 April 2015. – P. 925–929.

2. Alese, B.K. Comparative analysis of public-key encryption schemes / B.K. Alese, E.D. Philemon, S.O. Falaki // International Journal of Engineering and Technology. – 2012. – Vol. 2, №9. – P. 1552–1568.

3. Boato, G. Multimedia asymmetric watermarking and encryption / G. Boato, N. Conci, V. Conotter, F.G.B. De Natale, C. Fontanari// Institute of Electrical and Electronics Engineers University. – 2008. – Vol. 44, №9. – P. 601–603.

4.Bokhari, M.U. A Review on Symmetric Key Encryption Techniques in Cryptography/ M.U. Bokhari, Q.M. Shallal // International Journal of Computer Applications. – 2016. – Vol. 147, №10. – P. 43–48.

5. Darrel, H. Guide to elliptic curve cryptography // Springer-Verlag Professional Computing Series, 2004. – P. 1–311.

6. Прикладная математика. Применение Wolfram Mathematica для шифрования данных [Электронный ресурс] / БНТУ, Кафедра «Инженерная математика»; сост.: М.А. Гундина, Н.А. Кондратьева. – Минск: БНТУ, 2020.