Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Эффективные алгоритмы в криптографии

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Андриянова Алексея Юрьевича

Научный руководитель

профессор, д.ф.-м.н. _____ В.А. Молчанов

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Понятие эффективного алгоритма постепенно формировалось и к 1970 году его определяли, как детерминированный или рандомизированный алгоритм, время которого полиномиально зависит от размера исходных данных [1], [2]. Данный вид алгоритмов применяется для решения многих задач, в том числе криптографических. Но в комбинаторике, теории графов, криптографии и многих других науках существуют трудноразрешимые задачи — задачи, у которых нет известных полиномиальных алгоритмов решения. Алгоритмы с субэкспоненциальной временной сложностью не подходят под классическое определение эффективных алгоритмов, но их можно считать эффективными по отношению к другим алгоритмам с экспоненциальной сложностью. Например, подобрать ключ шифрования намного быстрее, если использовать дополнительные сведения или предположения, хотя такой перебор все равно будет экспоненциальным по сложности.

Машина Тьюринга является основой теории алгоритмов, позволяет ввести понятие алгоритма и вычислимой функции, определить классы временной сложности, которые важны для криптографии.

Целью дипломной работы является изучение вероятностных алгоритмов: их классификация, компьютерная реализация таких алгоритмов, проведение различных тестов разработанной программы.

Дипломная работа состоит из введения, трех разделов, заключения, списка использованных источников и двух приложений. Общий объем работы — 67 страниц, из них 43 страницы — основное содержание, включая 16 рисунков и 10 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы вводятся основные понятия теории сложности вычислений.

В подразделе 1.1 описывается детерминированная машина Тьюринга [3], вводятся понятия массовой задачи [4], распознаваемого языка, временной сложности алгоритма [1].

В подразделе 1.2 описывается недетерминированная и вероятностная машины Тьюринга, вводится понятие полиномиального времени, класса $\mathcal{P}$, $\mathcal{NP}$ и $\mathcal{PP}$ [1].

Подраздел 1.3 содержит примеры рандомизированных алгоритмов и описание следующих подклассов вероятностных языков из работы [1]:

1) $\mathcal{ZPP}$ (сокращение от названия «полиномиальные вероятностные алгоритмы с нулевой ошибкой»);
2) $\mathcal{PP}$(Монте-Карло);
3) $\mathcal{PP}$(Лас-Вегас);
4) $\mathcal{BPP}$ (сокращение от названия «вероятностные полиномиальные алгоритмы с ограниченной вероятностью ошибки»).

Во втором разделе представлены подробные описания известных рандомизированных алгоритмов из работ [8] и [12]:

a) проверки чисел на простоту, а именно:
    1) тест простоты на основе малой теоремы Ферма;
    2) тест Соловея-Штрассена;
    3) тест Миллера-Рабина;
    4) тест Фробениуса;
b) факторизации чисел, а именно:
    1) ρ-метод Полларда;
    2) $(p-1)$-метод Полларда;
    3) метод Диксона.

Подраздел 2.5 также содержит теорему под названием «Парадокс дней рождения» и её доказательство из работы [8]. Данная теорема используется для оценки временной сложности и вероятности успеха (нахождения разложения числа) алгоритма.

В третьем разделе представлен разработанный на языке Java программный продукт, реализующий вероятностные тесты чисел на простоту и факторизацию составных чисел. Так же приведены результаты некоторых тестов компьютерных реализаций рассмотренных алгоритмов.

Подраздел 3.1 содержит результаты тестов полиномиальных вероятностных алгоритмов в виде таблиц и скриншотов работы программы. К полиномиальным вероятностным алгоритмам относятся тесты простоты чисел, которые входят в подкласс $\mathcal{PP}$(Монте-Карло). Для оценки вероятности ошибки использовались составные числа:

- $90597 = 3 \times 13 \times 23 \times 101$ — число, содержащее много множителей;
- $3277 = 29 \times 113$ — псевдопростое число по основанию 2;
- $51983 = 229 \times 227$ — число, множители которого близки к значению корня числа;
- $13021 = 29 \times 449$ — псевдопростое число по основанию 5;
- $41041 = 7 \times 11 \times 13 \times 41$ — число Кармайкла.

