Практикум по криптографии (В.А. Носов, А.В. Галатенко)

1. Введение

Данное пособие содержит перечень задач по практикуму “Криптография”. Предлагаемые задачи могут быть сгруппированы по двум признакам: области и сложности. Области включают в себя булеву алгебру, перестановки, арифметику в конечных полях и кольцах вычетов (ключевые математические модели в задачах криптографии и криптоанализа), шифры простой замены и лозунговые шифры, шифры гаммирования с зависимой или неравновероятной гаммой (упрощенные модели шифров), а также реальные криптографические стандарты и методы криптоанализа. Все задачи разделены на три группы сложности. Каждый студент должен решить по одной задаче из каждой группы.

Изложенный материал сгруппирован по областям. Каждой задаче сопоставлена римская цифра I, II или III, определяющая группу сложности.

2. Задачи по булевым функциям

В задачах класса II и III дополнительно должен быть предоставлен отчет с описанием использованных алгоритмов и статистикой по решениям (например, оценкой методом Монте-Карло математического ожидания и дисперсии для различных значений параметров).

Задача I1. Генерация входных данных для задачи 2-выполнимость. На вход поступает число переменных и число элементарных дизъюнкций, на выход в текстовый файл записывается случайная 2-КНФ с заданным числом элементарных дизъюнкций, или выдается отказ, если такая КНФ не существует. Дополнительная информация о задаче может быть найдена в книге В.А. Носов, “Основы теории алгоритмов и анализа их сложности”,
`http://www.intsys.msu.ru/staff/vnosov/theoralg.htm`

Задача I2. Генерация входных данных для задачи 3-выполнимость. На вход

поступает число переменных и число элементарных дизъюнкций, на выход в текстовый файл записывается случайная 3-КНФ с заданным числом элементарных дизъюнкций, или выдается отказ, если такая КНФ не существует. Дополнительная информация о задаче может быть найдена в книге В.А. Носов, "Основы теории алгоритмов и анализа их сложности",
`http://www.intsys.msu.ru/staff/vnosov/theoralg.htm`

Задача I3. Генерация случайного полинома Жегалкина. На вход поступает число переменных, число слагаемых и максимальная степень слагаемых, на выход в текстовый файл записывается случайный полином Жегалкина, удовлетворяющий входным условиям, или выдается отказ, если такой полином не существует. Дополнительная информация о задаче может быть найдена в книге С.В. Яблонского "Введение в дискретную математику".

Задача I4. Расстоянием Хэмминга между двумя булевыми функциями назовем число отличающихся разрядов в столбцах значений. На вход программе поступает булева функция в виде столбца значений, записанного в текстовом файле, на выходе в текстовый файл записывается ближайшая по Хэммингу в входной функции линейная функция, а также расстояние между функциями. Дополнительная информация о задаче может быть найдена в книгах С.В. Яблонского "Введение в дискретную математику" и В.А. Носова "Специальные главы дискретной математики".

Задача II1. Методом резолюции решить задачу 2-выполнимости КНФ. На вход поступает текстовый файл с 2-КНФ, на выходе в текстовый файл записывается набор переменных, обращающий КНФ в единицу, или выдается отказ, если такой набор не существует. Дополнительно выдается время, затраченное на проверку выполнимости. Дополнительная информация о задаче может быть найдена в книгах В.А. Носов, "Основы теории алгоритмов и анализа их сложности", `http://www.intsys.msu.ru/staff/vnosov/theoralg.htm`, и Ч. Ченя и Р. Ли "Математическая логика и автоматическое доказательство теорем".

Задача II2. Методом Ивамы решить задачу 3-выполнимости КНФ. На вход поступает текстовый файл с 3-КНФ и ограничение по времени, на выходе в текстовый файл записывается набор переменных, обращающий КНФ в единицу, или выдается отказ, если такой набор не существует или если процесс решения нарушает заданное ограничение по времени. Дополнительно выдается время, затраченное на проверку выполнимости. Дополнительная информация о задаче может быть найдена в книге Н.Н. Кузюрина и С.А. Фомина "Эффективные алгоритмы и сложность вычислений".

