теплового потока и коэффициента теплопроводности композита с включениями в виде сфер и многогранников с учетом термосопротивления границы раздела для различной толщины покрытия из вольфрама. Сделано сопоставление указанных параметров с расчетом по формулам, полученным в рамках микромеханической модели Такаянаги, гипотезы составного включения и эквивалентной матрицы, показавшее достаточно хорошее совпадение аналитических и конечноэлементных оценок.

Исследование поддержано БРФФИ (Т22КИ-032 «Эволюция микроструктуры и стабильность термических свойств композитов алмаз/алюминий при термоциклировании)».

Список литературы

1 Finite Element Analysis of the Effect of Particle Shape on the Thermal Conductivity in Diamond/Cu Composites / H. Guo [et al.] // Materials Science Forum. – 2014. – Vol. 788. – P. 689–692. – DOI: 10.4028/ www.scientific.net/msf.788.689.

2 **Шилько, С. В.** Математическое моделирование процесса теплопередачи и термонапряженного состояния в металло-алмазных композитах / С. В. Шилько, Д. А. Черноус // Математическое моделирование и биомеханика в современном университетете : тез. докл. XVI Всерос. школы (Дивноморское, 26 – 31 мая 2022 г.). – Ростов-н/Д ; Таганрог : ЮФУ, 2022. – С. 102.

УДК 51+004

РЕАЛИЗАЦИЯ НЕКОТОРЫХ АЛГОРИТМОВ ШИФРОВАНИЯ В WOLFRAM MATHEMATICA

О. В. ЮХНОВСКАЯ, М. А. ГУНДИНА
Белорусский национальный технический университет, г. Минск

Проблема сохранности данных не утрачивает своей актуальности. Методы криптографической защиты находят свое применение в системах управления на транспорте. Суть шифрования заключается в следующем. Вначале 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 др. Недостатком таких методов является низкий уровень безопасности, поскольку отправитель и получатель используют один и тот же ключ (закрытый) 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. Существуют различные алгоритмы для реализации этого механизма шифрования: RSA, Diffie-Hellman, ECC (криптография на эллиптических кривых) и алгоритм цифровой подписи [3].

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

Рассмотрим реализацию алгоритма шифрования в системе Wolfram Mathematica.

Вначале 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 число, 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 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]].

Шифр Цезаря входит в класс шифров, называемых «подстановка» или «простая замена». Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация. Пример реализации шифрования в Wolfram Mathematica выглядит следующим образом: StringReplace["Квадрат гипотенузы равен сумме квадратов катетов",{"а"->"г","б"->"д",…,"э"->"а","ю"->"б","я"->"в"}]

Процесс шифрования является очень важным вопросом в задачах прикладной информатики. Он позволяет обеспечить сохранность данных и упростить процесс ее дешифровки.

Список литературы

1 A new hybrid technique for data encryption / M. A. Khan [et al.] // 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, no. 9. – P. 1552–1568.

3 Multimedia asymmetric watermarking and encryption / G. Boato [et al.] // Institute of Electrical and Electronics Engineers University. – 2008. – Vol. 44, no. 9. – P. 601–603.