Тест Ферма показал самое большое количество ошибок и самое медленное их уменьшение с возрастанием повторов в тесте. Тест Соловея-Штрассена лишен недостатков теста Ферма: способен эффективно распознавать числа Кармайкла, выдает меньшее количество ошибок и более быстрое их снижение при возрастании количества повторов в тесте. Тест Миллера-Рабина показал лучшие результаты, по сравнению с тестом Ферма и тестом Соловея-Штрассена. Особо стоит выделить, как быстро уменьшается количество ошибок с возрастанием количества повторов в тесте. Это связано с вероятностью успеха теста Миллера-Рабина, которая не меньше $3/4$ [8]. Тест Фробениуса имеет наименьшую

вероятность неправильного ответа (менее 7710^{-1} [13]) из представленных алгоритмов. Данный факт подтвердился на практике, все результаты запуска теста Фробениуса оказались верными. В подразделе 3.1 также представлены сравнительные графики результатов алгоритмов для разных чисел и графики зависимости числа ошибок от вида тестируемого числа для каждого алгоритма. Тест Ферма показал плохие результаты на псевдопростых числах по основанию 2, а хуже всего — на числах Кармайкла. Результаты для остальных видов составных чисел были удовлетворительны. Тест Соловея-Штрассена оказался лучше теста Ферма, но он также выдает относительно много ошибок для псевдопростых чисел по основанию 2 и чисел Кармайкла. Наименьшее количество ошибочных результатов было у теста Миллера-Рабина. Данный алгоритм хорошо распознает числа Кармайкла. Наибольшее количество ошибок тест Миллера-Рабина выдает для псевдопростых чисел.

В подразделе 3.2 описываются тесты экспоненциальных вероятностных алгоритмов, к которым относятся ρ-метод Полларда и $(p-1)$-метода Полларда. Результаты тестов содержаться в таблицах и графиках, результаты отдельных запусков программы представлены в виде скриншотов. ρ-метод показал хорошие результаты времени работы. Для тестов было выбрано число $2782118136041 \times 7352138821673$. $(p-1)$-методом Полларда не удалось разложить такие же большие числа, как и ρ-методом. Время работы $(p-1)$-метода сильно зависит от правильно выбранной величины базы разложения. В тестах использовалось число $224390955521 = 282019 \times 795659$. 795659 является сильным простым числом, так как $795658 = 2 \times 397829$, где 397829 — простое число.

В подразделе 3.3 описываются тесты субэкспоненциального вероятностного алгоритма — метода Диксона. Для тестов данного алгоритма факторизации числа были выбраны следующие составные числа $1142667233 = 33311 \times 34303$ и $90751 = 151 \times 601$. Результаты запусков программы представлены в таблицах и на скриншоте. В следующих тестах использовалось составное число $N = 79244063000239 = 7951667 \times 9965717$, $B =$

$e^{\frac{1}{2}\ln N \ln(\ln N)}$. По результатам очевидно, что слишком большие значения δ замедляют работу алгоритма.

ЗАКЛЮЧЕНИЕ

Вероятностные алгоритмы, как частный случай эффективных алгоритмов, широко используются в криптографии, они снижают до полиномиальной сложность решения некоторых задач и могут определять некоторую вероятность ошибки. Вероятностные алгоритмы используются в перспективной квантовой криптографии, например, в протоколе QKD.

В первом разделе дипломной работы рассмотрены основные понятия и определения теории сложности вычислений и классы вероятностной сложности, приведены примеры алгоритмов из соответствующих классов. Во втором разделе описаны важные рандомизированные алгоритмы, в том числе решение задачи факторизации целых чисел, на которой основана криптостойкость известных криптосистем. Приведены программные реализации этих алгоритмов и произведен анализ этих программ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мао, Венбо. Современная криптография: теория и практика [Электронный ресурс] / Венбо Мао ; пер. с англ Д. А. Клюшина. М. : Вильямс, 2005. 768 с. Загл. с экрана. Яз. рус.

2. Кузюрин, Н. Н. Эффективные алгоритмы и сложность вычислений. Учеб. пособие [Электронный ресурс] / Н. Н. Кузюрин, С. А. Фомин. М. : МФТИ, 2016. 369 с. Загл. с экрана. Яз. рус.