Задача II3. Методом поиска с возвратом решить задачу 3-выполнимости КНФ. На вход поступает текстовый файл с 3-КНФ и ограничение по времени, на выходе в текстовый файл записывается набор переменных, обращающий КНФ в единицу, или выдается отказ, если такой набор не существует или если процесс решения нарушает заданное ограничение по времени. Дополнительно выдается

время, затраченное на проверку выполнимости. Дополнительная информация о задаче может быть найдена в книге Д. Кнута “Искусство программирования”, т. 3.

Задача II4. Методом линеаризации решить систему булевых уравнений, порожденную с помощью решения задачи I3. На вход в текстовом файле поступает список булевых функций, заданных полиномами Жегалкина, на выходе в текстовый файл записывается хотя бы один набор переменных, обращающий все функции в 0, или отказ, если такой набор не существует. Дополнительно выдается время, затраченное программой на решение. Пусть уравнения системы записаны в виде $f_i(x_1, \ldots, x_n) = a_i$, где f_i — функции алгебры логики, a_i — булевы константы. Идея заключается в следующем. Пусть найдено подмножество переменных, такое что после подстановки произвольных значений вместо переменных из найденного подмножества система становится линейной. Пусть мощность такого подмножества равна m. Тогда сложность решения исходной системы не превышает $2^m * L$, где L — максимальная сложность решения возникающих линейных систем. Следовательно, если m невелико, исходная система может быть достаточно эффективно решена.

Задача III1. Генерация S-блоков. На вход поступает булев оператор, заданный таблицей значений. На выходе в текстовый файл записывается реализация оператора в базисе из конъюнкции, дизъюнкции и отрицания, оптимизированная по максимальной глубине вычислений. Дополнительная информация о задаче может быть найдена в книге С.В. Яблонского “Введение в дискретную математику”.

Задача III2. Генерация S-блоков. На вход поступает булев оператор, заданный таблицей значений. На выходе в текстовый файл записывается реализация оператора в базисе из конъюнкции, дизъюнкции и отрицания, оптимизированная по числу использованных конъюнкций и дизъюнкций. Дополнительная информация о задаче может быть найдена в книге С.В. Яблонского “Введение в дискретную математику”.

3. Задачи по перестановкам

Задача I5. Сгенерировать все перестановки в лексикографическом порядке. На вход поступает натуральное число n, на выходе в текстовом файле записываются все перестановки порядка n в лексикографическом порядке. Дополнительная информация о задаче может быть получена, например, в книге А.Г. Куроша “Курс высшей алгебры”.

Задача I6. Сгенерировать все перестановки с условием, что соседние перестановки отличаются на одну транспозицию. На вход поступает натуральное число n, на выходе в текстовом файле записываются все перестановки порядка n, при-

чем соседние перестановки отличаются на одну транспозицию. Дополнительная информация о задаче может быть получена, например, в книге А.Г. Куроша "Курс высшей алгебры".

Задача II5. Проверка перестановочности системы булевых функций. На вход подается текстовый файл с булевыми функциями, заданными таблицами значений, на выходе выдается ответ, является ли поданная система перестановочной. В случае положительного ответа дополнительно выдается цикловая структура перестановки и разностные характеристики. Дополнительная информация о задаче может быть найдена в книге В.А. Носова "Специальные главы дискретной математики".

Задача II6. Исследование свойств случайных перестановок. На вход подаются натуральные числа n и m. n задает порядок перестановок, m — количество испытаний. Требуется методом Монте-Карло вычислить среднее число независимых циклов, среднюю длину максимального цикла и среднюю длину максимальной монотонной последовательности и вывести вычисленные характеристики в текстовый файл. Проанализировать зависимость характеристик от значения n. Дополнительная информация о задаче может быть найдена в книге В.А. Носова "Специальные главы дискретной математики".

4. Задачи по арифметике в конечных полях и кольцах вычетов

Задача I7. Проверка числа на простоту. На вход подается натуральное число n и максимальное время вычислений t, на выходе выдается, является ли n простым, или отказ, если это не удалось установить за время t. Дополнительная информация о задаче может быть найдена в книге И.М. Виноградова "Основы теории чисел".

