

ТЕОРИЯ ЧИСЕЛ В КРИПТОГРАФИИ

*Допущено Учебно-методическим объединением вузов
по университетскому политехническому образованию
в качестве учебного пособия
для студентов высших учебных заведений, обучающихся
по направлению «Информатика и вычислительная техника»*



Москва 2011

УДК 511:003.26 (075.8)
ББК 22.18
Т 33

Авторы:

В.А. Орлов, Н.В. Медведев,
Н.А. Шимко, А.Б. Домрачева

Рецензенты:

д-р физ.-мат. наук, проф. *В.К. Леонтьев*;
д-р техн. наук, проф. *Е.Е. Тимонина*,

Теория чисел в криптографии : учеб. пособие / В. А. Ор-
Т 33 лов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева. – М. :
Изд-во МГТУ им. Н. Э. Баумана, 2011. – 223, [1] с.

ISBN 978-5-7038-3520-3

Изложены основы математического аппарата, используемого в современной криптографии; показано его применение при анализе криптосистем и выборе их параметров. Особое внимание уделено вопросам построения криптосистем с открытым ключом. Описание большинства рассмотренных алгоритмов приведено в виде программ на языке программирования Си.

Пособие соответствует курсам лекций, которые авторы читают в МГТУ им. Н.Э. Баумана и в МФТИ.

Для студентов и аспирантов, изучающих дисциплины по информационной безопасности.

УДК 511:003.26 (075.8)
ББК 22.18

ISBN 978-5-7038-3520-3

© Оформление. Издательство
МГТУ им. Н. Э. Баумана, 2011

ПРЕДИСЛОВИЕ

Цель учебного пособия – ознакомить читателей с основами математического аппарата, используемого в современной криптографии, и продемонстрировать его применение при анализе криптосистем и выборе их параметров.

Материал изложен в соответствии со стандартом дисциплины «Теоретико-числовые методы в криптографии» специальности «Компьютерная безопасность».

Пособие состоит из семи глав.

В криптографии важную роль играют простые числа. В главе 1 рассмотрены основы теории делимости. Приведены простые (с методической точки зрения) алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. Рассмотрены алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. Показаны области использования непрерывных дробей в криптографии. Описаны важнейшие функции теории чисел, в том числе широко используемая в криптографии функция Эйлера.

Важнейшим разделом теории чисел в современной криптографии является теория сравнения. В главе 2 доказаны важные для криптографии с открытым ключом теоремы Ферма и Эйлера о свойстве операции возведения в степень по заданному модулю. Исследовано нахождение решений сравнений первой степени и систем таких сравнений. В частности, доказана широко используемая в современной криптографии Китайская теорема об остатках. Приведены алгоритмы нахождения символов Лежандра и Якоби, значения которых позволяют решить вопрос о разрешимости сравнений второй степени по простому модулю.

В современной криптографии объектами преобразований являются не только вычеты по простому модулю, но и более слож-

ные образования – конечные поля. В главе 3 рассмотрены основные свойства конечных полей. Для облегчения усвоения материала вначале даны более простые математические понятия.

Оценки сложности алгоритмов, реализующих криптопреобразования, и алгоритмов, используемых для нахождения параметров криптосистем, исследованы в главе 4. В основном в пособии критерием сложности алгоритма является число используемых для его реализации двоичных операций.

При построении современных криптосистем требуются очень большие простые числа. Например, в криптосистеме RSA и различных системах, основанных на задаче дискретного логарифмирования в конечных полях, используются «случайные» простые числа, записи которых в десятичной системе счисления состоят из сотен цифр. В главе 5 доказана теорема Чебышева о доле простых чисел и приведены другие результаты о распределении простых чисел в натуральном ряде. Затем определены различные понятия псевдопростоты числа.

Вопросы применения теоретико-числовых методов в криптографии рассмотрены в главе 6. На содержательном уровне описаны основные проблемы и понятия криптографии. В традиционной криптографии довольно часто используют преобразование $y = ax + b \pmod{m}$, которое называют линейным. Рассмотрено использование таких преобразований для генерации псевдослучайных последовательностей.

Исследованы проблемы криптографии с открытым ключом и математический аппарат, на котором основана современная криптография, – односторонние функции. Проведен анализ криптосистем Эль-Гамала и Рабина.

Подробный анализ широко используемой криптосистемы RSA приведен в главе 7.

Изучение курсов по информационной безопасности предполагает проведение практических занятий. В связи с этим в пособии даны тексты программ, реализующих рассмотренные алгоритмы. Приведенные программы написаны на языке программирования Си.

Решение предлагаемых в пособии упражнений поможет более глубокому усвоению изложенного материала.

В заключение отметим, что защита информации (особенно с использованием криптографии) является наиболее наукоемким

разделом информатики. В связи с этим читатель должен приложить усилия при освоении изложенного материала.

При написании пособия использован опыт преподавания ряда дисциплин по информационной безопасности в МФТИ (ТУ) (Московском физико-техническом институте) и в МГТУ им. Н.Э. Баумана.

Глава 3 написана Н.А. Шимко, глава 5 – Н.В. Медведевым, А.Б. Домрачевой, остальные главы написаны В.А. Орловым.

Авторы выражают благодарность В.А. Конявскому, М.П. Сычеву, А.С. Кузьмину за замечания, высказанные при подготовке учебного пособия.

ВВЕДЕНИЕ

Наибольший практический интерес представляет защита информации, находящейся в компьютере, с использованием программного обеспечения.

При компьютерной обработке информация представляется в виде наборов из 0 и 1 (двоичных наборов). Каждому такому набору ставится в соответствие натуральное число, запись которого в двоичной системе счисления (двоичная запись) совпадает с этим набором. Таким образом, компьютерная обработка информации сводится к обработке натуральных чисел.

В современной криптографии сообщения представляются символами некоторого конечного алфавита (или последовательностями таких символов). Этим символам ставятся в соответствие числа от 0 до $N - 1$, где N – число элементов (мощность) алфавита. Поэтому шифрование и расшифровывание сообщений представляют собой преобразование натуральных чисел, меньших N . Разделом математики, предметная область которого – натуральные числа, является теория чисел.

Таким образом, современная криптография связана с использованием результатов теории чисел, имеющей долгую историю развития. Ввиду конечности алфавитов сообщений важную роль играет раздел теории чисел – сравнения, в котором числа, имеющие одинаковые остатки от деления на фиксированное число (модуль), считаются одинаковыми. В качестве модуля естественно выбрать мощность алфавита сообщений.

В традиционной криптографии с несложными преобразованиями (простая замена, перестановка, гаммирование), не было необходимости применять глубокие результаты теории чисел. Ситуация изменилась с появлением криптосистем с открытым ключом, в основе которых лежат односторонние преобразования, например операция возведения в степень по огромным модулям.

Аргументом преобразования шифрования является открытое сообщение, а функцией – зашифрованное сообщение (криптограмма).

