НГТУ НЭТИ

Факультет автоматики и вычислительной техники

А. Б. АРХИПОВА

ОСНОВНЫЕ МАТЕМАТИЧЕСКИЕ ПРИНЦИПЫ В РЕАЛИЗАЦИИ НЕКОТОРЫХ АЛГОРИТМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОВОСИБИРСК
2022

УДК 004.056:512.5(078.5)
А 877

Рецензенты:
А. А. Ракитский, канд. техн. наук, доцент
А. В. Иванов, канд. техн. наук, доцент

Архипова А. Б.
А 877 Основные математические принципы в реализации некоторых алгоритмов информационной безопасности: учебное пособие / А. Б. Архипова. – Новосибирск : Изд-во НГТУ, 2022. – 123 с.

ISBN 978-5-7782-4325-5

Пособие включает в себя описание основных математических принципов в реализации некоторых алгоритмов информационной безопасности. Предназначено для студентов направлений 10.00.00 «Информационная безопасность» при освоении дисциплин «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», «Программирование», «Технологии и методы программирования», «Криптография».

УДК 004.056:512.5(078.5)

ISBN 978-5-7782-4325-5

ОГЛАВЛЕНИЕ

Введение 4
1. Алгоритмические средства защиты информации 5
2. Числовые кольца и поля 8
2.1. Отношения на множестве. Понятие алгебры 8
2.2. Делимость в кольце целых чисел 11
2.3. Наибольший общий делитель 16
2.4. Наименьшее общее кратное 28
2.5. Распределение простых чисел 30
3. Определение сравнения 41
4. Теоремы Эйлера и Ферма 51
4.1. Функция Эйлера 51
4.2. Теоремы Эйлера и Ферма 56
5. Основные алгоритмы в информационной безопасности 63
5.1. Используемые вычислительно сложные задачи и достигаемый уровень безопасности алгоритмических средств 65
5.2. Тесты на простоту 70
5.2.1. Тест Миллера на простоту 71
5.2.2. Тест Поклингтона 72
5.2.3. Процедура генерации простых чисел ГОСТ Р 34.10–94 74
5.3. Криптографические протоколы распределения ключей 76
5.4. Криптографические протоколы аутентификации, использующие хэш-функции и симметричную криптографию 104
5.5. Криптографические протоколы аутентификации, использующие криптографию с открытым ключом 109
Библиографический список 113
Приложения 115
Приложение А Данные для проверки на простоту 115
Приложение Б. Таблица простых чисел 119

1. АЛГОРИТМИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Безопасность информационно-телекоммуникационных технологий определяется всеми аспектами, связанными с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности данного вида технологий [1]. Информация, обрабатываемая с использованием информационно-телекоммуникационных технологий, не является жестко привязанной к физическому носителю, поэтому мощными и универсальными средствами обеспечения конфиденциальности, неотказуемости, аутентичности, достоверности и анонимности являются алгоритмические средства обеспечения безопасности.

Современные алгоритмы и протоколы защиты информации в информационно-телекоммуникационных системах используются для обеспечения конфиденциальности, целостности, неотказуемости, подотчетности, аутентичности, достоверности и анонимности.

Алгоритмы и протоколы аутентификации и защиты информации в информационно-телекоммуникационных системах можно разделить на три группы, в зависимости от используемого типа ключей:

1) бесключевые КА – не используют в вычислениях никаких ключей;

2) одноключевые КА – работают с одним ключевым параметром (секретным ключом);

3) двухключевые КА – на различных стадиях работы в них применяются два ключевых параметра: секретный и открытый ключи.

Ярким примером алгоритма аутентификации с общим ключом является имитовставка, позволяющая проверяющему с определенной вероятностью (например, 2^{-32}) утверждать, что сообщение не было изме-

нено в процессе передачи [23, 29]. Но методы с обладанием общим ключом сталкивается с трудностями передачи и хранения этого ключа от одной стороны к другой, дополнительно такие методы не могут обеспечить выполнения всех требуемых свойств, например, неотказуемость субъекта от созданного цифрового объекта. Использование пары открытого и секретного ключей позволяет строить такие алгоритмы и протоколы защиты информации, которые используются для обеспечения конфиденциальности, целостности, неотказуемости, подотчетности, аутентичности, достоверности и т. д.

В современном мире примером этому служат системы электронных цифровых подписей, являющихся мощным средством для обеспечения неотказуемости субъекта от созданного им цифрового объекта, аутентичности, целостности и достоверности цифрового объекта, созданного субъектом [23, 29].

В рамках учебного пособия введем ряд определений.

Протокол порядок действий, предпринимаемых двумя или более сторонами, предназначенный для решения определенной задачи. То есть протокол выполняется в определенной последовательности, с начала до конца. Каждое действие должно выполняться в свою очередь и только после окончания предыдущего.

У протоколов есть также и другие характеристики:

– каждый участник протокола должен знать протокол и последовательность составляющих его действий;

– каждый участник протокола должен согласиться следовать протоколу;

– протокол должен быть непротиворечивым, каждое действие должно быть определено так, чтобы не было возможности непонимания.

– протокол должен быть полным, каждой возможной ситуации должно соответствовать определенное действие.

Криптографический протокол – это протокол, использующий криптографию для решения, по крайней мере, одной из задач:

– обеспечение конфиденциальности;

– обеспечение целостности;

– аутентификация и т.д.

Стороны могут быть друзьями и доверять друг другу или врагами и не верить друг другу даже при сообщении времени суток.

Криптографический протокол определен однозначно и включает некоторый криптографический алгоритм.

Для демонстрации работы протоколов используют несколько абонентов (игроков), которых обозначают последовательно буквами латинского алфавита. В русскоязычной трактовке допустимо обозначение *A* – Алиса (Alice), *B* – Боб (Bob). Как правило, Алиса начинает все протоколы, а Боб отвечает. Если для протокола нужна третья или четвертая сторона, в игру вступают Кэрол (Carol) и Дэйв (Dave).

В рамках криптографических протоколов с посредниками (незаинтересованной третьей стороной) вводят имя Трент. Это заслуживающий доверия посредник, которому доверено завершение протокола.

Но построение алгоритмов информационной безопасности и протоколов невозможно без базовых знаний классической алгебры, теории сравнений, обоснования использования односторонних функций, поэтому представим последовательно цепочку теоретических изысканий в рамках рассмотрения алгоритмических средств защиты информации.

2. ЧИСЛОВЫЕ КОЛЬЦА И ПОЛЯ

2.1. Отношения на множестве. Понятие алгебры

Введем основные определения классической алгебры.

Понятие множества не определяется в строгом смысле. Множество – это совокупность некоторых объектов (называемых элементами множества). Факт принадлежности элемента a множеству A обозначаем как $a \in A$.

Определение. Символ Ø обозначает множество, у которого нет ни одного элемента.

Определение. Пусть $A_1, A_2, ..., A_n$ – некоторые множества. Их декартовым произведением назовем множество всевозможных упорядоченных наборов, содержащих n-позиций:

$$A = \{(a_1, a_2, ..., a_n) \| a_i \in A_i,\ i = 1, 2, ..., n\}.$$

Произведение множеств обозначим через $A_1 \times A_2 \times \ldots \times A_n$.

Определение. n-й (декартовой) степенью множества A назовем множество $A^n = A_1 \times A_2 \times \ldots \times A_n$, где $A_i = A,\ i = 1, 2, \ldots, n$.

Определение. Непустое подмножество множества A^n назовем n-местным отношением на множестве A.

Заметим, что часто вместо термина «n-местное» используют термин «n-арное» отношение. При $n = 2$ будем говорить о бинарных отношениях, а при $n = 1$ – об унарных отношениях.

Если P – бинарное отношение на множестве A, то факт принадлежности пары (a, b) отношению P будем обозначать так: $a\ P\ b$ и говорить, что элементы a, b множества A состоят в отношении P.

Определение. Бинарное отношение ~ на множестве А назовем *отношением эквивалентности*, если отношение ~ обладает следующими свойствами:

1) рефлексивности: $\forall a \in A,\ a \sim a$;

2) симметричности: $\forall a, b \in A,\ a \sim b \to b \sim a$;

3) транзитивности: $\forall a, b, c \in A,\ a \sim b,\ b \sim c \to a \sim c$.

Определение. Бинарное отношение ~ на множестве A назовем *отношением частичного (нестрогого) порядка*, если отношение ~ обладает следующими свойствами:

1) рефлексивности: $\forall a \in A,\ a \sim a$;

2) антисимметричности: $\forall a, b \in A,\ a \sim b,\ a \neq b \to b$ не эквивалентно a;

3) транзитивности: $\forall a, b, c \in A,\ a \sim b,\ b \sim c \to a \sim c$.

Определение. Отображение (полное и однозначное)

$$f = A^n \to A$$

n-й (декартовой) степени множества A в множество A называется n-местной операцией на множестве A.

Определение. Непустое множество A с набором операций $f_1, f_2, ..., f_k$ называется *алгеброй* и обозначается как

$$A = < A;\ f_1, f_2, ..., f_k > .$$

Множество A называется *носителем* алгебры A, а набор $< f_1, f_2, ..., f_k >$ называется *сигнатурой* алгебры A.

Набор арностей $< n_1, n_2, ..., n_k >$ соответственно операций $f_1, f_2, ..., f_k$ называется типом алгебры A.

Определение. Непустое множество B носителя A алгебры $A = < A;\ f_1, f_2, ..., f_k >$ называется *подалгеброй* алгебры A, если подмножество B замкнуто относительно операций $f_1, f_2, ..., f_k$.

Приведем пример некоторых классических алгебр.

Определение. Алгебра $G = < G; \times, {}^{-1}, e >$ типа < 2, 1, 0 > называется группой, если

1) $\forall a, b, c, (a \times b) \times c = a \times (b \times c)$;

2) $\forall a,\ a \times a^{-1} = a^{-1} \times a = e$;

3) $\forall a,\ a \times e = e \times a = a$.

Заметим, что обозначения сигнатурных символов в группе могут быть отличными от введенных. Так, например, множество целых чисел Z с операциями +, – и выделенным элементом 0 является группой. В этом случае говорят об аддитивной записи операций группы. Другим примером группы может служить множество R^+ всех строго положительных чисел с операциями умножения, взятия обратных элементов $a^{-1} = \frac{1}{a}$ и выделенным элементом 1.

Определение. Группа G называется абелевой, или коммутативной, если в G справедливо тождество $\forall x,\ y,\ x \times y = y \times x$.

Определение. Алгебра $K = < K; +, -, \cdot, 0 >$ типа $< 2, 1, 2, 0 >$ называется *кольцом*, если

1) алгебра $K = < K; +, -, 0 >$ является абелевой группой;

2) выполнены тождества

$$\forall x,\ x \cdot 0 = 0 \cdot x = 0,$$

$$\forall x,\ y,\ z,\ (x + y) \cdot z = xz + yz, z(x + y) = zx + zy.$$

Определение. Кольцо K называется коммутативным кольцом, если в K справедливо тождество

$$\forall x,\ y,\ x \cdot y = y \cdot x.$$

Определение. Кольцо K называется ассоциативным кольцом, если в K справедливо тождество

$$\forall x,\ y,\ z,\ (x \cdot y)z = x(y \cdot z).$$

Определение. Кольцо K называется кольцом с единицей, если в K существует элемент единица такой, что справедливо тождество

$$\forall x,\ x \cdot 1 = 1 \cdot x = x.$$

Примером коммутативного ассоциативного кольца с единицей может служить кольцо целых чисел Z. Кольцо целых чисел является одним из основных числовых колец. Методы решения многих задач в кольце Z нередко служат основой для аналогий при изучении других колец (например, кольцо многочленов).

Определение. Алгебра $K = <K; +, -, \cdot, ^{-1}, 0, 1>$ типа < 2, 1, 2, 1, 0, 0 > называется *полем*, если

1) алгебры $K = <K; +, -, 0>$ и $K = <K \setminus \{0\}; \cdot, ^{-1}, 1>$ являются абелевыми группами;

2) выполнены тождества:

$$\forall x,\ y,\ z,\ (x + y)z = xz + yz,$$

$$\forall x,\ x \cdot 0 = 0 \cdot x = 0.$$

Хорошо известные примеры полей – это числовые поля рациональных чисел *Q,* вещественных чисел *R*.

2.2. Делимость в кольце целых чисел

Определение. Пусть K – коммутативное кольцо и $a,\ b \in K$. Говорят, что элемент b делится на a, если существует такой элемент $c \in K$, что $b = ac$.

Тот факт, что a делит b, кратко записывают в виде $a|b$. Факт того, что a не делит b, будем записывать в виде $a \nmid b$.

Теорема 2.1. Для любых элементов *a, b, c* коммутативного кольца K справедливы импликации:

1) $a|b,\ b|c \rightarrow a|c$;

2) $a|b,\ b|c \rightarrow a|(b \pm c)$;

3) $a|b \rightarrow a|bc$.

Если K – коммутативное кольцо с единицей e, то оно обладает также свойствами:

4) $\forall a \in K,\ \forall r \in R^{*} : (r|a,\ ar|a),$ где $R^{*} = R \setminus \{0\}$;

5) $\forall a, b \in K,\ \forall r_1, r_2 \in R^{*} : (a|b,\ ar_1|br_2)$.

Доказательство

Импликации 1−3 следуют непосредственно из определения.

Докажем импликацию 4.

Рассматриваем множество $R^{*} = R \setminus \{0\}$ − значит, у нас есть обратимый элемент, удовлетворяющий свойствам:

$$r \cdot r^{-1} = r^{-1} \cdot r = e.$$

Получим:

$$a = e \cdot a = r \cdot r^{-1} \cdot a = r(r^{-1} \cdot a);$$

$$a = a \cdot e = a \cdot r \cdot r^{-1} = (a \cdot r)r^{-1}.$$

Значит, r делится на a, ar делится на a.

Докажем импликацию 5.

У нас $a|b$. Тогда $b = a \cdot c$ при $c \in K$.

$$b \cdot r_2 = a \cdot c \cdot r_2,$$

$$a \cdot \left(r_1 \cdot r_1^{-1}\right) c \cdot r_2 = (a \cdot r_1)\left(r_1^{-1} c r_2\right),$$

$$a \cdot r_1 \mid b \cdot r_2,$$

что и требовалось доказать.

Теорема 2.2. Для любых элементов $a, b \in Z$:

1) $a|b \rightarrow \pm a| \pm b$;

2) $a|b,\ b \neq 0 \rightarrow |a| \leq |b|$;

3) $a|b,\ b|a \rightarrow a = \pm b$.

Доказательство

Свойство 1 является уточнением свойства 5 теоремы 2.1, поскольку обратимые элементы кольца Z исчерпываются числами +1, –1.

Свойство 2. Из условия $a|b$ следует, что $b = a \cdot c$ при некотором $c \in Z$. Отсюда по свойству модулей имеем: $|b|=|a| \cdot |c|$.

Так как $b \neq 0$, то $|c| > 0$, т. е. $|c| = 1 + x$, где $x \in N_0$. *Следовательно,* $|b|=|a|(1 + x) = |a| + |a| \cdot x$.

Значит, $|b| \geq |a|$.

Свойство 3.

Дано:

$$\begin{cases} a \mid b \Rightarrow b = a \cdot q, \\ b \mid a \Rightarrow a = b \cdot x. \end{cases}$$

Данная система имеет решение только в случае $q = x = t$.

Получим:

$$\begin{cases} b = a \cdot t, \\ a = b \cdot t. \end{cases}$$

Разделим первое уравнение на второе: $\frac{b}{a} = \frac{a}{b} \Rightarrow a|b = b|a \Rightarrow$ $\Rightarrow |a| = |b|$.

Свойство 1 сводит описание всех делителей и всех кратных для данного числа к описанию лишь положительных (натуральных) делителей и кратных. Из свойства 2 следует конечность числа различных делителей у любого отличного от нуля целого числа, что дает принципиальную возможность нахождения всех делителей числа.

В том случае, когда одно натуральное число не делится на другое, алгоритм деления «уголком» приводит к неполному частному и остатку от деления. Оказывается, что понятие деления с остатком можно обобщить на любые целые числа.

Определение. Разделить с остатком целое число a на целое число b – это значит найти целые числа q (неполное частное) и r (остаток), удовлетворяющие условиям:

$$a = b \cdot q + r,$$
$$0 \le r < |b|.$$

Теорема 2.3. Если $a, b \in Z$ и $b \neq 0$, то a можно разделить на и b остатком, причем неполное частное и остаток определяются **однозначно.**

Доказательство

Сначала докажем существование чисел q и r, удовлетворяющих условиям $a = b \cdot q + r$, $0 \le r < |b|$.

Рассмотрим отдельно три случая.

1	2	3
$\boldsymbol{A \ge 0,}$ $\boldsymbol{b > 0}$	$\boldsymbol{A < 0,}$ $\boldsymbol{b > 0}$	***a – любое,*** $\boldsymbol{b < 0}$

а) $\boldsymbol{a \ge 0, b > 0.}$

Аксиома Архимеда утверждает, что $\forall a, b \in N, q_1 \in N$ верно при $a < b \cdot q_1$.