3. Хопкрофт, Д. Введение в теорию автоматов, языков и вычислений [Электронный ресурс] / Д. Хопкрофт, Р. Мотвани, Д. Ульман ; пер. О. И. Васылык [и др.]. 2-е изд. М. : Вильямс, 2002. 528 с. Загл. с экрана. Яз. рус.

4. Гэри, М. Вычислительные машины и труднорешаемые задачи [Электронный ресурс] / М. Гэри, Д. Джонсон ; пер. А. Фридман. М. : Мир, 1982. 420 с. Загл. с экрана. Яз. рус.

5. Кормен, Т. Алгоритмы. Построение и анализ [Электронный ресурс] / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн ; пер. с англ. Н. Ореховой [и др.] под ред. И. Красикова. 2-е изд. М. : Вильямс, 2012. 1296 с. Загл. с экрана. Яз. рус.

6. Singh, H. Quantum key distribution protocols: A review [Электронный ресурс] / H. Singh, D. L. Gupta, A. K. Singh // IOSR Journal of Computer Engineering. 2014. Vol. 16. P. 1-9. Загл. с экрана. Яз. англ.

7. Кронберг, Д. А. Квантовая криптография. Учеб. пособие [Электронный ресурс] / Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Чернявский. М. : Изд-во МГУ им. Ломоносова, 2006. 112 с. Загл. с экрана. Яз. рус.

8. Глухов, М. М. Введение в теоретико-числовые методы криптографии: учеб. пособие [Электронный ресурс] / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. СПб. : Лань, 2011. 400 с. Загл. с экрана. Яз. рус.

9. Granville, A. Primality testing and Carmichael numbers [Электронный ресурс] / A. Granville // Notices of the American Mathematival Society. 1992. Vol. 39. P. 696-700. Загл. с экрана. Яз. англ.

10. Solovay, R. A fast Monte-Carlo test for primality [Электронный ресурс] / R. Solovay, V. Strassen // SIAM Journal on Computin. 1977. Vol. 6. P. 84-86. Загл. с экрана. Яз. англ.

11. Grantham, J. Frobenius pseudoprimes [Электронный ресурс] / J. Grantham // Mathematics of Computation. 2000. Vol. 70. P. 873-891. Загл. с экрана. Яз. англ.

12. Seysen, M. A simplified quadratic frobenius primality test [Электронный ресурс] / M. Seysen // Cryptology ePrint Archive. 2005. P. 4-13. Загл. с экрана. Яз. англ.

13. Grantham, J. A probable prime test with high confidence [Электронный ресурс] / J. Grantham // Journal of Number Theory. 1998. Vol 72. P. 32-47. Загл. с экрана. Яз. англ.

14. Коблиц, Н. Курс теории чисел и криптографии [Электронный ресурс] / Н. Коблиц ; пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова. М. : Научное изд-во ТВП, 2001. 254 с. Загл. с экрана. Яз. рус.

15. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] / О. Н. Василенко. М. : МЦНМО, 2003. 328 с. Загл. с экрана. Яз. рус.

16. Dixon, J. D. Asymptotically fast factorization of integers [Электронный ресурс] / J. D. Dixon // Mathematics of Computation. 1981. Vol. 36. P. 255-260. Загл. с экрана. Яз. англ.

17. Кнут, Д. Искусство программирования. В 2 т. Т. 2. Получисленные алгоритмы [Электронный ресурс] / Д. Кнут. ; пер. В. Тертышный. М. : Вильямс, 2001. 832 с. Загл. с экрана. Яз. рус.

18. Маховенко, Е. Б. Теоретико-числовые методы в криптографии: учеб. пособие [Электронный ресурс] / Е. Б. Маховенко. М. : Гелиос АРВ, 2006. 320 с. Загл. с экрана. Яз. рус.

19. Arora, S. Computational complexity: A modern approach [Электронный ресурс] / S. Arora, B. Barak. New York : Cambridge University Press, 2009. 594 p. Загл. с экрана. Яз. англ.

20. Pollard, J. M. Theorems on factorization and primality testing [Электронный ресурс] / J. M. Pollard // Proceeding of the Cambridge Philosophical Society. 1974. Vol. 76. P. 521-528. Загл. с экрана. Яз. англ.