Авторами криптосистем с открытым ключом были американские ученые У. Диффи и М. Хеллман. Однако впервые она была реализована в виде системы RSA, название которой образовано начальными буквами фамилий авторов: Р. Райвест, А. Шамир, Л. Адлеман.

В криптосистеме RSA используется степенная функция

$$y = x^e \pmod{N}.$$

При этом возникает задача выбора модуля N и степени e , таких, что существует степень d , удовлетворяющая условию

$$y^d = x \pmod{N}$$

для любого $0 \leq x \leq N - 1$. Кроме того, алгоритм вычисления по N и e степени d должен иметь очень большую сложность.

Диффи и Хэллман предложили использовать показательную функцию

$$y = a^x \pmod{N}.$$

В этом случае актуальна задача о подборе параметров a и N , обеспечивающих взаимную однозначность этой функции. Кроме того, алгоритм вычисления по N , a и y аргумента x должен иметь очень большую сложность.

В криптографии важную роль играет умение строить алгоритмы, реализующие достаточно сложные преобразования и имеющие малую сложность. В пособии эти вопросы рассмотрены подробно.

В современной криптографии обеспечение конфиденциальности информации является самой простой задачей. Более сложной является, например, задача подписания электронного сообщения, придающая сообщению статус документа. С использованием криптосистемы RSA эта задача решается следующим образом.

Для простоты изложения рассмотрим процедуру подписания сообщения, оставляя в стороне обеспечение его конфиденциальности. Пользователям, которые могут проверить подпись, числа N и e известны. Им посылается сообщение $M \parallel M^d \pmod{N}$, где M – сообщение, а через \parallel обозначена операция конкатенации (присоединения). Проверяющий вычисляет значение выражения $(M^d \pmod{N})^e \pmod{N}$ и в случае совпадения этого значения с M признает подпись подлинной. Напомним, что нахождение по N и e степени d требует очень много времени.

Недостатком описанной процедуры являются большие накладные расходы (размер подписи равен размеру подписываемого сообщения). Для устранения этого недостатка используют криптографические хэш-функции, при построении которых используются также теоретико-числовые методы.

Конечно, при создании криптосистем важную роль играет теория вероятностей. Мы должны оценить вероятность того, что случайно выбранное число совпадет, например, со степенью расширения в криптосистеме RSA. В пособии использованы только общеизвестные результаты теории вероятностей.

Информация может являться очень ценным продуктом, в этом случае ее защита весьма актуальна. Как известно, защиту информации можно осуществить двумя способами: ограничить доступ к неизменяемой информации или преобразовать информацию известным только законным пользователям способом (зашифровать). В современных условиях глобализации бизнеса информацию приходится передавать по незащищенным каналам связи и второй способ имеет несомненное преимущество.

В пособии рассмотрены теоретико-числовые методы, используемые при создании современных систем защиты конфиденциальной информации. Особое внимание уделено вопросам построения криптосистем с открытым ключом. Эти криптосистемы помимо стойкой защиты данных от попыток ознакомления с ними позволяют решать более сложные задачи: проверку целостности данных, установление источника сообщений (аутентификация) и, таким образом, невозможность отказа от авторства сообщения (цифровая подпись). Цифровая подпись играет важную роль в обеспечении надежного оборота электронных документов.

ГЛАВА 1. ОСНОВЫ ТЕОРИИ ДЕЛИМОСТИ

Рассмотрены целые числа и свойства операций над этими числами.

Определены простые числа, играющие важную роль в криптографии. Сформулирована фундаментальная теорема арифметики об однозначном представлении целого числа в виде произведения простых чисел. Рассмотрены простые алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа.

Приведены понятия наибольшего общего делителя и наименьшего общего кратного множества чисел и важное в криптографии понятие взаимной простоты чисел. Даны алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел.

Определено представление действительных чисел в виде непрерывных дробей и рассмотрены свойства непрерывных дробей. Показаны области использования непрерывных дробей в криптографии.

Рассмотрены важнейшие функции теории чисел, в том числе широко используемая в криптографии функция Эйлера.

1.1. Основные понятия и теоремы

Под числом, если не оговорено иное, будем понимать *целое* число, т. е. натуральное число (положительное целое), нуль и натуральное число со знаком минус (отрицательное целое).

Сумма, разность и произведение двух целых чисел являются целыми числами. Частное от деления двух целых чисел (делитель отличен от нуля) может быть как целым, так и нецелым.

Если частное от деления a на b – целое число, то, обозначая его через c , получаем $a = bc$. В этом случае говорят, что a делится на b или b делит a .

Отметим, что теорема 1.29 используется далее для доказательства некоторых свойств объекта современной криптографии – конечных полей.

Контрольные задания и вопросы

1. Сформулируйте фундаментальную теорему арифметики.
2. В чем состоит вклад П.Л. Чебышева в теорию чисел?
3. Опишите алгоритм факторизации длинных целых чисел.
4. В чем состоит преимущество бинарного алгоритма Евклида?
5. Расскажите о свойствах наибольшего общего делителя двух чисел.
6. Приведите свойства непрерывных дробей.
7. Опишите каноническое разложение произведения $n!$.
8. Дайте определение мультипликативной функции и приведите примеры таких функций.
9. Дайте определение функции Эйлера и приведите формулы для нахождения ее значения.

Упражнения

1. Сумма квадратов двух целых чисел кратна n . Доказать, что при $n = 3$ сумма этих чисел также кратна 3. Проверить справедливость аналогичного утверждения при $n = 5, 7$.
2. Доказать, что любое натуральное число, десятичная запись которого состоит из одной 1, двух 2, трех 3 и четырех 4, не является полным квадратом.
3. Доказать, что при простом $n > 3$ число $n^2 - 1$ делится на 24. Вывести необходимое и достаточное условие того, что $n^2 - 1$ делится на 24.
4. Сколько делителей имеет число 945? Перечислить их все.
5. Пусть n – положительное нечетное число. Доказать, что существует взаимно однозначное соответствие между делителями нечетного числа n , меньшими \sqrt{n} , и делителями, большими \sqrt{n} .
6. Доказать, что существует взаимно однозначное соответствие между множеством делителей числа n , не меньших \sqrt{n} , и множеством представлений n в виде разности квадратов двух неотрица-

тельных целых чисел. Например, 15 имеет два делителя 5, 15, которые не меньше $\sqrt{15}$, и $15 = 4^2 - 1^2 = 8^2 - 7^2$. Указать все возможные способы записи числа 945 в виде разности квадратов двух неотрицательных целых чисел.

7. Найти максимальное число простых делителей в каноническом разложении числа, меньшего 2^{32} (каждый делитель считается один раз).

8. Найти степени чисел 2, 3, 5, 7 в каноническом разложении $100!$.

9. Пусть $S_q(n)$ означает сумму цифр числа n в q -ичной системе счисления. Доказать, что степень числа 2, точно делящая $n!$, равна $n - S_2(n)$. Вывести аналогичную формулу для любого простого делителя числа n .