Задача I8. Проверка числа на псевдопростоту. На вход подается натуральное число n, рациональное число ε, $0 < \varepsilon < 1$. Требуется найти ближайшее к n число, являющееся псевдопростым с вероятностью не ниже $1 - \varepsilon$. n является небольшим числом. Дополнительная информация о задаче может быть найдена в книге О.Н. Василенко "Теоретико-числовые алгоритмы в криптографии".

Задача I9. Быстрое возведение в степень. На вход подается натуральные числа n и k. С помощью алгоритма быстрого возведения в степень требуется найти n^k, записать ответ в текстовый файл и выдать время вычисления. n и k являются небольшими ($n^k < 2^{64}$). Дополнительная информация о задаче может быть найдена в книге Д. Кнута "Искусство программирования", т. 2.

Задача II7. Реализация операций в кольцах вычетов. Сначала производится инициализация, в процессе которой на вход подяется натуральное число n.

Затем на вход поступают пары чисел, для которых необходимо вычислить заданные операции — сложение, вычитание, умножение и возведение в степень по модулю n. Числа задаются в текстовом файле, в двоичном представлении. Дополнительная информация о задаче может быть найдена в книге Д. Кнута "Искусство программирования", т. 2.

Задача II8. Реализация операции деления в кольце вычетов. Сначала производится инициализация, в процессе которой на вход подяется натуральное число n. Затем на вход поступают пары чисел, задаваемых в текстовом файле, в двоичном представлении. Требуется вычислить частное по модулю n или выдать отказ, если делитель не является обратимым. Дополнительная информация о задаче может быть найдена в книге Д. Кнута "Искусство программирования", т. 2.

Задача II9. Поиск образующего элемента. На вход поступает простое число p, на выход выдается порождающий элемент Z_p^*. Порядок мультипликативной группы небольшой (меньше 2^{32}). Дополнительная информация о задаче может быть найдена в книге А.В. Черемушкина "Лекции по арифметическим алгоритмам в криптографии".

Задача III3. Проверка числа на псевдопростоту. На вход подается натуральное число n, рациональное число ε, $0 < \varepsilon < 1$. Требуется найти ближайшее к n число, являющееся псевдопростым с вероятностью не ниже $1 - \varepsilon$. n является большим числом (порядка 2^k, где k — несколько тысяч). Дополнительная информация о задаче может быть найдена в книге О.Н. Василенко "Теоретико-числовые алгоритмы в криптографии".

Задача III4. Реализация библиотеки арифметики в конечных полях. Библиотека состоит из функции инициализации, в которой задается базовое поле и неприводимый многочлен, и функций вычисления суммы, разности, произведения и частного двух чисел, а также возведения в степень. Дополнительно должна быть реализована функция тестирования, зачитывающая из текстового файла входные данные и совершающая заданные действия. Дополнительная информация о задаче может быть найдена в книге Д. Кнута "Искусство программирования", т. 2.

5. Задачи по шифру простой замены и лозунговым шифрам

В качестве источников дополнительной информации по задачам этого раздела можно использовать книги А.П. Алферова, А.Ю. Зубова, А.С. Кузьмина и А.В. Черемушкина "Основы криптографии" и "Введение в криптографию" под редакцией В.В Ященко.

Задача I10. Анализ частотных характеристик текстов. На вход поступает текстовый файл, на выходе в текстовый файл записывается статистика встречаемости отдельных символов, биграмм и триграмм.

Задача I11. Анализ характеристик текстов. На вход подается текстовый файл и натуральное число n, на выходе вычисляется минимальная, средняя и максимальная длина непрерывного участка, в котором встречается не менее n различных символов.

Задача I12. Анализ частотных характеристик пар текстов. На вход поступает пара текстовых файлов одинаковой длины, на выход в текстовый файл выдается стастистика встречаемости символов тексте, полученном суммированием входных данных по модулю 33.

Задача II10. Вычисление числа вариантов ключей в различных ограничениях шифра простой замены. Задается ограничение на перестановку (например, максимальный модуль разности между символом и его образом). Требуется вычислить число ключей, удовлетворяющих заданному ограничению.