10. Найти НОД(360, 294) двумя способами: разложением обоих чисел на простые множители и с помощью алгоритма Евклида.

11. С помощью алгоритма Евклида найти НОД для следующих четырех пар чисел и выразить его как линейную комбинацию этих чисел с целыми коэффициентами: а) 26, 19; б) 187, 34; в) 841, 160; г) 2 613, 2 171.

12. Разложить в непрерывную дробь $\alpha = \frac{125}{92}$.

13. Найти $\varphi(5\,040)$.

14. Написать программу разложения обыкновенной дроби в непрерывную дробь.

ГЛАВА 2. СРАВНЕНИЯ

Рассмотрены важнейший для криптографии раздел теории чисел – сравнения, а также основные свойства числовых сравнений.

Введено понятие систем вычетов и исследованы их свойства.

Доказаны важные для криптографии с открытым ключом теоремы Ферма и Эйлера о свойстве операции возведения в степень по заданному модулю.

Приведены сравнения первой степени и системы таких сравнений. В частности, доказана широко используемая в современной криптографии Китайская теорема об остатках.

Рассмотрены сравнения второй степени, которые используются в криптографии для решения проблемы факторизации громадных чисел. Приведены алгоритмы нахождения символов Лежандра и Якоби, значения которых позволяют решить вопрос о разрешимости сравнений второй степени по простому модулю.

2.1. Свойства сравнений

Рассмотрим классификацию целых чисел по их остаткам от деления на заданное положительное число m , которое называют *модулем*. Числа, имеющие одинаковый остаток, относят к одному классу и называют *сравнимыми по модулю m* .

Сравнимость чисел a и b по модулю m записывается следующим образом: $a \equiv b \pmod{m}$ (читается: a сравнимо с b по модулю m).

Теорема 2.1. *Сравнимость чисел a и b по модулю m равносильна возможности представления $a = b + mt$, где t – целое.*

Доказательство. Из $a \equiv b \pmod{m}$ следует, что

$$a = mk_1 + r, \quad b = mk_2 + r, \quad 0 \leq r < m.$$

Отсюда

```
puts("Вычисление символа Якоби.");
puts("Введите n и m!");
scanf("%ul %ul", &n, &m);
res = yakoby(n, m);
printf("Символ Якоби(%ld/ %ld) = %d \n", n,
m, res);
ch = getchar(); /*Для сохранения изображения
на экране*/
ch = getchar();
putchar(ch);
}
```

Отметим, что алгоритм вычисления квадратного корня по простому модулю рассмотрен в 4.4.

Контрольные задания и вопросы

1. Сформулируйте свойства сравнений, аналогичные свойствам равенств.
2. Приведите примеры полных систем вычетов.
3. Дайте определение и приведите примеры приведенных систем вычетов.
4. Может ли полная система вычетов совпадать с приведенной системой вычетов (по одному модулю)?
5. Сформулируйте малую теорему Ферма и теорему Эйлера.
6. Дайте определение обобщенной функции Эйлера.
7. Расскажите о вычислении решений сравнений первой степени с использованием непрерывных дробей.
8. Расскажите о вычислении решений сравнений первой степени с использованием расширенного алгоритма Евклида.
9. Сформулируйте Китайскую теорему об остатках.
10. Дайте определение квадратичного вычета.
11. Сформулируйте свойства символа Лежандра.

12. В чем заключается закон взаимности квадратичных вычетов?
13. Опишите алгоритм нахождения символа Якоби.

Упражнения

1. Найти значения обобщенной функции Эйлера от 561, 1105 и 5040.
2. Доказать, что при взаимно простых a и m сравнение $ax \equiv b \pmod{m}$ имеет решение $x \equiv ba^{\varphi(m)-1} \pmod{m}$.
3. Решить сравнение $256x \equiv 179 \pmod{337}$, используя непрерывные дроби.
4. Решить сравнение $1215x \equiv 560 \pmod{2755}$, используя расширенный алгоритм Евклида.
5. Решить систему сравнений: $2x \equiv 1 \pmod{3}$, $3x \equiv 4 \pmod{5}$, $x \equiv 2 \pmod{7}$, $4x \equiv 9 \pmod{11}$, $7x \equiv 3 \pmod{13}$.
6. Показать, что число 2 является квадратичным вычетом по простым модулям вида $8m + 1$.
7. Найти все m , при которых число 3 является квадратичным невычетом по простым модулям вида $8m + 1$.
8. Выполнить задание п. 7 для чисел 5 и 7.
9. Используя программу 2.1, вычислить символ Якоби
$$\left(\frac{173\ 657}{4\ 239\ 781} \right).$$

ГЛАВА 3. КОНЕЧНЫЕ ПОЛЯ

В современной криптографии объектами преобразований являются не только вычеты по простому модулю, но и более сложные образования – конечные поля.

Рассмотрены основные свойства конечных полей. Для облегчения усвоения материала вначале даны более простые математические понятия.

3.1. Математические понятия, поясняющие понятие конечного поля

Множества и отношения

Для более адекватного понимания наиболее сложного объекта криптографических преобразований – *конечных полей* – напомним более простые понятия математики.

Под *множеством* понимают неупорядоченную совокупность различных элементов.

Кроме известных еще из школьной программы операций *объединения* и *пересечения* множеств рассмотрим *прямое (декартово) произведение* множеств. Декартово произведение $A \times B$ множеств A и B определяется как множество всех упорядоченных пар (x, y) , таких, что $x \in A$ и $y \in B$. Это определение записывают следующим образом:

$$A \times B = \{(x, y) \mid x \in A \text{ и } y \in B\}.$$

Через $|A|$ обозначают число элементов (*мощность*) конечного множества A . Нетрудно проверить, что для конечных множеств имеет место равенство $|A \times B| = |A| \cdot |B|$.

*Отношением между множествами A и B называется подмножество декартова произведения $A \times B$. В случае $B = A$ это отношение называется *отношением на множестве A* . Примером отношения на множестве \mathbf{Z} целых чисел является отношение*

Контрольные задания и вопросы

1. Перечислите свойства, которыми могут обладать отношения между множествами.
2. Перечислите дополнительные (к п. 1) свойства, которыми могут обладать отношения на множестве.
3. Дайте определение отношений эквивалентности, полного и частичного порядка.
4. Дайте определение бинарной операции на множестве и перечислите свойства, которыми она может обладать.
5. Сформулируйте определения группы и кольца.
6. Дайте определение поля.
7. Какие поля называются изоморфными?
8. Приведите примеры полей.
9. Дайте определение характеристики поля.
10. Запишите соотношение между порядком элемента конечного поля и мощностью этого поля.
11. Какую мощность может иметь конечное поле?
12. Дайте определение неприводимого многочлена.

Упражнения

1. Для $p = 2, 3, 5, 7, 11, 13, 17$ найти наименьшее положительное целое число, которое порождает \mathbf{F}_p^* , и определить, сколько среди чисел $1, 2, 3, \dots, p-1$ образующих.
2. Найти мощность наименьшего расширения \mathbf{F}_5 , содержащего все корни многочленов $X^2 + X + 1$ и $X^3 + X + 1$.
3. Для каждой степени $d \leq 5$ найти число всех нормированных неприводимых многочленов над \mathbf{F}_2 степени d и записать эти многочлены.
4. Для каждой степени $d \leq 6$ найти число всех нормированных неприводимых многочленов над \mathbf{F}_3 степени d и для $d \leq 3$ записать эти многочлены.
5. С помощью обобщения алгоритма Евклида на многочлены найти НОД(f, g) для $f, g \in \mathbf{F}_p[X]$ в каждом из следующих примеров. В каждом случае выразить НОД(f, g) как комбинацию f и g :
 - а) $f = X^3 + X + 1, g = X^2 + X + 1, p = 2$;
 - б) $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, g = X^4 + X^2 + X + 1, p = 2$;

- в) $f = X^3 - X + 1$, $g = X^2 + 1$, $p = 3$.
6. Вычислив НОД(f, g), найти все кратные корни $f(X) = X^7 + X^5 + X^4 - X^3 - X^2 - X + 1 \in \mathbf{F}_3[X]$ в его поле разложения.
7. Пусть $\alpha \in \mathbf{F}_{p^2}$ удовлетворяет уравнению $X^2 + aX + b = 0$, где $a, b \in \mathbf{F}_p$. Доказать, что α^p также удовлетворяет этому уравнению.
8. Для каждого из следующих полей \mathbf{F}_q , $q = p^n$, записать неприводимый многочлен с коэффициентами из простого поля, корень которого α был бы примитивным (т. е. порождал бы \mathbf{F}_q^*), и выписать все степени α в виде многочленов от α степени меньше n :
- а) \mathbf{F}_4 ; б) \mathbf{F}_8 .
9. Доказать, что если b – образующий элемент поля \mathbf{F}_q^* , $q = p^n$ и $d \mid n$, то $b^{(p^n-1)/(p^d-1)}$ – образующий элемент поля \mathbf{F}_r^* , где $r = p^d$.
10. Описать алгоритм выявления неприводимости многочленов степеней 2 и 3.

ГЛАВА 4. СЛОЖНОСТЬ РЕАЛИЗАЦИИ КРИПТОАЛГОРИТМОВ

Рассмотрены вопросы оценки сложности реализации криптографических преобразований (или их фрагментов) и алгоритмов выбора параметров криптосистем.

В качестве характеристики алгоритма выбрано число двоичных операций, использованных при его реализации (сложность алгоритма).

Сложность алгоритма, вообще говоря, зависит от способа представления данных. Как уже было отмечено ранее, в криптографических преобразованиях символам ставят в соответствие натуральные числа. В связи с этим проанализированы способы представления чисел.

Рассмотрены оценки сложности реализации арифметических операций. Затем на их основе получены оценки сложности алгоритмов, используемых при проектировании криптосистем.

4.1. Системы счисления

Основные понятия

Цифрами в математических дисциплинах принято называть символы, участвующие в записи числа. Под числом подразумевается его значение. Отметим, что обычно при работе с компьютером вводят *записи чисел*, а не сами числа.

Целью создания любой системы счисления является выработка наиболее удобного способа записи чисел, в частности, для простого и быстрого решения задач. Для удобства использования система счисления должна обладать следующими свойствами:

- простота способа записи числа на физическом носителе,
- удобство выполнения арифметических операций,
- наглядность обучения основам работы с числами.

25/ 3; 26/ (4, 3, 1); 27/ (5, 2, 1); 28 /1; 29/ 2; 30/ 1; 31/ 3;
32/ (7, 3, 2); 33/ 10; 34/ 7; 35/ 2; 36/ 9; 37/ (6, 4, 1);
38/ (6, 5, 1); 39/ 4; 40/ (5, 4, 3); 41/ 3; 42/ 7; 43/ (6, 4, 3);
44/ 5; 45/ (4, 3, 1); 46/ 1; 47/ 5; 48/ (11, 5, 1) 49/ 9;
50/ (4, 3, 2) 51/ (6, 3, 1); 52/ 3; 53/ (6, 2, 1); 54/ 9; 55/ 7;
56/ (7, 4, 2); 57/ 4; 58/ 19; 59/ (7, 4, 2); 60/ 1; 61/ (5, 2, 1);
62/ 29; 63/ 1; 64/ (11, 2, 1).

Число, выделенное полужирным шрифтом, означает степень многочлена. После символа «/» следует описание многочлена этой степени.

Контрольные задания и вопросы

1. Дайте определение q -ичной системы счисления.
2. Бывают ли позиционные системы счисления, отличные от q -ичных?
3. Опишите алгоритм перевода q -ичной записи числа в десятичную запись этого числа.
4. Оцените сложность алгоритма сложения двух k -битовых чисел.
5. Опишите «школьный» алгоритм умножения двух k -битовых чисел и оцените его сложность.
6. Опишите алгоритм умножения Карацубы.
7. Опишите алгоритм деления k -битового числа на r -битовое число и оцените его сложность.
8. Дайте определение полиномиального по сложности алгоритма и приведите примеры таких алгоритмов.
9. Приведите примеры алгоритмов, не являющихся полиномиальными по сложности.
10. Опишите алгоритмы Евклида и оцените их сложность.
11. На каких утверждениях основана корректность алгоритмов Евклида?
12. Оцените сложность нахождения решений сравнения первой степени.
13. Оцените сложность алгоритма нахождения символа Якоби.

14. Опишите алгоритм извлечения квадратного корня по простому модулю и оцените его сложность.

15. Оцените сложность алгоритма быстрого возведения в целую степень по модулю.

16. Каким образом представляются элементы конечных полей при компьютерной обработке? Оцените сложность алгоритма умножения таких элементов.

17. Опишите алгоритмы нахождения обратного элемента конечного поля и оцените их сложность.

Упражнения

1. Описать алгоритм перевода римской записи числа в его десятичную запись и алгоритм обратного перевода.

2. Описать алгоритм, отвечающий на вопрос: является ли запись в алфавите I, V, X, L, C, D и M римской записью числа?

3. Перемножить двоичные числа 101101 и 11001 и разделить 10011001 на 1011.

4. Используя обозначение O большое, оценить число двоичных операций при вычислениях в двоичной системе счисления: а) 3^n ; б) n^n ; в) N^n .

5. Для суммы квадратов первых n натуральных чисел справедлива формула

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Используя обозначение O большое, оценить число двоичных операций, требующихся для вычисления: а) левой части этого равенства; б) правой части.

6. Оценить число двоичных операций для проверки простоты числа n с помощью последовательного деления на все нечетные числа, не превосходящие \sqrt{n} .

7. Пусть n – большое целое число, записанное в двоичной системе счисления. Описать алгоритм вычисления $\lceil \sqrt{n} \rceil$ с использованием $O(\log^3 n)$ двоичных операций.

ГЛАВА 5. НАХОЖДЕНИЕ ОЧЕНЬ БОЛЬШИХ ПРОСТЫХ ЧИСЕЛ

Для построения современных криптосистем необходимы очень большие простые числа. Например, в системе RSA и различных системах, основанных на задаче дискретного логарифмирования в конечных полях, требуются «случайные» простые числа, записи которых в десятичной системе счисления состоят из сотен цифр.

Доказана теорема Чебышева о количестве простых чисел, не превосходящих заданного числа. Кроме того, без доказательства приведены некоторые утверждения о распределении простых чисел. Введены понятия псевдопростых, эйлеровых псевдопростых и сильно псевдопростых чисел. На основе этих понятий описаны тесты на проверку простоты очень больших чисел.

5.1. Распределение простых чисел

Вначале рассмотрим вопросы распределения простых чисел в натуральном ряду. Напомним, что в главе 1 была доказана бесконечность множества простых чисел. Кроме того, справедливо следующее утверждение.

Теорема 5.1. *Для любого сколь угодно большого натурального числа k в натуральном ряду существует k последовательных составных чисел.*

Доказательство. Рассмотрим k последовательных чисел

$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k + 1.$$

Нетрудно проверить, что i -е число этой последовательности, $1 \leq i \leq k$, делится на $i + 1$. Таким образом, все эти числа являются составными.

Как было отмечено ранее, только в 1850 г. П.Л. Чебышев получил хорошую оценку доли простых чисел.

$$1) d = p; 2) d = q; 3) d = N; 4) d = 1.$$

Таким образом, с вероятностью 0,5 найдем нетривиальный делитель числа N .

На основе метода разности квадратов разработан самый быстрый из известных алгоритмов факторизации – *квадратичное решето в числовом поле*.

Контрольные задания и вопросы

1. Сформулируйте теорему Чебышева о количестве простых чисел.
2. Оцените количество простых чисел, не превосходящих 4 000 000 000.
3. Приведите формулу для асимптотической оценки значения $n!$.
4. Опишите асимптотический закон распределения простых чисел.
5. Сформулируйте утверждение о распределении простых чисел в арифметических прогрессиях.
6. Дайте определение псевдопростого числа.
7. Дайте определение числа Кармайкла.
8. Сформулируйте условия того, что данное число является числом Кармайкла.
9. Определите эйлеровы псевдопростые числа и опишите тест Соловея – Штрассена.
10. Дайте определение сильно псевдопростого числа и опишите тест Миллера – Рабина.
11. Как соотносятся между собой псевдопростые и эйлеровы псевдопростые числа?
12. Как соотносятся между собой сильно псевдопростые и эйлеровы псевдопростые числа?
13. Опишите метод разности квадратов в алгоритмах факторизации.

Упражнения

1. Доказать, что существует 36 оснований $b \in (\mathbf{Z}/91\mathbf{Z})^*$ (т. е. половина всех возможных оснований), для которых 91 – псевдопростое число.
2. Показать, что если p и $2p - 1$ – простые числа и $n = p(2p - 1)$, то n – псевдопростое число для половины возможных оснований b ,

а именно для тех b , которые являются квадратичными вычетами по модулю $2p - 1$.

3. Пусть n – нечетное составное натуральное число и $\text{НОД}(b, n) = 1$. Показать, что если p – простой делитель n и $m = n/p$, то n – псевдопростое число по основанию b только при $b^{m-1} \equiv 1 \pmod{p}$.

4. Доказать, что никакое целое число $n = 3p$ ($p > 3$ – простое число) не может быть псевдопростым по основаниям 2, 5 или 7.

5. Доказать, что никакое целое число $n = 5p$ ($p > 5$ – простое число) не может быть псевдопростым по основаниям 2, 3 или 7.

6. Пусть p – простое число. Показать, что p^2 – псевдопростое по основанию b тогда и только тогда, когда $p^{b-1} \equiv 1 \pmod{p^2}$.

7. Пусть $n = pq$ – произведение двух различных простых чисел и $d = \text{НОД}(p - 1, q - 1)$. Доказать, что n – псевдопростое число по основанию b в том и только в том случае, когда $b^d \equiv 1 \pmod{n}$. Выразить через d число различных оснований, по которым n псевдопростое.

8. Доказать, что существует бесконечно много псевдопростых чисел по основаниям 2, 3, 5.

9. Пусть m – натуральное число, такое, что $6m + 1$, $12m + 1$, $18m + 1$ – простые числа. Доказать, что $(6m + 1)(12m + 1)(18m + 1)$ является числом Кармайкла.

10. Показать, что следующие натуральные числа являются числами Кармайкла: $1105 = 5 \cdot 13 \cdot 17$; $1729 = 7 \cdot 13 \cdot 19$; $2465 = 5 \cdot 17 \cdot 29$; $2821 = 7 \cdot 13 \cdot 31$; $6601 = 7 \cdot 23 \cdot 41$; $29341 = 13 \cdot 37 \cdot 61$; $172081 = 7 \cdot 13 \cdot 31 \cdot 61$; $278545 = 5 \cdot 17 \cdot 29 \cdot 113$.

11. Найти все числа Кармайкла вида $3pq$ и $5pq$ (p, q простые).

12. Доказать, что 561 – наименьшее число Кармайкла.

13. Привести пример составного числа n и основания b , таких, что $b^{(n-1)/2} \equiv \pm 1 \pmod{n}$, однако n не есть эйлерово псевдопростое число по основанию b .

14. Доказать, что если n – псевдопростое число по основанию 2, то $N = 2^n - 1$ является сильно псевдопростым и эйлеровым псевдопростым по основанию 2.

15. Доказать, что существует бесконечно много сильно псевдопростых и эйлеровых псевдопростых чисел по основанию 2.

16. Показать, что 65 – сильно псевдопростое число по основанию 8 и по основанию 18, однако не является таковым по основанию $14 \equiv 8 \cdot 18 \pmod{65}$.

ГЛАВА 6. АНАЛИЗ КРИПТОСИСТЕМ

Рассмотрены вопросы применения теоретико-числовых методов в криптографии. На содержательном уровне описаны основные проблемы и понятия криптографии.

В традиционной криптографии довольно часто используют преобразование $y = ax + b \pmod{m}$, которое называют линейным. Показано использование таких преобразований для генерации псевдослучайных последовательностей.

Рассмотрены проблемы криптографии с открытым ключом и математического аппарата, на котором основана современная криптография – односторонние функции.

Проведен анализ криптосистем Эль-Гамала и Рабина

6.1. Введение в криптографию

Рассмотрим вопросы защиты данных на компьютерах и с использованием компьютеров. Существуют два принципиально различных подхода к защите конфиденциальной информации: ограничение доступа и шифрование. При использовании первого подхода информация не изменяется, а затрудняется доступ к ней, например, требуется знание паролей. При шифровании информация изменяется с использованием известного только законным пользователям способа. Доступ к зашифрованной информации, как правило, не ограничивается. Наука о шифровании называется *криптографией*.

Современная криптография рассматривает следующие проблемы информационной безопасности:

- обеспечение конфиденциальности,
- обеспечение целостности,
- обеспечение аутентификации,
- обеспечение невозможности отказа от авторства.

Четыре варианта расшифровывания

4 410, 5 851, 15 078, 16 519

получаются из формулы

$$s - \frac{B}{2} = s - \frac{12\,345}{2}.$$

Таким образом, можно сделать следующие выводы.

Шифрование с открытым ключом основано на использовании односторонних функций, примерами которых считаются факторизация чисел, извлечение корней по составному модулю, дискретное логарифмирование и задача Диффи – Хеллмана.

Соотношение сложностей решения этих задач можно выявить сведением одной задачи к другой.

Криптостойкость системы Эль-Гамала основана на трудности решения задачи Диффи – Хеллмана.

Криптостойкость алгоритма Рабина гарантируется сложностью извлечения корней по составному модулю. Поскольку эта задача полиномиально эквивалентна проблеме факторизации, можно считать, что безопасность системы Рабина обеспечивается сложностью разложения больших чисел на множители.

Контрольные задания и вопросы

1. Назовите два принципиально различных подхода к защите конфиденциальной информации на компьютере.
2. Дайте определение конфиденциальности информации.
3. Дайте определение целостности информации.
4. Дайте определение идентификации и аутентификации.
5. Дайте определение невозможности отказа от авторства.
6. Охарактеризуйте следующие методы шифрования информации: простая замена, перестановка, гаммирование.
7. Что представляет собой самый быстрый в настоящее время алгоритм разложения на множители?
8. В чем заключаются задачи факторизации, RSA и определения квадратичного вычета по составному модулю? Расположите эти задачи в порядке увеличения их сложности.

9. Сформулируйте проблему дискретного логарифмирования и задачу Диффи – Хеллмана. Расположите их в порядке увеличения сложности.

10. Хорошо или плохо, что в шифровании по алгоритму Эль-Гамала присутствует элемент случайности, обеспечивающий разные шифротексты при шифровании одного сообщения дважды?

11. Расскажите о двух преимуществах, которые система Рабина имеет перед RSA. Имеет ли алгоритм Рабина какие-либо недостатки?

Упражнения

1. Объяснить, почему при передаче большого числа данных наиболее приемлемый способ заключается в том, что сначала с помощью криптосистемы с открытым ключом передается секретный ключ, а потом с его помощью шифруются основные данные симметричным алгоритмом.

2. Показать, что вскрытие шифрующего алгоритма Рабина эквивалентно разложению натуральных чисел на множители.

ГЛАВА 7. КРИПТОСИСТЕМА RSA

Весьма подробно рассмотрена широко распространенная криптосистема с открытым ключом – криптосистема RSA. На примере этой криптосистемы показано применение почти всех рассмотренных нами понятий и методов теории чисел.

В полном объеме доказана корректность алгоритма RSA. Описан способ ускорения процедуры расшифровывания. Рассмотрены вопросы сопоставления сложностей взлома криптосистемы RSA и проблемы факторизации. Уделено внимание правильному выбору параметров криптосистемы. Описана достаточно сложная атака на криптосистему RSA – атака Винера.

Кроме того, предложены две учебные версии криптосистемы RSA, предназначенные для наглядного и более глубокого изучения проблем программной реализации этой криптосистемы.

7.1. Описание алгоритма RSA

RSA – наиболее популярная криптосистема с открытым ключом. Алгоритм RSA, первый из алгоритмов шифрования с открытым ключом, достойно выдержал испытание временем. Этот алгоритм основывается на задаче RSA, которую мы рассмотрели в главе 6. Напомним, что она сводится к поиску простых делителей больших натуральных чисел. Можно утверждать, что криптостойкость алгоритма RSA базируется на сложности проблемы факторизации, но не в полной мере, поскольку задачу RSA можно решать, не прибегая к разложению модуля на множители.

Пусть пользователь А считает нужным разрешить всем желающим отправлять ему конфиденциальные сообщения, расшифровать которые способен только он. Тогда А подбирает два больших простых числа p и q . Держа их в секрете, А публикует их произведение $N = p \cdot q$, которое называют модулем алгоритма. Кроме того, А выбирает число E , удовлетворяющее соотношению

```
ms2[i+4] = tmp % M; tmp /= M;
ms2[i+5] = tmp % M; tmp /= M;

for(i=0; i<6; i++)
ms2[i] += KA;
ms2[6] = 0;
printf("ms2 ");
puts(ms2);
gets(ms1);
gets(ms1);
}
```

Выбор параметров проводится по аналогии со случаем 16-битового модуля, однако эта процедура более трудоемкая.

Контрольные задания и вопросы

1. Опишите алгоритм шифрования RSA.
2. Может ли шифрующая экспонента в системе RSA быть четной?
3. Эквивалентны ли по сложности задача взлома криптосистемы RSA и проблема факторизации ее модуля?
4. Опишите процедуру ускорения расшифровывания.
5. Расскажите о выборе параметров криптосистемы RSA.
6. Какой раздел теории чисел использован в атаке Винера?
7. Можно ли построить аналог криптосистемы RSA с модулем, являющимся произведением трех простых чисел?

Упражнения

1. Пусть N – модуль шифрования алгоритма RSA и $L(N) = \text{НОК}(p-1, q-1)$. Доказать, что если E – экспонента шифрования алгоритма, то экспоненту расшифровывания d можно выбрать так, чтобы

$$Ed \equiv 1 \pmod{L(N)}.$$

2. Пусть N – модуль в алгоритме RSA и $L(N) = \text{НОК}(p - 1, q - 1)$. Предположим, что порядок экспоненты шифрования E в группе $(\mathbf{Z}/L(N)\mathbf{Z})^*$ равен k . Показать, что

$$m^{E^k} \equiv m \pmod{N}.$$

Доказать, что порядок элемента E по модулю $p - 1$ или $q - 1$ должен быть большим.

3. Показать, что схему шифрования RSA с простым модулем $N = p$ очень легко взломать.

4. Доказать, что если найдется такое b , что n – псевдопростое число по основанию b , но n не является сильно псевдопростым по основанию b , то можно быстро найти нетривиальный делитель числа n . Объяснить, как в этом случае выбрать модуль $n = pq$ в криптосистеме RSA.

5. Подсчитать количество чисел из интервала $(2^{15}, 2^{16})$, равных произведению двух простых чисел.

6. Доказать корректность процедуры расшифровывания в криптосистеме RSA при известных делителях модуля (см. стр. 183).

ОТВЕТЫ К УПРАЖНЕНИЯМ

Глава 1

4. 16 делителей: 1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, 315, 945.

6. $473^2 - 472^2$, $159^2 - 156^2$, $97^2 - 92^2$, $71^2 - 64^2$, $57^2 - 48^2$, $39^2 - 24^2$, $33^2 - 12^2$, $31^2 - 4^2$.

8. $100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^9 \cdot 13^7 \cdot 17^5 \cdot 19^5 \cdot 23^4 \cdot 29^3 \times$
 $\times 31^3 \cdot 37^2 \cdot 41^2 \cdot 43^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97$.

10. $360 = 2^3 \cdot 3^2 \cdot 5$, $294 = 2 \cdot 3 \cdot 7^2$, $\text{НОД}(360, 294) = 6$.

11. а) $1 = 11 \cdot 19 - 8 \cdot 26$; б) $17 = 1 \cdot 187 - 5 \cdot 34$; в) $1 = 205 \cdot 160 -$
 $- 39 \cdot 841$; г) $13 = 65 \cdot 2171 - 54 \cdot 2613$.

13. $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. $\varphi(5040) = 5040(1-1/2)(1-1/3)(1-1/5) \times$
 $\times (1-1/7) = 1152$.

Глава 2

1. $561 = 3 \cdot 11 \cdot 17$. Отсюда $L(561) = \text{НОК}(3-1, 11-1, 17-1) = 80$.
 $1105 = 5 \cdot 13 \cdot 17$. Отсюда $L(1105) = \text{НОК}(5-1, 13-1, 17-1) = 48$.
 $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Отсюда $L(5040) = \text{НОК}(16-8, 9-3, 5-1,$
 $7-1) = 24$. Отметим, что $\varphi(5040) = 1152$.

6. $\left(\frac{2}{8m+1}\right) = (-1)^{\frac{(8m+1)^2-1}{8}}$. Нетрудно проверить, что $(8m+1)^2 -$
 -1 кратно 16.

7. Для нахождения символа Лежандра $\left(\frac{q}{p}\right)$ при простых p и q (q фиксировано) используем следующий подход. Представим p в виде $p = 4qt + r$, $1 \leq r < 4q$ и $\text{НОД}(r, 4q) = 1$. Теперь
 $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}} \left(\frac{r}{q}\right)$. В нашем случае ($q = 3$)

имеем $\left(\frac{3}{p}\right) = (-1)^{\frac{r-1}{2} \frac{3-1}{2}} \left(\frac{r}{3}\right) = (-1)^{\frac{r-1}{2}} \left(\frac{r}{3}\right)$. При $q=3$ число r при-

нимает четыре значения: 1, 5, 7, 11. Таким образом,

$$\left(\frac{3}{12t+1}\right) = (-1)^{\frac{1-1}{2}} \left(\frac{1}{3}\right) = 1, \quad \left(\frac{3}{12t+5}\right) = (-1)^{\frac{5-1}{2}} \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{3}{12t+7}\right) = (-1)^{\frac{7-1}{2}} \left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

$$\left(\frac{3}{12t+11}\right) = (-1)^{\frac{11-1}{2}} \left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

Теперь находим все m , для которых $8m+1$ имеет вид $12t+5$ или $12t+7$. Это равносильно решению сравнений $8m \equiv 4 \pmod{12}$ и $8m \equiv 6 \pmod{12}$.

Ответ: число 3 является квадратичным невычетом для простых чисел вида $8m+1$ при $m=12n+k$, где n – натуральное число и $k=2, 5, 8$ или 11.

8. См. п. 7

Глава 3

1.	Простое число	2	3	5	7	11	13	17
	Наименьший образующий	1	2	2	3	2	2	3
	Число образующих	1	1	2	2	4	4	8

2. 5^6 .

3. Два для $d=1$: $X, X+1$. Один для $d=2$: X^2+X+1 . Два для $d=3$: X^3+X^2+1, X^3+X+1 . Три для $d=4$: $X^4+X^3+1, X^4+X+1, X^4+X^3+X^2+X+1$. Шесть для $d=5$: $X^5+X^3+1, X^5+X^2+1, X^5+X^4+X^3+X^2+1, X^5+X^4+X^3+X+1, X^5+X^4+X^2+X+1, X^5+X^3+X^2+X+1$.

4. Три для $d=1$: $X, X \pm 1$; Три для $d=2$: $X^2+1, X^2 \pm X+1$. Восемь для $d=3$: $X^3+X^2 \pm (X-1), X^3-X^2 \pm (X+1), X^3 \pm (X^2-1), X^3-X \pm 1$; Восемнадцать для $d=4$. Сорок восемь для $d=5$. Сто шестнадцать для $d=6$.

5. а) НОД = $1 = X^2g + (X+1)f$; б) НОД = $X^3 + X^2 + 1 = f + (X^2 + X)g$; в) НОД = $1 = (X-1)f - (X^2 - X + 1)g$.

6. Так как $\text{НОД}(f, f') = X^2 + 1$, кратные корни – это $\pm a^2$, где a – образующий элемент F_9^* .

8. а) пусть a – корень $X^2 + X + 1 = 0$, т. е. три последовательные степени a – это $a, a + 1$ и 1 ;

б) пусть a – корень $X^3 + X + 1 = 0$, тогда семь последовательных степеней a – это $a, a^2, a + 1, a^2 + a, a^2 + a + 1, a^2 + 1, 1$.

9. Возведите $b^{(p^n-1)/(p^d-1)}$ в степень p^d , покажите, что элемент не изменился, т. е. он принадлежит $F_{p^d}^*$. Далее убедитесь, что он – образующий, так как его степени различны. Это следует из того, что первые $p^n - 1$ степеней элемента b различны.

Глава 4

4. а) требуется $n - 1$ умножений, в каждом из них промежуточное произведение 3^j имеет не более $O(n)$ разрядов и число 3 имеет два бита, поэтому требуется $O(n)$ двоичных операций. Таким образом, в итоге получаем $O(n^2)$;

б) здесь промежуточное произведение имеет $O(n \log n)$ разрядов. Поэтому каждое произведение требует $O(n \log^2 n)$ двоичных операций. Общая сложность – $O(n^2 \log^2 n)$ двоичных операций;

в) $O(n^2 \log^2 N)$.

5. а) $O(n \log^2 n)$. б) $O(\log^2 n)$.

6. $O(\sqrt{n} \log^2 n)$.

7. Пусть $n - (k+1)$ -битовое число. В качестве первого приближения для $m = \lceil \sqrt{n} \rceil$ возьмем единицу с $\lceil k/2 \rceil$ нулями за ней. Находим знаки разрядов числа m , сдвигаясь от этой единицы направо и поочередно пробуя заменить 0 на 1 . Если при этой замене квадрат полученного числа m становится больше n , то в этом разряде оставляем 0 .

Глава 5

2. Показать, что $n - 1 \equiv p - 1 \pmod{2p - 2}$. Таким образом, $b^{n-1} \equiv 1 \pmod{p}$ и $b^{(2p-1-1)/2} \equiv \left(\frac{b}{2p-1}\right) \pmod{2p-1}$. Тогда $b^{n-1} \equiv 1 \pmod{p(2p-1)}$ равносильно $\left(\frac{b}{2p-1}\right) = 1$.

7. Предположим сначала, что n – псевдопростое число по основанию b . Так как $n - 1 = pq - 1 \equiv q - 1 \pmod{p-1}$, то $b^{q-1} \equiv 1 \pmod{p}$. Однако по малой теореме Ферма, $b^{p-1} \equiv 1 \pmod{p}$. Поскольку d представляется как целочисленная линейная комбинация $p - 1$ и $q - 1$, то $b^d \equiv 1 \pmod{p}$. Меняя ролями p и q , получаем, что $b^d \equiv 1 \pmod{q}$, откуда следует, что $b^d \equiv 1 \pmod{n}$. Обратное утверждение доказывается аналогично. В $(\mathbf{Z}/n\mathbf{Z})^*$ имеется d^2 оснований.

9. Показать, что $n - 1$ делится на $36m$ и, следовательно, на $6m$, $12m$, $18m$.

13. $n = 21$, $b = 8$.

16. $8^2 \equiv 18^2 \equiv -1 \pmod{65}$; $14^2 \equiv 1 \pmod{65}$, но $14^1 \not\equiv \pm 1 \pmod{65}$.

ЛИТЕРАТУРА

- Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: Учеб. пособие. М.: Гелиос АРВ, 2005.
- Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов / Пер. с англ. А.О. Слисенко; под. ред. Ю.В. Матиясевиич. М.: Мир, 1979.
- Боревич З.И., Шафаревич И.Р.* Теория чисел. М.: Наука, 1985.
- Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНПО, 2003.
- Введение в криптографию* / Под общ. ред. В.В. Ященко. М.: МЦНМО, «ЧеРо», 1998.
- Виноградов И.М.* Основы теории чисел, изд. 9-е, перераб. М.: Наука, 1981.
- Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.
- Гашков С.Б., Чубариков В.Н.* Арифметика, алгоритмы, сложность вычислений: Учеб. пособие. М.: Высш. шк., 2000.
- Карацуба А.А., Офман Ю.П.* Умножение многозначных чисел на автоматах // Докл. АН СССР. 1961. Т. 145(2).
- Коблиц Н.* Курс теории чисел и криптографии. М.: ТВП, 2001. 254 с.
- Ноден П., Китте К.* Алгебраическая алгоритмика. / Пер. с фр. В.А. Соколова; под ред. Л.С. Казарина. М.: Мир, 1999.
- Орлов В.А., Карташова М.В.* О псевдослучайных последовательностях на основе линейных преобразований // Безопасность информационных технологий, 2009. № 3.
- Сингх С.* Книга кодов. М.: АСТ: Астрель, 2007.
- Смарт Н.* Криптография. М.: Техносфера, 2005.
- Тришин А.Е.* Криптографические системы с открытым ключом. М., 2000.
- Diffie W., Hellman M.E.* New directions in cryptography // IEEE Trans. On Inf. Theory. 1976. IT-22.
- Rivest R., Shamir A. and Adleman L. A.* Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Comm. Of the ACM. 1978. N 21.

ОГЛАВЛЕНИЕ

Предисловие	3
Введение	6
Глава 1. Основы теории делимости	9
1.1. Основные понятия и теоремы	9
1.2. Простые числа	11
1.3. Алгоритмы Евклида	20
1.4. Непрерывные дроби	28
1.5. Важнейшие функции в теории чисел	33
Контрольные задания и вопросы	38
Упражнения	38
Глава 2. Сравнения	40
2.1. Свойства сравнений	40
2.2. Системы вычетов	43
2.3. Теоремы Ферма и Эйлера	46
2.4. Сравнения первой степени	48
2.5. Системы сравнений первой степени	52
2.6. Сравнения второй степени	55
Контрольные задания и вопросы	70
Упражнения	71
Глава 3. Конечные поля	72
3.1. Математические понятия, поясняющие понятие конечного поля	72
3.2. Введение в теорию конечных полей	78
3.3. Построение конечных полей	87
Контрольные задания и вопросы	94
Упражнения	94
Глава 4. Сложность реализации криптоалгоритмов	96
4.1. Системы счисления	96
4.2. Сложность реализации арифметических операций	100
4.3. Сложность алгоритмов, схожих с алгоритмом Евклида	109
4.4. Извлечение квадратного корня по простому модулю	114
4.5. Алгоритмы возведения в степень	118

4.6. Сложность операций в конечных полях	120
Контрольные задания и вопросы	124
Упражнения	125
Глава 5. Нахождение очень больших простых чисел	126
5.1. Распределение простых чисел	126
5.2. Псевдопростые числа	134
5.3. Эйлеровы псевдопростые числа	139
5.4. Сильно псевдопростые числа	140
Контрольные задания и вопросы	144
Упражнения	144
Глава 6. Анализ криптосистем	146
6.1. Введение в криптографию	146
6.2. Псевдослучайные последовательности на основе линейных преобразований	152
6.3. Криптография с открытым ключом	164
6.4. Односторонние функции	166
6.5. Криптосистема Эль-Гамала	173
6.6. Криптосистема Рабина	176
Контрольные задания и вопросы	179
Упражнения	180
Глава 7. Криптосистема RSA	181
7.1. Описание алгоритма RSA	181
7.2. Корректность алгоритма RSA	183
7.3. Криптостойкость алгоритма RSA	185
7.4. Выбор параметров криптосистемы RSA	189
7.5. Атаки на криптосистему RSA	193
7.6. Учебные версии криптосистемы RSA	197
Контрольные задания и вопросы	215
Упражнения	215
Ответы к упражнениям	217
Литература	221

Учебное издание

Орлов Валентин Александрович
Медведев Николай Викторович
Шимко Наталия Александровна
Домрачева Анна Борисовна

ТЕОРИЯ ЧИСЕЛ В КРИПТОГРАФИИ

Редактор *Н.Г. Ковалевская*
Технический редактор *Э.А. Кулакова*
Художник *С.С. Водчиц*
Корректор *Е.В. Авалова*
Компьютерная верстка *А.Ю. Ураловой*

Оригинал-макет подготовлен
в Издательстве МГТУ им. Н.Э. Баумана.

Санитарно-эпидемиологическое заключение
№ 77.99.60.953.Д.003961.04.08 от 22.04.08 г.

Подписано в печать 21.12.2011. Формат 60×90 1/16.
Усл. печ. л. 14,0. Тираж 500 экз. Заказ

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская, 5.
E-mail: press@bmstu.ru
<http://www.baumanpress.ru>

Отпечатано в типографии МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., 5.
E-mail: mgtupress@mail.ru