Задача II11. Дешифрование шифра простой замены с помощью частотного анализа. На вход подается текстовый файл с осмысленным текстом, зашифрованным шифром простой замены. На выходе в файл записывается открытый текст и шифрующая перестановка.

Задача II12. Ограничение возможных ключей в шифре простой замены. Используя собранные данные о биграммах и триграммах, которые не встречаются в осмысленных текстах, сузить множество возможных ключей. На вход подается текстовый файл с шифр-текстом, полученным простой заменой, на выходе в текстовый файл для каждого символа выдаются возможные прообразы.

Задача III5. Криптоанализ методом протяжки. Реализовать систему, которая получает на вход текстовый файл с текстом, зашифрованным методом простой замены или с помощью лозунга, и текстовый файл со словарем. Определить, каким шифром зашифрован текст, и выдать в текстовый файл открытый текст.

6. Задачи по шифру гаммирования с зависимой или неравновероятной гаммой

В качестве источников дополнительной информации по задачам этого раздела можно использовать книги А.П. Алферова, А.Ю. Зубова, А.С. Кузьмина и А.В. Черемушкина “Основы криптографии” и “Введение в криптографию” под редакцией В.В Ященко.

Задача II13. Криптоанализ гаммирования в случае зависимости в гамме. На вход поступает текстовый файл с осмысленным текстом, зашифрованным гаммированием на гамме, также представляющей собой осмысленный текст, и словарь.

Методом протяжки выполнить дешифрование и записать результат в текстовый файл.

Задача II14. Криптоанализ гаммирования в случае неравновероятной гаммы. На вход поступает текстовый файл с осмысленным текстом, зашифрованным гаммированием на гамме, также представляющей собой осмысленный текст. С помощью частотного анализа выполнить дешифрование и записать результат в текстовый файл.

7. Задачи по криптографическим стандартам

Задача III6. Алгоритм DES. Реализовать преобразование блока алгоритма DES, в качестве параметра принимающее число раундов в схеме Фейстеля. Оценить скорость работы полной версии (16 раундов). Провести линейный криптоанализ для версии с четырьмя раундами. Описание алгоритма DES можно найти по адресу `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`. Описание линейного криптоанализа можно найти в работе M. Matsui "Linear cryptanalysis method for DES cipher",
`http://homes.esat.kuleuven.be/~abiryuko/Cryptan/matsui_des.PDF`

Задача III7. Алгоритм RSA. Реализовать алгоритм RSA. Оценить скорость работы. Написать функцию расшифровки при небольших значениях открытого ключа. Описание алгоритма RSA можно найти по адресу
`ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf`.

Задача III8. Алгоритм IDEA. Реализовать алгоритм IDEA. Оценить скорость работы полной версии. Провести поиск слабых ключей в усеченной версии. Описание алгоритма IDEA можно найти по адресу
`http://www.iso-register.com/0002.pdf`.

Задача III9. Алгоритм SHA1. Реализовать алгоритм SHA1. Оценить скорость работы. Найти коллизию при усечении выхода до 60 бит. Описание алгоритмов семейства SHA можно найти по адресу
`http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`.

Задача III10. Алгоритм Эль-Гамаля. Реализовать алгоритм электронной подписи Эль-Гамаля. Оценить скорость работы. Методом Монте-Карло оценить среднее число попыток на сообщение. Описание алгоритма Эль-Гамаля можно найти по адресу
`http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf`.

Задача III11. Алгоритм A5/1. Реализовать алгоритм A5. Реализовать дешифрование алгоритма A5/1. Изначально алгоритм держался в секрете, затем был реконструирован в работе M. Briceno, I. Goldberg и D. Wagner "A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms".

Задача III12. Алгоритм AES. Реализовать преобразование блока алгоритма

AES, в качестве параметра принимающее число раундов. Оценить скорость работы полной версии на 128-битном ключе. Провести дифференциальный криптоанализ для реализации с двумя раундами. Описание алгоритма AES можна найти по адресу
`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`. Описание дифференциального криптоанализа можно найти по адресу
`http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf`