

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Механико-математический факультет  
Кафедра теоретической кибернетики

А. А. Городилова, Н. Н. Токарева, Г. И. Шушуев

КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ  
Сборник задач

Учебное пособие

Новосибирск

2014

УДК 519.7  
ББК В185.33я73-1  
Г 701

**Городилова А. А., Токарева Н. Н., Шушуев Г. И.** Криптография и криptoанализ. Сборник задач: Учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2014. 325 с.

ISBN 978-5-4437-0226-1

Учебное пособие является практическим введением в современные математические методы криптографии и служит учебным материалом для спецкурса «Криптография и криptoанализ» и спецсеминара «Криптография в задачах», проводимых авторами для студентов ММФ НГУ и учащихся СУНЦ НГУ. Пособие содержит 750 задач, охватывающих различные области криптографии и криptoанализа, а также необходимую для их решения краткую теоретическую информацию. В пособие включены как типовые задачи, так и нерешённые проблемы, требующие исследовательского подхода. Некоторые задачи в области криптографических булевых функций могут служить темами дипломных работ студентов. В пособии представлены и олимпиадные задачи по криптографии. Предназначено для школьников старших классов, студентов и преподавателей.

Рецензент  
канд. физ.-мат. наук, доц. А. Л. Пережогин

Издание подготовлено в рамках реализации *Программы развития государственного образовательного учреждения высшего профессионального образования «Новосибирский государственный университет»* на 2009–2018 годы.

ISBN 978-5-4437-0226-1

© Новосибирский государственный университет, 2014  
© А. А. Городилова, Н. Н. Токарева,  
Г. И. Шушуев, 2014

# ОГЛАВЛЕНИЕ

|   |            |
|---|------------|
| <b>От авторов</b>                                       | <b>7</b>   |
| <b>1 Криптография: основные понятия и история</b>       | <b>9</b>   |
| 1.1 Весёлые старты . . . . .                            | 9          |
| 1.2 Основные понятия . . . . .                          | 11         |
| 1.3 История и искусство . . . . .                       | 14         |
| <b>2 Олимпиадные задачи по криптографии</b>             | <b>27</b>  |
| 2.1 Математические задачи . . . . .                     | 27         |
| 2.2 Интересные задачи разных типов . . . . .            | 32         |
| 2.3 Шифры перестановки . . . . .                        | 42         |
| 2.4 Шифры замены . . . . .                              | 44         |
| 2.5 Комбинированные шифры . . . . .                     | 49         |
| 2.6 «Восстановите секретное сообщение...» . . . . .     | 52         |
| 2.7 Задачи последних олимпиад ИКСИ . . . . .            | 57         |
| 2.8 Задачи олимпиады по компьютерной безопасности . .   | 85         |
| 2.9 Задачи Белорусского государственного университета . | 86         |
| <b>3 Комбинаторные задачи</b>                           | <b>99</b>  |
| 3.1 Сочетания и перестановки . . . . .                  | 99         |
| 3.2 Метод включения и исключения . . . . .              | 104        |
| 3.3 Числа Фибоначчи . . . . .                           | 106        |
| 3.4 Латинские квадраты . . . . .                        | 107        |
| 3.5 Системы троек Штейнера . . . . .                    | 109        |
| <b>4 Элементы алгебры и теории чисел</b>                | <b>111</b> |
| 4.1 Целые числа. Алгоритм Евклида . . . . .             | 111        |
| 4.2 Простые и взаимно простые числа . . . . .           | 113        |
| 4.3 Двоичное представление чисел . . . . .              | 114        |
| 4.4 Сравнение по модулю . . . . .                       | 115        |
| 4.5 Обратный элемент и возведение в степень . . . . .   | 117        |
| 4.6 Решение сравнений первой степени . . . . .          | 120        |
| 4.7 Цепные дроби . . . . .                              | 122        |
| 4.8 Проверка простоты числа . . . . .                   | 123        |
| 4.9 Поле Галуа . . . . .                                | 126        |

|   |            |
|---|------------|
| <b>5 Криптосистемы с открытым ключом</b>                | <b>131</b> |
| 5.1 Протокол Диффи — Хеллмана . . . . .                 | 131        |
| 5.2 Криптосистема Шамира . . . . .                      | 133        |
| 5.3 Криптосистема RSA . . . . .                         | 136        |
| 5.4 Криптосистема Гольдвассер — Микали . . . . .        | 138        |
| 5.5 Криптосистема Эль-Гамаля . . . . .                  | 141        |
| <b>6 Цифровая подпись</b>                               | <b>144</b> |
| 6.1 Цифровая подпись RSA . . . . .                      | 144        |
| 6.2 Цифровая подпись Эль-Гамаля . . . . .               | 146        |
| 6.3 Цифровая подпись Фиата — Шамира . . . . .           | 147        |
| <b>7 Криптография на эллиптических кривых</b>           | <b>150</b> |
| 7.1 Эллиптическая кривая . . . . .                      | 150        |
| 7.2 Группа точек эллиптической кривой . . . . .         | 152        |
| 7.3 Протокол Диффи — Хеллмана на эллиптических кривых   | 155        |
| 7.4 Криптосистема Эль-Гамаля на эллиптических кривых    | 158        |
| <b>8 Криptoанализ асимметричных систем</b>              | <b>161</b> |
| 8.1 Атаки на основе алгоритмов факторизации . . . . .   | 161        |
| 8.2 Атаки на основе вычисления дискретного логарифма .  | 164        |
| 8.3 Частные алгоритмические атаки . . . . .             | 167        |
| 8.4 Атаки с использованием свойств ключа . . . . .      | 170        |
| <b>9 Теория секретности Шеннона</b>                     | <b>173</b> |
| 9.1 Совершенно секретные системы . . . . .              | 173        |
| 9.2 Избыточность языка открытых текстов . . . . .       | 176        |
| 9.3 Расстояние единственности шифра . . . . .           | 179        |
| <b>10 Анализ псевдослучайных последовательностей</b>    | <b>181</b> |
| 10.1 Линейные рекуррентные последовательности . . . . . | 181        |
| 10.2 Минимальный период ЛРП . . . . .                   | 182        |
| 10.3 Алгоритм Берлекэмпа — Мэсси . . . . .              | 184        |
| <b>11 Булевые функции</b>                               | <b>188</b> |
| 11.1 Булев куб. Метрика Хэмминга . . . . .              | 188        |
| 11.2 Грани и подпространства . . . . .                  | 190        |
| 11.3 Алгебраическая нормальная форма булевой функции    | 192        |

|   |            |
|---|------------|
| <b>Оглавление</b>   | <b>5</b>   |
| 11.4 Характеристики булевой функции . . . . .                 | 194        |
| 11.5 Спектр Уолша — Адамара . . . . .                         | 197        |
| 11.6 Классификация булевых функций . . . . .                  | 199        |
| 11.7 Трейс-форма булевой функции . . . . .                    | 204        |
| <b>12 Криптографические свойства булевых функций</b>          | <b>207</b> |
| 12.1 Сбалансированность . . . . .                             | 207        |
| 12.2 Устойчивость и корреляционная иммунность . . . . .       | 208        |
| 12.3 Алгебраическая иммунность . . . . .                      | 210        |
| 12.4 Высокая нелинейность . . . . .                           | 212        |
| <b>13 Векторные булевые функции (S-блоки)</b>                 | <b>217</b> |
| 13.1 Основные понятия . . . . .                               | 217        |
| 13.2 Нелинейные функции . . . . .                             | 219        |
| 13.3 Дифференциальноправномерные функции . . . . .            | 221        |
| 13.4 Связь АВ- и APN-свойств . . . . .                        | 224        |
| 13.5 Эквивалентность векторных функций . . . . .              | 225        |
| 13.6 Алгебраическое представление векторной функции . . . . . | 227        |
| <b>14 Криptoанализ симметричных шифров</b>                    | <b>229</b> |
| 14.1 Частотный анализ . . . . .                               | 229        |
| 14.2 А попробуем и мы! . . . . .                              | 230        |
| 14.3 Линейный криptoанализ . . . . .                          | 232        |
| 14.4 Дифференциальный криptoанализ . . . . .                  | 241        |
| 14.5 Алгебраический криptoанализ . . . . .                    | 244        |
| <b>15 Трудные и нерешённые задачи о булевых функциях</b>      | <b>250</b> |
| 15.1 Экстремальные булевые функции . . . . .                  | 250        |
| 15.2 Автоморфизмы различных классов булевых функций . . . . . | 254        |
| 15.3 Бент-функции и сильно регулярные графы . . . . .         | 255        |
| <b>16 Задачи на программирование</b>                          | <b>257</b> |
| 16.1 Простые навыки . . . . .                                 | 257        |
| 16.2 Криптографические задачи . . . . .                       | 263        |
| <b>Ответы к задачам</b>                                       | <b>270</b> |
| <b>Список литературы</b>                                      | <b>322</b> |



Всё, что видим мы, видимость только одна.  
Далеко от поверхности моря до дна.  
Полагай несущественным явное в мире,  
Ибо тайная сущность вещей не видна.

О. Хайям

# ОТ АВТОРОВ

Мы разделяем убеждение в том, что по-настоящему познакомиться с той или иной областью знаний можно лишь решая задачи. В том числе — сложные и нерешённые. Так возникла идея этого пособия.

В пособии мы постарались собрать математические задачи, охватывающие различные области криптографии и криптоанализа, а также необходимую для их решения краткую информацию по теории. Среди них как типовые задачи, так и открытые проблемы, требующие исследовательского подхода и увлечённости. Некоторые задачи в области криптографических булевых функций могут служить темами дипломных работ студентов и отдельных научных публикаций. Для указания сложных задач мы используем обозначения: \* для задач, требующих смекалки, \*\* для более сложных задач, но решения которых известны, \*\*\* для нерешённых задач.

Задачник во многом опирается на учебное пособие [33] по симметричной криптографии и в некотором роде служит его продолжением.

В первой главе пособия представлена серия заданий на знание основных терминов криптографии и её истории. Далее предлагаются задачи по таким направлениям математики и криптографии, как:

- комбинаторика, теория чисел, конечные поля;
- булевы функции и их криптографические свойства;
- теория секретности Шеннона;
- линейные рекуррентные последовательности;
- криптография с открытым ключом;
- криптоанализ.

Отдельное внимание уделяется олимпиадным задачам. Их решение будет полезно при подготовке к олимпиадам по криптографии, в том числе к ежегодной олимпиаде по криптографии и математике, проводимой Институтом криптографии, связи и информатики.

Авторы очень благодарны А. Л. Пережогину за полезные замечания по тексту работы, С. В. Агиевичу за предоставленные криптографические задачи Белорусского государственного университета, Николаю Коломейцу и Валерии Виткуп за предложения и активную помощь в работе над пособием.

*Анастасия Городилова, Наталья Токарева, Георгий Шушуев  
Академгородок, Новосибирск*



# ГЛАВА 1. КРИПТОГРАФИЯ: ОСНОВНЫЕ ПОНЯТИЯ И ИСТОРИЯ

В этой главе мы предлагаем ряд заданий по криптографии, связанных с её понятиями, историей, влиянием на культуру и искусство.

Желаем удачи!

## 1.1 Весёлые старты

**Задача 1. Слова.** Кроме выделенного слова найдите на картинке  
ещё 30 слов, связанных с криптографией.



**Задача 2. Вам сообщение!** Известно, что естественные языки избыточны. Например, русский язык избытен примерно на 73 %, английский — на 75 %. Проверьте это на деле и прочитайте следующие сообщения:

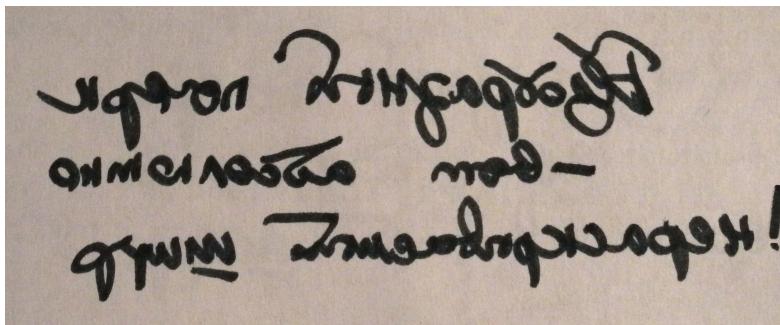
a) TH15 M3554G3 53RV35 T0 PR0V3 H0W OUR M1ND5 C4N D0  
4M4Z1NG TH1NG5! 1MPR3SS1V3 TH1NG5! 1N TH3 B3G1NN1NG 1T  
W4S H4RD BUT N0W, ON TH15 L1N3 Y0UR M1ND 1S R34D1NG 1T  
4UT0M4T1C4LLY W1TH PR4CT1C4LLY N0 TH1NK1NG 1NV0LV3D  
R1GHT? B3 V3RY PR0UD! Y0U D35ERVE 4 P4T 0N TH3 B4CK!  
R3P05T 1F Y0U C4N R34D 1T :)

б) ‘ +‘к\*=\*ръя w‘б з\$+\$-ый;  
 З+(т(я ц\$пь -( w‘б\$ т\*=:  
 # w-\$= # -\*чью к\*t ‘ч\$-ый  
 Bс\$ x\*w#t п\* ц\$p# кр‘г\*=;

**Задача 3.** Дешифруйте сообщение:

В\*т\*р з\*б\*р\*лс\* в п\*ст\*\* к\*мн\*т\* \* в п\*чн\*\* в\*ющ\*\* тр\*б\*,  
 \* ст\*р\*й д\*м, в\*сь р\*сш\*т\*нн\*й, д\*р\*в\*й, п\*л\*р\*зв\*л\*вш\*йс\*,  
 вдр\*г \*ж\*вл\*лс\* стр\*нн\*м\* зв\*к\*m\*, к к\*t\*р\*m \* пр\*сл\*ш\*в\*лс\*  
 с н\*в\*льн\*й тр\*в\*г\*й. В\*т т\*чн\* взд\*хн\*л\* чт\*-т\* в б\*л\*й з\*л\*,  
 взд\*хн\*л\* гл\*б\*k\*, пр\*р\*в\*ст\*, п\*ч\*льн\*. В\*т з\*x\*д\*л\* \*  
 з\*скр\*п\*л\* гд\*-т\* д\*л\*k\* в\*c\*xш\*\* гн\*л\*\* п\*л\*в\*ц\* п\*д чь\*m\*-т\*  
 т\*ж\*л\*m\* \* б\*cш\*mн\*m\* ш\*г\*m\*.

**Задача 4.** Вашему вниманию — ещё одно секретное сообщение:



**Задача 5.** Восстановите открытый текст и опишите метод шифрования, с помощью которого было получено сообщение:

сВредцкежаодтйурндсоитркеоствязоомижсоята. Э. найтшиен

**Задача 6.** Прочитайте отрывок из замечательного стихотворения Г. Шпаликова:

По несчастью или к счастью, / Выглядит вполне, / Никогда не возвращайся / Ни тебе, ни мне. / Даже если пепелище / Истина проста: / Не найти того, что ищем, / В прежние места.

## 1.2 Основные понятия

Серия вопросов этого раздела поможет вам проверить начальные знания основных криптографических терминов. Для основательного знакомства с терминологией рекомендуем книги [29] и [37].

**Задача 7. Криптографические термины I.** Для каждого термина выберите правильное определение.

1. *Криптография* — это

- а) научная деятельность, связанная с разработкой криптографических средств защиты информации;
- б) искусство создания шифров;
- в) научная и практическая деятельность, связанная с разработкой криптографических средств защиты информации, а также анализом и обоснованием их криптографической стойкости;
- г) искусство тайнописи;
- д) научная и практическая деятельность по исследованию криптографических алгоритмов с целью получения обоснованных оценок их криптографической стойкости.

2. *Криptoанализ* — это

- а) научная деятельность, связанная с разработкой методов взлома шифров;
- б) наука о дешифровании;
- в) научная и практическая деятельность, связанная с разработкой криптографических средств защиты информации, а также анализом и обоснованием их криптографической стойкости;
- г) искусство взлома шифров;
- д) научная и практическая деятельность по исследованию криптографических алгоритмов с целью получения обоснованных оценок их криптографической стойкости.

3. *Криптология* — это

- а) понятие, объединяющее криптографию и криptoанализ;
- б) синоним термина «криптография»;
- в) синоним термина «криptoанализ».

**Задача 8. Криптографические термины II.** Для каждого термина выберите правильное определение.

1. *Открытый текст* — это

- а) информация, находящаяся в открытом доступе;
- б) секретное сообщение, подлежащее зашифрованию;
- в) рассекреченная информация;
- г) часть открытого ключа;
- д) несекретное сообщение.

2. *Шифртекст* — это

- а) секретное сообщение, подлежащее зашифрованию;
- б) информация, находящаяся в закрытом доступе;
- в) часть закрытого ключа;
- г) результат зашифрования;
- д) засекреченная информация.

3. *Ключ* — это

- а) объединение закрытого и открытого ключей абонента;
- б) изменяемый элемент (параметр) шифра, каждому значению которого однозначно соответствует одно из отображений, реализуемых шифром;
- в) изменяемый элемент (параметр) шифра, с помощью которого осуществляется зашифрование;
- г) информация, позволяющая восстанавливать открытый текст;
- д) информация, доступ к которой пытаются получить злоумышленник.

**Задача 9. Соответствие I.** Установите соответствие между понятиями и их определениями.

Понятия:

- 1) авторизация;
- 2) аутентификация;
- 3) идентификация.

Определения:

- а) установление (т. е. проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: содержания и источника передаваемых сообщений, сеанса связи, времени взаимодействия и т. д. Является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон;

- б) процедура предъявления абонентом взаимодействия его уникального системного имени — идентификатора, которое позволяет отличать его от других абонентов;
- в) процесс предоставления пользователю прав на определённые ресурсы. Обычно выполняется после успешной аутентификации.

В каком порядке обычно проводятся эти процедуры?



**Задача 10. Соответствие II.** Установите соответствие между понятиями и их определениями.

Понятия:

- 1) шифрование;
- 2) расшифрование;
- 3) дешифрование;
- 4) зашифрование.

Определения:

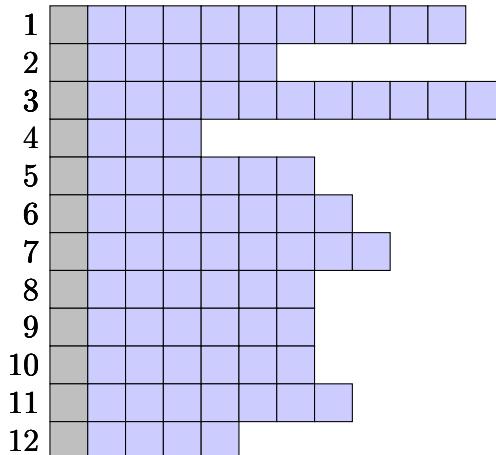
- а) процесс преобразования открытого текста в шифртекст с помощью функции шифрования, зависящей от ключа;
- б) термин, объединяющий зашифрование и расшифрование;
- в) процесс восстановления открытого текста из шифртекста, реализуемый при известном значении ключа (процесс, обратный зашифрованию);
- г) процесс получения открытого текста из шифртекста без предварительного знания ключа.

## 1.3 История и искусство

Вопросы этого раздела связаны с историей криптографии. Большая часть из них — по истории криптографии в России.

В качестве литературы по истории криптографии рекомендуем книги и статьи Т. А. Соболевой [30], Ю. И. Гольева, Д. А. Ларина, А. Е. Тришиной, Г. П. Шанкина [14], А. В. Бабаша и др. [4], [5], [6], Л. С. Бутырского и др. [7], Д. Кана [16], С. Сингха [28], обзор в пособии [33], статью Г. П. Агибалова [2], сборник [25], главы по истории в книгах А. П. Алфёрова, А. Ю. Зубова, А. С. Кузьмина, А. В. Черёмушкина [3], В. И. Нечаева [22] и другие.

**Задача 11.** Отгадайте криптографический кроссворд.



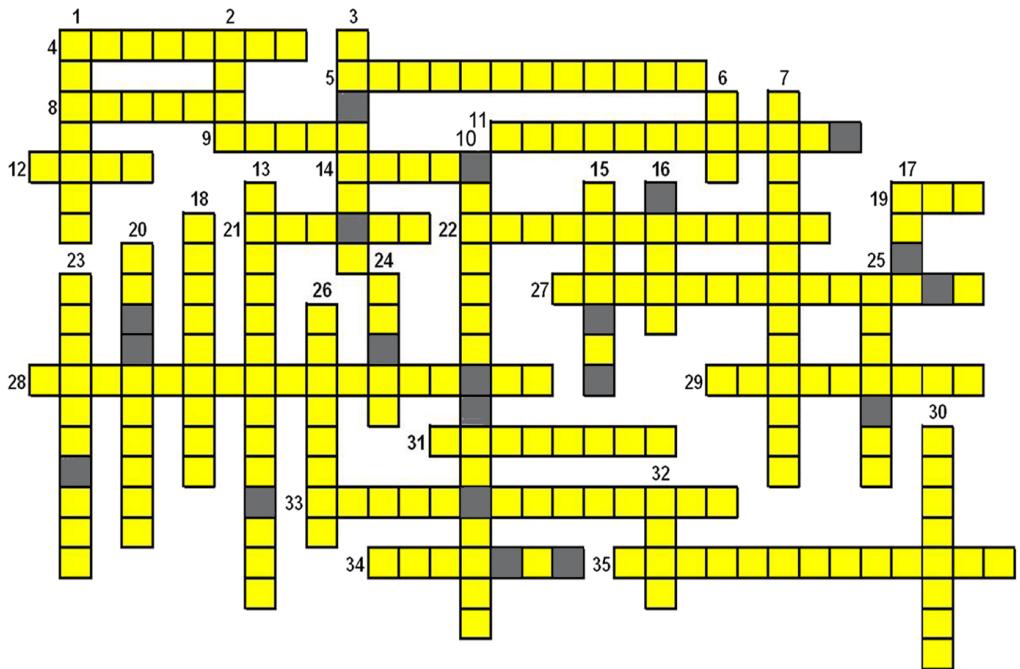
1) Фамилия выдающегося советского криптографа, «патриарха секретной телефонии», под руководством которого была разработана специальная шифровальная аппаратура во время Великой Отечественной войны. С помощью этой аппаратуры СССР удалось обеспечить надёжную секретную связь самого высокого уровня, что внесло существенный вклад в нашу победу.

2) Один из авторов самой известной крипtosистемы с открытым ключом. Кстати, это он назвал криптографию «повивальной бабкой всех компьютерных наук».

- 3) Дополнительная информация, которая добавляется к секретному сообщению с целью обеспечить его целостность и аутентификацию источника данных.
- 4) Один из правителей России, принимавший личное участие в разработке и использовании шифров.
- 5) Британский ученый, осуществлявший взлом немецкой шифрмашиной «Энигма» с помощью разработанной им вычислительной техники.
- 6) Вице-канцлер России (1725 г.), при котором шифры стали неалфавитными — кодировались уже комбинации букв, а в качестве шифробозначений начали использоваться цифры.
- 7) Русский писатель и дипломат, использовавший в своей переписке шифр «решётка Кардано». Созданная им знаменитая пьеса разлетелась на цитаты.
- 8) Французский кардинал, прославившийся в криптографии разработкой собственного шифра перестановки: открытый текст разбивался на отрезки, внутри каждого отрезка буквы переставлялись в соответствии с фиксированной перестановкой.
- 9) Ещё один автор самой известной крипtosистемы с открытым ключом.
- 10) Известный учёный, «отец американской криптографии», предложивший термин «криптоанализ».
- 11) Родина математика, в честь которого двузначные функции названы булевыми.
- 12) Американский криптограф, выпустивший книгу воспоминаний «Американский чёрный кабинет». Книга навлекла преследование автора со стороны США.

**Задача 12. Дешифрование «Энигмы».** Назовите фамилии польских математиков, выпускников Познанского университета, разработавших первый математический аппарат для дешифрования немецкой шифрмашиной «Энигма».

**Задача 13. (\*)** Отгадайте кроссворд, посвящённый криptoанализу.



- 1) Для стойкости крипосистемы его сформулировал Керкгоффс.
- 2) То, что хотел бы получить злоумышленник.
- 3) Часть шифрсистемы, которая полагается известной злоумышленнику.
- 4) Иногда криптографическая атака может быть направлена на него, а не на шифрсистему.
- 5) Метод приведения системы уравнений к линейному виду (например, в алгебраическом криptoанализе).
- 6) «Международное» имя злоумышленника.
- 7) Группа методов криptoанализа, направленных на точное (невероятностное) восстановление информации о ключе.
- 8) Воинственный клич злоумышленника.
- 9) Разложение его на множители является трудной задачей, лежащей в основе нескольких крипосистем с открытым ключом.
- 10) Метод криptoанализа, опирающийся на статистический анализ пар открытых текстов и соответствующих им пар шифртекстов, разности между которыми определены.

- 11) Способ защиты от атак по сторонним каналам, заключающийся в усложнении компонентов шифра (например, S-блоков) при их реализации.
- 12) На анализ чего направляет свои усилия злоумышленник?
- 13) Информационные системы должны обладать этим видом устойчивости.
- 14) Часть итерированного шифра.
- 15) Фамилия криптографа, предложившего один из самых популярных методов разложения числа  $n = pq$  на множители, названный в его честь.
- 16) Автор одного из самых известных методов криptoанализа системы RSA. Метод также назван в его честь.
- 17) Единица зашифрования в блочном шифре.
- 18) Метод криptoанализа симметричных шифров, предложенный в 1999 г. А. Бирюковым и Д. Вагнером. Особенностью метода является то, что его успешность не зависит от числа раундов шифра.
- 19) Единица измерения информации.
- 20) Именно «здесь» происходит «встреча» в одном из известных методов криptoанализа.
- 21) Название одной из самых известных криptoаналитических операций XX в., направленной на дешифрование «Энигмы».
- 22) Трудная задача, которая лежит в основе криptoсистемы RSA.
- 23) Другое (российское) название метода криptoанализа 10).
- 24) Так называлась первая ЭВМ, созданная для решения задач криptoанализа.
- 25) Криptoанализ с ним подойдет для любого шифра (однако эффективность метода не гарантирована).
- 26) Принцип, использующийся в криptoанализе, в названии которого фигурирует один из праздников.
- 27) Метод криptoанализа, для работы которого требуется минимальное количество пар «открытый текст — шифртекст».
- 28) В одном из методов криptoанализа по сторонним каналам проводится измерение именно этого параметра.
- 29) Противоположность активному криptoанализу.
- 30) Документ, разрешающий выполнение тех или иных действий.
- 31) Один из методов статистического криptoанализа.
- 32) Значение, которое может принимать бит.

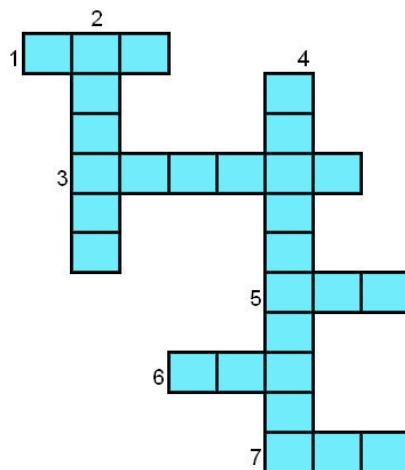
33) Метод статистического криптоанализа, применяющийся в основном к поточным шифрам.

34) Легальный пользователь системы.

35) Нелегальный или нечестный пользователь, ставящий задачу получить (или изменить) чужую секретную информацию.

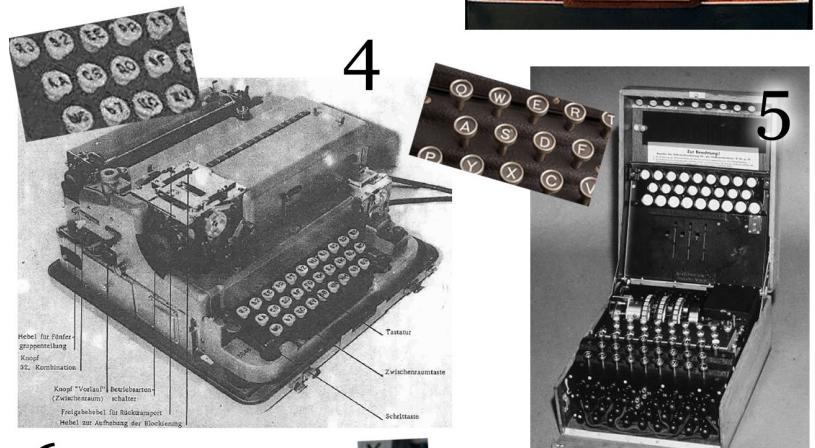
\*\*) Расшифруйте вопрос, заданный в серых клетках.

**Задача 14.** Отгадайте кроссворд на английском языке.



- 1) Самая известная крипtosистема с открытым ключом.
- 2) Один из авторов дифференциального криптоанализа.
- 3) Итальянский криптограф, предложивший понятие псевдослучайного генератора.
- 4) Криптограф, предложившая вместе с учёным 3) принцип вероятностного шифрования, а также идеи протоколов с нулевым разглашением.
- 5) Иначе этот шифр называют Rijndael.
- 6) Симметричный шифр, в котором вместо сложения по модулю 2 используется сложение по модулю  $2^{32}$ .
- 7) Поточный шифр, использовавшийся в системе безопасности беспроводных сетей WEP.

**Задача 15. Шифрмашины.** Определите, фотографии каких шифрмашин приведены на следующем рисунке.



**Задача 16. (\*) «Рифы и мифы острова Оденсхольм».** В 1914 г. — сто лет назад — возле острова Оденсхольм в Балтийском море потерпел крушение немецкий крейсер «Магдебург». В результате его захвата русские моряки получили в распоряжение экземпляры «Сигнальной книги» германского флота. Со временем эта история «обогатилась» множеством вымыщленных подробностей и по сути превратилась в красивую легенду, миф. Её изложение можно найти в нескольких современных книгах и статьях, к числу которых относится и учебное пособие [33]. Отчасти такую судьбу «Магдебург» обрёл из-за долгого отсутствия серьёзных военно-исторических публикаций на эту тему.

Обсуждению подлинной истории крейсера «Магдебург» и мифам вокруг неё посвящены статьи *«Рифы и мифы острова Оденсхольм. К истории захвата секретных документов германского флота на крейсере “Магдебург” в августе 1914 года»*, *«“Магдебургская” история — “работа над ошибками”»* (автор — М. А. Парталя) в журнале *«Защита информации. Inside»* (2007, 2014). Мы благодарны автору статей за указание на эти работы.

Предлагаем вам изучить этот эпизод истории отечественной радиоразведки, и ответить на следующие вопросы.

- 1) Какие документы были захвачены на «Магдебурге»?
  - а) военные шифры германского флота;
  - б) шифры Германии мирного времени;
  - в) секретные карты квадратов Балтийского моря;
  - г) «Сигнальная книга» германского флота;
  - д) кодовые книги Великобритании.
- 2) Какие последствия вызвал захват секретных документов?
  - а) вскрытие действующих шифров германского флота;
  - б) чтение шифрованных радиограмм Германии;
  - в) чтение нешифрованных радиограмм Германии;
  - г) чтение шифрованных радиограмм союзников Германии;
  - д) смену шифра германского флота;
  - е) активизацию русской радиоразведки на Балтийском море.
- 3) Назовите руководителя радиоразведки Балтийского флота — специалиста, принимавшего непосредственное участие в дешифровании шифра «гамма–альфа» для германской радиосвязи:
  - а) М. В. Гамильтон;
  - б) А. И. Непенин;
  - в) И. И. Ренгартен.

186

| Zahlen-<br>Signal | Buchstaben-<br>Signal | Bedeutung   |
|-------------------|-----------------------|---|
| 505 54            | A S C                 | Aluminium   |
| 55.               | A S D                 | am  |
| 56                | A S E                 | Ambulanz  |
| 57                | A S F                 | Amerikaner -isch                                  |
| 58                | A S G                 | Amnestie -ren                                     |
| 59                | A S H                 | Ampere, Ampèremeter<br>gebe mit (n) Ampère in der |
| 505 60            | A S I                 | Amplitude   |
| 61                | A S J                 | Amputation, amputieren                            |
| 62                | A S K                 | Amt -lich, Amts- [s. A.<br>Liste]                 |
| 63                | A S L                 | an  |
| 64                | A S M                 | an mich   |
| 65                | A S N                 |   |

371

| Zahlen-<br>Signal | Buchstaben-<br>Signal | Bedeutung  |
|-------------------|-----------------------|--|
| 694 05            | U I C                 | unbrauchbar -keit (als, weg<br>Geschütz, Munition) |
| 06                | U I D                 | unbrauchbar geworden (durch,                       |
| 07                | U I E                 | und  |
| 08                | U I F                 | und so weiter                                      |
| 09                | U I G                 | undank -bar -keit                                  |
| 694 10            | U I H                 | undenkbar  |
| 11                | U I J                 | undeutlich -keit                                   |
| 12                | U I K                 | undicht -igkeit                                    |
| 13                | U I L                 | undurchführbar -keit                               |
| 14                | U I M                 | undurchlässig -keit                                |
| 15                | U I N                 | undurchsichtig -keit                               |
| 16                | U I O                 | uneben -heit                                       |
| 17                | U I P                 |  |

Фрагменты страниц германской «Сигнальной книги».

**Задача 17. (\*) Даты.** Установите соответствие между годами и событиями в истории криптографии и защиты информации.

- 1) AES становится стандартом США.
- 2) Образована Высшая школа криптографов (СССР).
- 3) Создана Академия криптографии (РФ).
- 4) Образована «Лаборатория Касперского» (РФ).
- 5) Создан Спецотдел при ВЧК.
- 6) А. Шербиус изобретает шифрмашину «Энигма».
- 7) Появляется работа К. Шеннона «Теория связи в секретных системах».
- 8) У. Диффи и М. Хеллмана публикуют свою работу, положив тем самым начало асимметричной криптографии.
- 9) Изобретена система RSA.
- 10) Появляется метод линейного криптоанализа М. Мацуи.
- 11) Математик Х. Гольдбах становится первым профессиональным криптоаналитиком на службе российской криптографии.

Годы: а) 1921; б) 1993; в) 1742; г) 1997; д) 1978; е) 1949; ж) 1918; з) 2002; и) 1992; к) 1949; л) 1976.

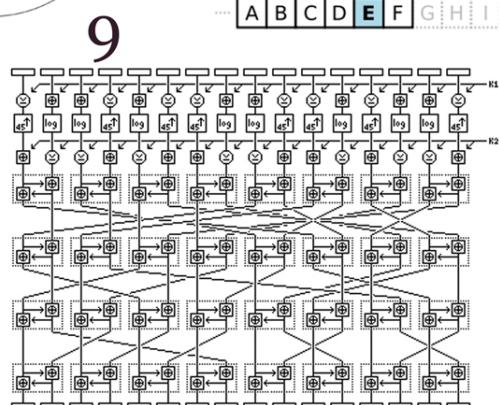
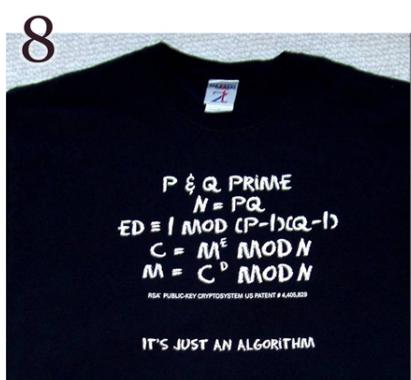
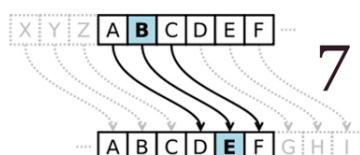
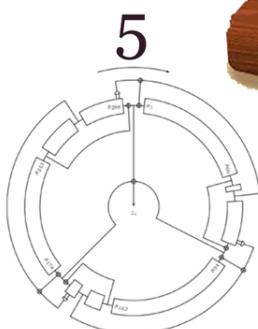
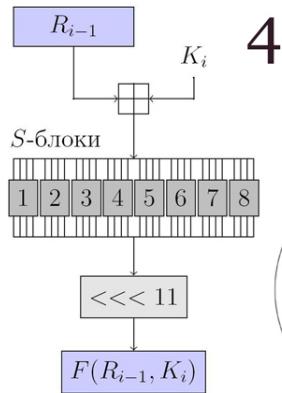
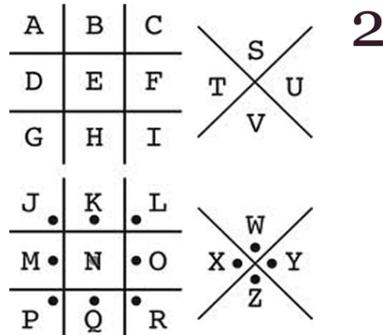
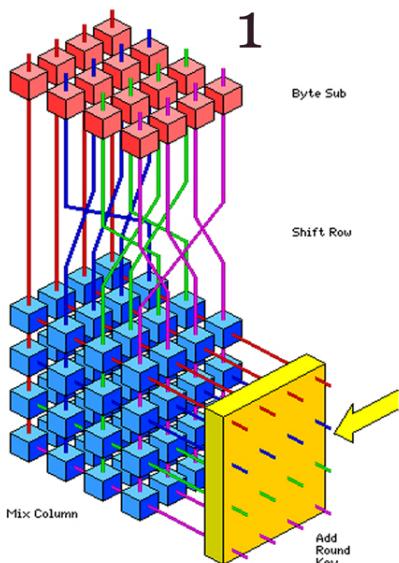
**Задача 18. (\*\*) Советская криптографическая служба.** Для каждого вопроса выберите один или несколько правильных ответов.

1. Какое название получила новая криптографическая служба России, созданная 5 мая 1921 г.?
  - а) Спецотдел ВЧК;
  - б) Особый отдел ВЧК;
  - в) Секретный отдел ВЧК;
  - г) Отдел внешней разведки ВЧК.
2. Кто был первым руководителем этой службы?
  - а) Ф. Э. Дзержинский;
  - б) Г. В. Чicherin;
  - в) Г. И. Бокий;
  - г) Я. Х. Петерс.
3. Кто из криптографов царской России работал в новой криптографической службе? Выберите несколько ответов.
  - а) И. А. Зыбин;
  - б) М. Раевский;
  - в) А. М. Горчаков;
  - г) В. И. Кривош-Неманич;
  - д) И. М. Ямченко;
  - е) Б. А. Аронский;
  - ж) С. С. Толстой.
4. Шифры каких стран частично или полностью были дешифрованы сотрудниками советской криптографической службы в 1920–30-е гг.?
  - а) Франция;
  - б) Германия;
  - в) Италия;
  - г) Турция;
  - д) Япония;
  - е) США;
  - ж) Великобритания.
5. Как называлась сложная засекречивающая аппаратура для речевого сигнала, разработанная во время Великой Отечественной войны в лаборатории В. А. Котельникова? Эта аппаратура позволила обеспечить надёжную секретную радиосвязь в СССР на протяжении войны и после неё.
  - а) М-125 Фиалка;
  - б) Инвертор ЕС;
  - в) ГОСТ 28147-89;
  - г) Энигма;
  - д) Москва;
  - е) Соболь-П.

**Задача 19.** Кто из перечисленных математиков и философов имел непосредственное отношение к криптографии? Какое?

- а) Х. Гольдбах;
- б) Аристотель;
- в) М. В. Келдыш;
- г) Ф. Эпинус;
- д) С. Л. Соболев;
- е) Н. Н. Лузин;
- ж) М. А. Лаврентьев;
- з) А. Н. Колмогоров;
- и) Пифагор;
- к) М. В. Остроградский;
- л) Н. И. Лобачевский;
- м) А. О. Гельфонд;
- н) А. А. Марков;
- о) Л. Эйлер.

**Задача 20. Шифры.** Определите, какие шифры или их элементы изображены на следующем рисунке.



Криптографические методы нередко упоминаются в художественной литературе, а сами криптографы и разведчики становятся прототипами героев книг и художественных фильмов. Теме «Криптография в искусстве» посвящены следующие задания.

### Задача 21. Разведчики и криптографы в кино.

- 1) Назовите имя сотрудника гестапо — советского разведчика, послужившего одним из прототипов Штирлица (фильм «Семнадцать мгновений весны»).
- 2) Знание шифровального дела способствовало внедрению этого агента разведки красногвардейцев в штаб Добровольческой армии во время Гражданской войны. Он стал прототипом главного героя фильма «Адъютант его превосходительства». Назовите этого человека.

### Задача 22. Художественные произведения. Определите, из каких художественных произведений взяты следующие отрывки:

- 1) «Савелий показал Саше, как надо перестукиваться: алфавит делится на шесть рядов, по пять букв в каждом. Первые удары означают ряд, вторые — место буквы в ряду. Между ударами короткие паузы — это ряд; между буквами паузы чуть длиннее, между словами еще длиннее, царапание по стене — “кончил” или “стоп!” или “повторите!”. Паузы и интервалы совсем крошечные, у опытных заключенных они измеряются долями секунды. В паузах и главная трудность — если их не уловить, звуки сливаются, получается не та буква и теряется смысл.

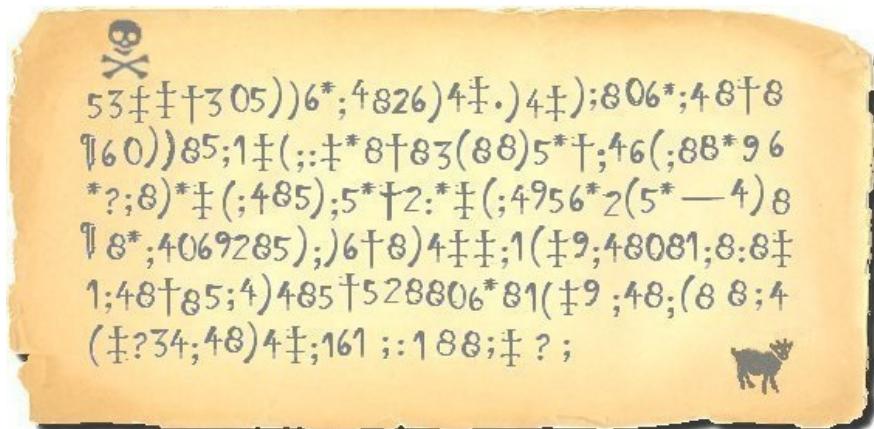
Обгоревшей спичкой Саша написал алфавит на картоне от пирожной коробки и начал перестукиваться. Стучал он медленно, с большими паузами, лежа на койке, прикрывшись одеялом, чтобы не услышал надзиратель. Сосед понимал его, но Саша понимал плохо, путал буквы, просил повторить, хотя сосед стучал чётко, ясно, с длинными паузами.»

- 2) «Штирлиц достал из книжного шкафа томик Монтеня, перевёл цифры в слова и соотнёс эти слова с кодом, скрытым среди мудрых истин великого и спокойного французского мыслителя. “Кем они считают меня? — подумал он. — Гением или всемогущим? Это же немыслимо...”»

3) «Долгий овал его лица, острый профиль, властная манера разговаривать с тюремной администрацией и ёщё тот едва голубоватый свет выцветших глаз, который даётся только абстрактным умам, — всё это странно делало Челнова похожим не то на Декарта, не то на Архимеда. Он был прислан для разработки математических оснований абсолютного шифратора, то есть прибора, который своим механическим вращением мог бы обеспечить включение и переключение множества реле, так запутывающих порядок посылки прямоугольных импульсов изуродованной речи, чтобы даже сотни людей, поставив аналогичные приборы, не могли бы расшифровать разговора, идущего по проводам. В конструкторском бюро своим чередом шли поиски конструктивного решения подобного шифратора.»

4) «Через несколько минут, когда сковорода накалилась, я вынул пергамент и с невыразимым восторгом увидел, что кое-где на нём появились знаки, напоминавшие цифры и расположенные в строку. Я снова положил пергамент на сковороду и подержал ёщё над огнем. Тут надпись выступила вся целиком — сейчас я вам покажу.

— Что ж! — сказал я, возвращая Леграну пергамент, — меня это не подвинуло бы ни на шаг. За все алмазы Голконды я не возьмусь решать подобную головоломку.»



5) «Андрей жил теперь на сумском подворье. Встретясь первый раз с Ваничкой и узнав, что работа близка к концу, дня два осталось, он, успокоенный, решил эти два дня посвятить учению: почитать с

толком книгу “Кожевенное производство”, купленную ещё в Петербурге. Читать было всё недосуг, а нужно. Вдруг — сообщение, Колька принёс, Ваничkin подручный, писано шифром. Здесь, в Харькове, ключевым словом было “ШТУНДИСТЫ”. Андрей ещё не привык читать сразу, в уме, пришлось набросать сетку: “Штундисты” написать колом, по-китайски, и затем к каждой букве приписать девять, следующих по алфавиту. В результате прочитал: “Срочно искать другое место пять на горке.”»

6) «В штабном вагоне, где разместились офицеры маршевого батальона, с начала поездки царила странная тишина. Большинство офицеров углубилось в чтение небольшой книжки в полотняном переплете, озаглавленной “Грехи отцов” Роман Людвига Гангофера. Все одновременно сосредоточенно изучали страницу сто шестьдесят первую. Командир батальона капитан Сагнер стоял у окна и держал в руке ту же книжку, открытую на той же сто шестьдесят первой странице. <...>

— Перед нами совершенно секретная информация, касающаяся новой системы шифровки полевых депеш. <...> Система, которую я вам объяснил, является не только одной из лучших, но, можно сказать, одной из самых непостигаемых. Все отделы контрразведки вражеских штабов теперь могут заткнуться, они скорее лопнут, чем разгадают наш шифр.»

## ГЛАВА 2. ОЛИМПИАДНЫЕ ЗАДАЧИ ПО КРИПТОГРАФИИ

Ежегодно Институт криптографии, связи и информатики Академии ФСБ России (ИКСИ) проводит олимпиаду по математике и криптографии для школьников, результаты выступления на которой учитываются при приёме в вузы. Олимпиада проходит в ноябре с выездом во многие города России, в том числе и в Новосибирск. Задачи рассчитаны на учащихся 8–11 классов, но в олимпиаде могут принять участие и более юные школьники.

В данной главе приведены задачи для подготовки к этой олимпиаде; ряд задач поможет в подготовке к олимпиаде школьников по информатике и компьютерной безопасности ([www.cryptolymp.ru/olmp\\_it](http://www.cryptolymp.ru/olmp_it)). Большинство задач взято с сайта [www.cryptolymp.ru](http://www.cryptolymp.ru), из сборника «Олимпиады по криптографии и математике для школьников» А. Ю. Зубова, А. В. Зязина, В. Н. Овчинникова, С. М. Рамоданова [15], книги В. В. Ященко [39].

Однако олимпиада ИКСИ не единственная. Соревнования по информационной безопасности и криптографии проходят в разных городах и странах мира. Так, в разделе 2.9 мы приводим непростые и очень любопытные задачи, предлагаемые студентам Белорусского государственного университета. Скоро студенческая олимпиада по криптографии пройдёт и в Новосибирском государственном университете. Приглашаем вас принять в ней участие!

### 2.1 Математические задачи

В этом разделе предлагается серия математических задач олимпиады ИКСИ для школьников.

**Задача 23.** Известно, что число вхождений некоторого символа в текст составляет от 10,5 до 11 % длины текста. Найдите минимально возможную длину текста.

**Задача 24. Кодовый замок.** На кодовом замке имеется круглый диск с риской. Вокруг диска нанесены числа от 0 до 99 по часовой стрелке. Для управления замком служат две кнопки: «вправо»

и «влево». При нажатии на кнопку «вправо» диск вращается на 43 деления по часовой стрелке, при нажатии на кнопку «влево» — на 20 делений против часовой стрелки. Каждая из этих операций выполняется за 1 секунду. Изначально замок установлен на число 0. Замок открывается при его установке на число 50 — ключ замка. Ответьте на следующие вопросы.

- а) За какое наименьшее время можно открыть замок при данном ключе 50?
- б) Докажите, что замок можно открыть при любом ключе (ключ — число от 1 до 99).
- в) За какое наименьшее время можно гарантированно открыть замок при любом ключе?

**Задача 25.** Криптоша изобрёл устройство, которое позволяет вычислить среднее арифметическое любых 9 чисел или любых 223 чисел. Как правильно использовать это устройство, чтобы найти среднее арифметическое любых 2006 чисел? При необходимости Криптоша может дополнительно провести одно деление и одно умножение.

**Задача 26.** Пусть  $a_1, a_2, a_3, \dots$  и  $b_1, b_2, b_3, \dots$  — числовые последовательности периодов 16 и 2013 соответственно. Найдите период последовательности  $a_1, b_1, a_2, b_2, a_3, b_3, \dots$  (периодом последовательности  $x_1, x_2, x_3, \dots$  называется наименьшее натуральное число  $T$  такое, что для всех натуральных  $n$  верно равенство  $x_{n+T} = x_n$ ).

**Задача 27. Бильярд.** Бильярдные шары плотно уложены в правильный треугольник с основанием из 2013 шаров. На каждом шаре написано вещественное число. Сумма трёх чисел, написанных на шарах при вершинах исходного треугольника, а также любых треугольников со сторонами, параллельными исходному треугольнику, равна 0. Какие числа могут быть написаны на шарах?

**Задача 28.** Пусть  $C_n(a, b) = abab\dots ab$  — целое число, десятичная запись которого образована  $n$ -кратным повторением пары цифр  $a$  и  $b$ , где  $a \neq 0$ . Выясните, при каких  $n$  число  $C_n(a, b)$  делится на 21 при любых значениях  $a$  и  $b$ .

**Задача 29. Серверы.** В здании находится восемь серверов. Они расположены в вершинах куба. Эти серверы объединены в сеть, при чём два сервера соединены линией связи «напрямую» в том и только том случае, когда они соответствуют двум соседним вершинам куба. Кроме того, два из этих серверов соединены дополнительно по радиоканалу.

Какое наименьшее число основных линий связи придётся вывести из строя злоумышленнику, для того чтобы потерялась связность сети (т. е. станет невозможно доставить информацию с одного сервера на другой, даже через серверы-посредники)?

**Задача 30.** Разложите на простые множители число  $3^{20} + 3^4 + 1$ , если известно, что оно делится на 167.

**Задача 31.** В бесконечной последовательности цифр 2, 0, 0, 8, 0, 8, 6 ... каждая цифра, начиная с пятой, равна последней цифре в десятичной записи суммы четырёх предыдущих цифр. Докажите, что в этой последовательности вновь встретятся подряд идущие цифры 2, 0, 0, 8.

**Задача 32.** Число  $n$  представляется в виде произведения двух простых чисел  $n = p \cdot q$ . Найдите эти числа и приведите решение, если известно, что

- а)  $n = 40003200063$ , а  $|p - q| = 2$ ;
- б)  $n = 40000398401$ , а  $p, q$  — простые и  $|p - q| \leq 100$ .

**Задача 33.** Делится ли число  $2^{2^{2007}+3^{2008}-2009} - 1$  на 1155?

**Задача 34.** Решите уравнение при всех значениях параметра  $a \in \mathbb{R}$

$$x^4 + 2x^3 - 4x^2 - 2(a+1)x - (a-3)(a+1) = 0.$$

**Задача 35.** При каких значениях параметра  $a$  уравнение

$$4(4a-1)x^2 + 2(4a+1)(x^2 + 1)x + (a+1)(x^2 + 1)^2 = 0$$

имеет ровно четыре различных решения?

**Задача 36.** Подсчитайте, сколько всего существует натуральных чисел, которые не превосходят число 841 и не имеют с ним общих делителей, отличных от 1.

**Задача 37.** Дан треугольник  $\triangle ABC$ , в котором  $AB = 99$ ,  $AC = 71$ ,  $\angle BAC = 67^\circ$ . Требуется только с помощью циркуля и линейки построить треугольник  $\triangle DEF$  со сторонами  $DE = 101$ ,  $EF = 73$  и углом между ними  $\angle DEF = 51^\circ$ .

**Задача 38.** Известно, что три числа  $a_1, a_2, a_3$  были получены следующим образом. Сначала выбрали натуральное число  $A$  и нашли числа  $A_1 = [A]_{16}, A_2 = [A/2]_{16}, A_3 = [A/4]_{16}$ , где  $[X]_{16}$  — остаток от деления целой части числа  $X$  на 16 (например,  $[53/2]_{16} = 10$ ). Затем было выбрано целое число  $B$  такое, что  $0 \leq B \leq 15$ . Числа  $A_1, A_2, A_3$  и  $B$  записывают в двоичной системе счисления, т. е. представляют каждое из них в виде цепочки из 0 и 1 длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд согласно правилу:  $1 + 1 = 0 + 0 = 0$  и  $0 + 1 = 1 + 0 = 1$ , а саму операцию посимвольного сложения обозначим символом  $\oplus$ . Например,  $3 \oplus 14 = (0011) \oplus (1110) = (1101) = 13$ . Положим  $a_1 = A_1 \oplus B$ ,  $a_2 = A_2 \oplus B$ ,  $a_3 = A_3 \oplus B$ . Найдите все возможные значения числа  $a_3$ , если известно, что  $a_1 = 4, a_2 = 10$ .

**Задача 39.** Найдите число решений системы уравнений

$$\begin{cases} x + |y| = 1 \\ y + a|x| = 2 \end{cases}$$

при всех возможных значениях параметра  $a$ .

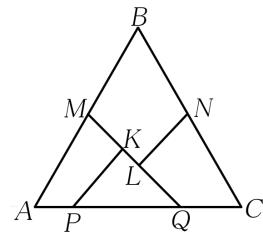
**Задача 40.** Изобразите на плоскости  $Oxy$  множество всех точек с координатами  $(x, y)$  таких, что  $y \geq x^2 - 1$  и при любом значении параметра  $a$  выполняется неравенство  $a^2y + 2ax - y - 2 \leq 0$ . Ответ обоснуйте.

**Задача 41.** Сколько существует упорядоченных пар натуральных чисел  $a$  и  $b$ , для которых известны их наибольший общий делитель  $d = 6$  и их наименьшее общее кратное  $m = 6930$ ? Сформулируйте ответ и в общем случае (для произвольных  $d, m$ ), используя канонические разложения  $d$  и  $m$  на простые множители.

**Задача 42.** Известно, что число  $n = 202718099$  является произведением двух простых чисел  $p$  и  $q$ , а количество натуральных чисел, меньших  $n$  и взаимно простых с  $n$ , равно 202687920. Найдите числа  $p$  и  $q$ .

**Задача 43.** Данна последовательность чисел  $c_1, c_2, \dots, c_n, \dots$ , в которой  $c_n$  есть последняя цифра числа  $n^n$ . Докажите, что эта последовательность периодическая и её наименьший период равен 20.

**Задача 44.** Равносторонний треугольник  $ABC$  разбит на четыре части так, как показано на рисунке, где  $M$  и  $N$  — середины сторон  $AB$  и  $BC$  соответственно. Известно, что  $PK \perp MQ$  и  $NL \perp MQ$ . В каком отношении точки  $P$  и  $Q$  делят сторону  $AC$ , если известно, что из этих частей можно составить квадрат?



**Задача 45.** Чтобы запомнить периодически меняющийся пароль в ЭВМ, математики придумали следующий способ. При известном числе  $a \in \mathbb{R}$  (например, номере месяца в году) пароль представляет собой первые шесть цифр наименьшего решения уравнения

$$a(x^2 - 1) = \sqrt{1 + \frac{x}{a}}.$$

(число меньшей значности дополняется справа необходимым числом нулей). Решите такое уравнение при произвольном  $a > 0$ .

**Задача 46.** Комбинация  $x, y, z$  трёх натуральных чисел, лежащих в диапазоне от 10 до 20 включительно, является отпирающей для кодового замка, если выполнено соотношение  $F(x, y, z) = 99$ . Найдите все отпирающие комбинации для замка с функцией

$$F(x, y, z) = 3x^2 - y^2 - 7z.$$

**Задача 47.** Из точки  $O$  внутри треугольника  $ABC$  на его стороны  $AB$ ,  $BC$ ,  $AC$  опущены перпендикуляры  $OP$ ,  $OQ$ ,  $OR$ . Докажите, что  $OA + OB + OC \geq 2(OP + OQ + OR)$ .

**Задача 48.** Решите уравнение:

$$\sqrt{3x+1}\sqrt{3x+71} - (7 + \sqrt{2x-1})\sqrt{2x+14\sqrt{2x-1}+118} = 0.$$

**Задача 49.** Квадратная таблица размером  $1997 \times 1997$  заполнена натуральными числами от 1 до 1997 так, что в каждой строке присутствуют все числа от 1 до 1997. Найдите сумму чисел, стоящих на диагонали, которая соединяет левый верхний и правый нижний углы таблицы, если заполнение таблицы симметрично относительно этой диагонали.

**Задача 50.** Докажите, что для каждого простого числа  $p$  последовательность  $a_1, a_2, a_3, \dots$  является периодической с периодом 2, если  $a_n$  равно остатку от деления числа  $p^{n+2}$  на 24 при всех  $n \geq 1$ .

**Задача 51.** Найдите все значения параметра  $a$ , при которых уравнение

$$\underbrace{\dots ||}_{1996 \text{ раз}} \underbrace{|x-a| - a| - \dots - |}_{1996 \text{ раз}} = 1996.$$

имеет ровно 1997 различных решений.

**Задача 52.** При  $a > 0, b > 0, c > 0$  докажите неравенство:

$$a^3 + b^3 + c^3 + 6abc > \frac{1}{4}(a+b+c)^3.$$

**Задача 53.** Для рисования на большой прямоугольной доске используется мел с квадратным сечением со стороной 1 см. При движении мела стороны сечения всегда параллельны краям доски. Как начертить выпуклый многоугольник площадью  $1 \text{ м}^2$  с наименьшей площадью границы (площадь границы не входит в площадь многоугольника)?

## 2.2 Интересные задачи разных типов

**Задача 54. Три шестерёнки.** На каждой из трёх осей установлено по одной вращающейся шестерёнке и неподвижной стрелке. Шестерёнки соединены последовательно. На первой шестерёнке 33 зубца,

на второй — 10, на третьей — 7. На каждом зубце первой шестерёнки по часовой стрелке написано по одной букве русского языка в алфавитном порядке:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я

На зубцах второй и третьей шестерёнок в порядке возрастания по часовой стрелке написаны цифры от 0 до 9 и от 0 до 6 соответственно. Когда стрелка первой оси указывает на букву, стрелки двух других осей указывают на цифры.

Буквы сообщения шифруются последовательно. Зашифрование производится вращением первой шестерёнки против часовой стрелки до первого попадания шифруемой буквы под стрелку. В этот момент последовательно выписываются цифры, на которые указывают вторая и третья стрелки. В начале шифрования стрелка 1-го колеса указывала на букву А, а стрелки 2-го и 3-го колёс — на цифру 0.

- зашифруйте слово О Л И М П И А Д А;
- расшифруйте сообщение 2 4 8 0 9 2 8 3 9 1 1 2 1 1.

**Задача 55.** Данна диаграмма:

$$\begin{array}{rcccl}
 \Phi & H & \times & Y & = & \Phi & A & \Phi \\
 + & & & \times & & - & & \\
 E & E & + & E & = & H & Z \\
 = & & = & & = & & \\
 I & I & H & A & + & M & P & = & I & M & H
 \end{array}$$

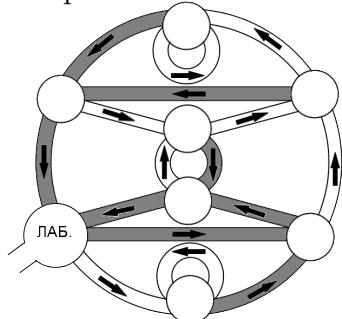
Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст.

**Задача 56. Короткое замыкание.** Порядковый номер каждой буквы алфавита русского языка, состоящего из 32 букв (Е и Ё отождествлены), представлен в двоичной системе счисления пятизначным числом, начиная с нуля. Например, букве А соответствует двоичное число 00000, а букве Ч — 10111. Передача каждой буквы сообщения осуществляется путём передачи каждой из цифр соответствующего пятизначного двоичного числа по отдельному проводу. Криптоша-

случайно замкнул какие-то два из этих пяти проводов. В результате на других концах замкнутых проводов появляется 1, как только по одному из них передается 1. Найдите переданное слово, если получен текст ТЕЬЕУТАЦ.

**Задача 57. Робот в лабиринте.** На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещёнными, возможно только по направлениям, указанным на схеме, и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот.

Робот управляет командами из нулей и единиц, при этом 0 соответствует движению по освещённому коридору, а 1 — по неосвещённому. Передайте команду роботу, которая приведёт его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более чем на 5 минут.



**Задача 58. Стёртые пиксели.** Цепочка ПТИУААМДЛ получена перестановкой букв в некотором слове. Имеется последовательность цифр, задающая порядок, в котором надо выписать буквы цепочки для получения исходного слова. Каждая цифра записывалась в прямоугольный шаблон размера 5 на 3 пикселей по образцу



При передаче часть пикселей на местах, одинаковых для каждой цифры, стёрлись. Получилось вот что:



Восстановите исходное слово и перехваченную перестановку.

**Задача 59.** Для передачи сообщения на русском языке Крокодил Гена и Чебурашка выполняют следующие действия. Каждый из них

выбирает свою последовательность, состоящую из целых чисел в пределах от 0 до 32, длина которой равна длине сообщения. Буквы сообщения заменяются числами по таблице:

|          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| <b>А</b> | <b>Б</b> | <b>В</b> | <b>Г</b> | <b>Д</b> | <b>Е</b> | <b>Ё</b> | <b>Ж</b> | <b>З</b> | <b>И</b> | <b>Й</b> | <b>К</b> | <b>Л</b> | <b>М</b> | <b>Н</b> | <b>О</b> | <b>П</b> | <b>Р</b> | <b>С</b> | <b>Т</b> | <b>У</b> | <b>Ф</b> | <b>Х</b> | <b>Ц</b> | <b>Ч</b> | <b>Ш</b> | <b>Щ</b> | <b>Ъ</b> | <b>Ы</b> | <b>Ь</b> | <b>Э</b> | <b>Ю</b> | <b>Я</b> |
| 1        | 2        | 3        | 4        | 5        | 6        | 7        | 8        | 9        | 10       | 11       | 12       | 13       | 14       | 15       | 16       | 17       | 18       | 19       | 20       | 21       | 22       | 23       | 24       | 25       | 26       | 27       | 28       | 29       | 30       | 31       | 32       | 0        |

Сначала Гена шифрует сообщение, используя свою последовательность. Для этого числовое значение первой буквы сообщения и первое число его последовательности складываются, а полученная сумма заменяется остатком от деления на 33 и вновь заменяется буквой по таблице 2. Затем эта процедура повторяется для вторых, третьих и т. д. чисел сообщения и последовательности. Полученный результат

**ЁЛИСУВШОЮЦМОЮВЫЗПЭЬМО**

передаётся Чебурашке. После этого Чебурашка шифрует полученное сообщение с помощью своей последовательности. Получается строка

**ЪЭЛВШРЕЭЭТЖЩЮИГВФБСЦХ,**

которую он и передает Гене. Гена вычитает из числовых значений букв полученного сообщения числа своей последовательности (к отрицательной разнице прибавляется число 33) и передаёт результат

**ЖЪЫХЙТСЖЫАШШЬЯМЫШЗЬВГ**

Чебурашке. Какое сообщение зашифровал Крокодил Гена?

**Задача 60.** Четыре фразы на русском языке записываются без знаков препинания и пробелов. Для зашифрования каждой фразы используются неизвестные последовательности цифр  $x_1, x_2, \dots$ . Буквы во фразе последовательно заменяются на пары цифр согласно таблице из прошлой задачи (к одноразрядным числам слева дописывается 0: например, А будет заменяться на 01). Зашифрование состоит в преобразовании получившейся цепочки цифр по следующему правилу. К первой цифре цепочки прибавляем цифру  $x_1$  и записываем последнюю цифру суммы, потом ко второй цифре цепочки прибавляем  $x_2$  и также записываем последнюю цифру суммы и т. д. Результат зашифрования выглядит следующим образом:

- 1) 0436389637110156289614062778022668915272874106897713780236
- 2) 903913973306253415922423357601144271609271
- 3) 17915094077497245567822036742365175971
- 4) 3703532519925327917085909750657981901587194945023834835000452922

Известно, что две фразы зашифрованы с помощью одной и той же последовательности. Укажите, какие именно (ответ обоснуйте).

**Задача 61.** Для зашифрования сообщения на русском языке, записанного без знаков препинания и пробелов, используется последовательность натуральных чисел  $x_1, x_2, \dots$ , удовлетворяющая соотношению:  $x_k = b \cdot 8^{a(k-1)}$ ,  $k = 1, 2, \dots$  Здесь  $a$  и  $b$  — фиксированные (но неизвестные) натуральные числа. Зашифрование производится следующим образом. Первую букву сообщения заменяют числом согласно таблице

|   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |   |
|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|
| А | Б | В | Г | Д | Е | Ё | Ж | Э | И, | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ы  | Ь, | Ѣ  | Ѥ  | Ѡ | Ѩ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |   |   |

и складывают с  $x_1$ . Потом так же заменяют вторую букву и складывают с  $x_2$  и т. д. Затем все суммы заменяют остатками от деления на 31, а остатки заменяют буквами согласно той же таблице. В результате получился текст:

ѠЯФРПЯФБКПЩСъИжъиясязтхжутнаЖБС ёНФВГМнуту ёШЖФН

Найдите исходное сообщение, представляющее собой отрывок известного стихотворения, если известно, что в нем есть слово РАВНИНЫ.

**Задача 62. Криптографическая дедукция.** Пользователи сети связи для обеспечения секретности сообщений выбирают (независимо друг от друга) пары преобразований  $(E, D)$ , одно из которых,  $E$  (открытый ключ), публикуют в справочнике, а второе,  $D$  (личный ключ), держат в секрете. Известно, что значения  $E(m)$  и  $D(n)$  легко вычислить для любых сообщений  $m$  и  $n$ , причём из равенства  $E(m) = n$  следует, что  $D(n) = m$ . В то же время нахождение  $m$  по  $E(m)$  является сложной задачей, которую невозможно решить (любыми средствами) за реальное время, если неизвестно  $D$ . Если

пользователь  $A$  хочет послать пользователю  $B$  сообщение  $m$ , он берет из справочника открытый ключ  $E_B$  пользователя  $B$ , вычисляет  $n = E_B(m)$  и посыпает  $n$  к  $B$ . Получив  $n$ ,  $B$  вычисляет  $D_B(n) = m$ . Злоумышленник, перехвативший  $n$ , не сможет вычислить  $m$ . Это гарантирует секретность информации.

Доктор Ватсон предложил Шерлоку Холмсу способ передачи секретных сообщений с уведомлением о получении:  $A$  передает  $B$  сообщение  $(A, E_B(m))$ ;  $B$ , получив сообщение, вычисляет  $m$  и направляет  $A$  уведомление  $(B, E_A(m))$ . Холмс возразил Ватсону, что этот способ не обеспечивает секретности информации от любого пользователя, который может перехватывать сообщения и как угодно их изменять. Дополнительно потребовав, чтобы для каждого преобразования  $E$  было сложно подобрать пару  $(m, n)$ , для которой  $E(m) = E(n)$ , Холмс предложил Ватсону свой способ:  $A$  передает  $B$  сообщение  $E_B(A, m)$ ;  $B$ , получив сообщение, находит  $m$  и направляет  $A$  уведомление  $E_A(B, m)$ . Объясните, почему способ Холмса лучше способа Ватсона.

**Задача 63. Автосигнализация.** Центральный замок автомобиля открывается и закрывается с помощью брелока. При получении сигнала брелока замок открывается (если был закрыт) или закрывается (если был открыт). В брелоке и замке имеются счётчики (назовем их СБ и СЗ), на которых изначально было выставлено одно и то же число. Пусть  $N$  — текущее значение СБ. При нажатии на кнопку брелока СБ меняет значение на  $N + 1$ , старое же значение  $N$  в зашифрованном виде передается замку. Микрокомпьютер замка расшифровывает полученный сигнал и находит число, переданное брелоком. Если это число равно или превосходит значение СЗ, то замок срабатывает, а значение СЗ становится  $N + 1$ . Если это число оказывается меньше или при расшифровании обнаруживается ошибка, то замок остается в прежнем состоянии. Злоумышленник способен: а) запоминать сигналы брелока, б) поставив помеху, искажать сигналы брелока (при этом сам злоумышленник получает сигнал без искажений), в) посыпать замку ранее запомненные сигналы. Как злоумышленнику открыть замок? Алгоритмы зашифрования и расшифрования ему неизвестны.

**Задача 64.** Цифры от 1 до 9 расположены на окружности в некотором неизвестном порядке. При зашифровании цифрового сообщения каждая отличная от 0 цифра заменяется на соседнюю с ней цифру на окружности по часовой стрелке, а при расшифровании — на соседнюю с ней цифру на окружности против часовой стрелки. Цифра 0 остаётся без изменения в обоих случаях.

Укажите условия, при которых порядок цифр на данной окружности можно однозначно восстановить по двум цифровым текстам — результатам расшифрования и зашифрования одного и того же цифрового текста с помощью данной окружности.

**Задача 65. Спутник.** Для наблюдения за страной Криптоландией запущен разведывательный спутник. Страна Криптоландия имеет форму прямоугольника. При этом спутник находится на расстоянии 700 км от одной вершины прямоугольника, на расстоянии 330 км от противоположной вершины прямоугольника и на расстоянии 650 км от третьей вершины прямоугольника. Найдите расстояние от спутника до четвёртой вершины прямоугольника.

**Задача 66. Торговые автоматы.** Торговые автоматы в Криптоландии принимают монетки номиналом только в 3 и 7 криптов. Укажите все цены, которые нельзя устанавливать на товары, продаваемые через автоматы подобного вида. Автоматы сдачу не дают.

**Задача 67. Путешественник.** Все 16 городов Криптоландии в качестве названий имеют различные четырёхразрядные комбинации, состоящие из нулей и единиц (например, «0011»). Все города попарно соединены непересекающимися дорогами, причём проезд из одного города в другой стоит столько криптов, в скольких разрядах различаются их имена (например, из «0011» в «1001» — 2 крипта). Путешественник, находящийся в «0000», хочет объехать все города страны и вернуться назад за минимальную цену. Как ему это сделать?

**Задача 68. Ключи поворотной решётки.** Ключом шифра, называемого «поворотная решётка», является трафарет, изготовленный из квадратного листа клетчатой бумаги размера  $n \times n$  ( $n$  — чётно).

Некоторые из клеток вырезаются. Одна из сторон трафарета помечена. При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причём каждая клетка оказывается под вырезом ровно один раз. Буквы сообщения, имеющего длину  $n^2$ , последовательно вписываются в вырезы трафарета, сначала наложенного на чистый лист бумаги помеченной стороной вверх. После заполнения всех вырезов трафарета буквами сообщения трафарет располагается в следующем положении и т. д. После снятия трафарета на листе бумаги оказывается зашифрованное сообщение. Найдите число различных ключей для произвольного чётного числа  $n$ .

**Задача 69. Разведчик.** Для передачи информации от резидента Гарриваса в Нагонии только что внедрённому разведчику был установлен следующий порядок: все сообщения резидента определены заранее и пронумерованы числами 1, 2, 3, ... Разведчик, обладающий феноменальной памятью, полностью запомнил соответствие между сообщениями и их номерами. Теперь для того чтобы передать информацию разведчику, достаточно сообщить ему лишь соответствующее число. Для передачи числа в условленном месте оставлялась равная этому числу денежная сумма. На момент разработки операции в Нагонии имели хождение денежные купюры достоинством 1, 3, 7 и 10 бут (бут — денежная единица Нагонии). Однако в результате денежной реформы купюры достоинством 1 и 3 бут были изъяты из обращения. Выясните, начиная с какого номера можно передать разведчику любое сообщение, пользуясь только оставшимися в обращении купюрами.

**Задача 70. Верный пароль.** Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите  $a, b, c$ . Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введённый в него набор  $P$  в набор  $Q = \varphi(P)$ . Отображение  $\varphi$  держится в секрете, однако про него известно, что оно определено не для каждого набора букв и обладает следующими свойствами. Для любого набора букв  $P$ :

- 1)  $\varphi(aP) = P;$
- 2)  $\varphi(bP) = \varphi(P)a\varphi(P);$
- 3) набор  $\varphi(cP)$  получается из набора  $\varphi(P)$  выписыванием букв в обратном порядке.

Устройство признаёт предъявленный пароль верным, если  $\varphi(P) = P$ . Например, трёхбуквенный набор  $bab$  является верным паролем, так как  $\varphi(bab) = \varphi(ab)a\varphi(ab) = bab$ . Подберите верный пароль, состоящий более чем из трёх букв.

**Задача 71. «Считала».** В древнем шифре, известном под названием «Считала», использовалась полоска папируса, которая наматывалась на круглый стержень виток к витку без просветов и нахлёстов. Далее при горизонтальном положении стержня на папирус построчно записывался текст сообщения. После этого полоска папируса с записанным на ней текстом посыпалась адресату, имеющему точно такой же стержень, что позволяло ему прочитать сообщение.

В наш адрес поступило сообщение, зашифрованное с помощью шифра «Считала». Однако его автор, заботясь о том, чтобы строчки были ровные, во время письма проводил горизонтальные линии, которые остались на полоске в виде чёрточек между буквами. Угол наклона этих чёрточек к краю ленты равен  $\alpha$ , ширина полоски равна  $d$ , а ширина каждой строки равна  $h$ . Укажите, как, пользуясь имеющимися данными, прочитать текст.

**Задача 72.** Рассмотрим преобразование цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена  $F(x) = b(x^3 + 7x^2 + 3x + a)$  на число 10, где  $a, b$  — фиксированные натуральные числа.

Выясните, при каких значениях  $a, b$  указанное преобразование может быть шифрпреобразованием (т. е. допускает однозначное расшифрование).

**Задача 73. Кодовый замок.** При установке кодового замка каждой из 26 латинских букв, расположенных на его клавиатуре, сопоставляется произвольное натуральное число, известное лишь обладателю замка. Разным буквам сопоставляются не обязательно различные числа. После набора произвольной комбинации попарно различных букв происходит суммирование числовых значений, соответству-

ющих набранным буквам. Замок открывается, если сумма делится на 26. Докажите, что для любых числовых значений букв существует комбинация, открывающая замок.

**Задача 74. Телефонная сеть.** Установите, можно ли создать проводную телефонную сеть связи, состоящую из 993 абонентов, каждый из которых был бы связан ровно с 99 другими.

**Задача 75. 10-угольник.** «Шифровальный диск» используется для зашифрования числовых сообщений. Он состоит из неподвижного диска и соосно вращающегося на нём диска меньшего диаметра. На обоих дисках нанесены цифры от 0 до 9, которые расположены в вершинах правильных 10-угольников, вписанных в диски.

Цифра  $X$  на неподвижном диске зашифровывается в цифру  $Y$  подвижного диска, лежащую на том же радиусе, что и  $X$ .

Для построения вписанного 10-угольника без транспортира надо уметь строить угол в  $36^\circ$ . Попытайтесь вычислить с точностью до 0,1 значение какой-либо тригонометрической функции такого угла без таблиц и калькулятора.

**Задача 76. Обход конём.** Знаменитый математик Леонард Эйлер в 1759 г. нашёл замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно по одному разу.

Прочтите текст, вписанный в клетки шахматной доски по такому маршруту, если известно, что начало текста в клетке а4.

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| Д | Л | Р | И | Л | П | Н | Б |
| У | К | А | О | Т | У | С | Т |
| О | О | О | А | Н | О | И | Р |
| Т | Б | Г | К | Т | Т | У | К |
| К | О | Е | О | Р | А | В | О |
| К | Д | Г | П | В | Л | Е | Т |
| Т | А | Н | Р | М | А | Г | О |
| Е | А | О | В | И | Д | У | Л |

**Задача 77. Система связи.** В системе связи, состоящей из 1997 абонентов, каждый абонент связан ровно с  $N$  другими. Определите все возможные значения  $N$ .

**Задача 78. Проводная сеть связи.** Какое наименьшее число соединений требуется для организации проводной сети связи из 10 узлов, чтобы при выходе из строя любых двух узлов связи сохранилась возможность передачи информации между любыми двумя оставшимися (хотя бы по цепочке через другие узлы)?

## 2.3 Шифры перестановки

Шифр, преобразования которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется *шифром перестановки*.

**Задача 79.** «Магический» квадрат. Клетки квадрата  $4 \times 4$  пронумеровали так, что клетка в правом нижнем углу получила номер 1, а все остальные получили разные номера от 2 до 16. Оказалось, что суммы номеров клеток каждой строки, каждого столбца, а также каждой из двух диагоналей квадрата одинаковы («магический» квадрат). Клетки квадрата заполнили буквами некоторого сообщения так, что его первая буква попала в клетку с номером 1, вторая — в клетку с номером 2 и т. д. В результате построчного выписывания букв заполненного квадрата (слева направо и сверху вниз) получилась последовательность букв:

Ы Р Е У С Т Е В Ъ Т А Б Е В К П.

Восстановите магический квадрат и исходное сообщение.

**Задача 80. Афинная перестановка.** Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо  $1, 2, \dots, L$ . Зашифрование происходит путём перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа  $a$  и  $b$ . Буква с номером  $n$  в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа  $a \cdot n + b$  на  $L$  (с одним исключением: если  $a \cdot n + b$  нацело делится на  $L$ , то остаток полагается равным  $L$ ). Например, если длина цепочки  $L = 25$  и  $a = 9, b = 11$ , то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (так как  $9 \cdot 3 + 11 = 38$ , а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

тыйтоеонсоовзмевтрадазедвмаянтоаысзаимнонвк

При этих же значениях  $a, b$  проведено зашифрование еще некоторой цепочки из 38 букв. Получилось вот что:

видхъврлмаояоаоддсемдроиввоеозтообнзо

Найдите значения  $a$  и  $b$  и восстановите исходное сообщение.

**Задача 81. Поворотная решётка.** Сообщение на русском языке, состоящее из 63 букв и восклицательного знака, зашифровано с использованием так называемой «поворотной решётки», которая представляет собой трафарет, изготовленный из квадратного листа клетчатой бумаги 8 на 8. В трафарете вырезано 16 клеток. Одна сторона трафарета помечена. При наложении трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причём каждая клетка оказывается под вырезом ровно один раз. Буквы сообщения построчно сверху вниз и слева направо вписываются в вырезы трафарета (пробелы между словами игнорируются). После заполнения всех вырезов буквами сообщения трафарет располагается в следующем положении и т. д. Результат зашифрования сообщения представлен в таблице.

Найдите исходное сообщение.

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| т | я | с | а | п | м | р | е |
| в | щ | е | р | е | ш | ш | о |
| ч | и | ч | н | ф | и | т | р |
| ё | а | е | т | т | е | т | к |
| р | а | ь | п | а | п | о | ф |
| т | в | о | е | з | о | к | р |
| о | с | а | в | т | р | о | т |
| л | е | я | н | ! | е | т | а |

**Задача 82. Блочный шифр.** В результате перестановки букв сообщения получена криптограмма:

БТИПЧЬЛОЯЧЫТЬТОТПУНТНОНЗЛЖАЧОБЬОТУНИХИППОЛОЬЧОЕЛОЛС

Прочтите исходное сообщение, если известно, что оно было разбито на отрезки одинаковой длины  $r$ , в каждом из которых буквы представлены одинаково по следующему правилу. Буква отрезка, имеющая порядковый номер  $x$  ( $x = 1, 2, \dots, r$ ), в соответствующем отрезке криптограммы имеет порядковый номер  $f(x) = ax * b$ , где  $a$  и  $b$  — некоторые натуральные числа,  $ax * b$  равно остатку от деления суммы  $ax + br$ , если остаток не равен нулю, и равно  $r$ , если остаток равен нулю.

**Задача 83. Перестановка столбцов.** Сообщение было построчно записано в таблицу, имеющую 20 столбцов. При этом в каждую клетку таблицы записывалось по одной букве сообщения, пробелы между словами были опущены, а знаки препинания заменены на условные комбинации: точка — ТЧК, запятая — ЗПТ. Затем столбцы таблицы были некоторым образом переставлены, в результате чего был получен текст:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Я | Н | Л | В | К | Р | А | Д | О | Е | Т | Е | Р | Г | О | М | И | З | Я | Е |
| Й | Л | Т | А | Л | Ф | Ы | И | П | Е | У | И | О | О | Г | Е | Д | Б | О | Р |
| Ч | Р | Д | Ч | И | Е | С | М | О | Н | Д | К | Х | И | Н | Т | И | К | Е | О |
| Н | У | Л | А | Е | Р | Е | Б | Ы | Е | З | И | О | Н | Н | Ч | Д |   |   |   |
| Ы | Т | Д | О | Е | М | П | П | Т | Щ | В | А | Н | И | П | Т | Я | З | С | Л |
| И | К | С | И | - | Т | Ч | Н | О | - | - | Е | - | Л | У | Л | - | Т | - | Ж |

Прочтите исходное сообщение.

**Задача 84. «Решётка».** Ключом шифра, называемого «решёткой», является прямоугольный трафарет размера  $6 \times 10$  клеток. В трафарете вырезано 15 клеток так, что при наложении его на прямоугольный лист бумаги размера  $6 \times 10$  клеток четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения (без пропусков) последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырёх его возможных положений. Прочтите исходный текст, если после зашифрования на листе бумаги оказался следующий текст (на русском языке):

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| Р | П | Т | Е | Ш | А | В | Е | С | Л |
| О | Я | Т | А | Л | - | Ь | З | Т | - |
| - | У | К | Т | - | Я | А | Ь | - | С |
| Н | П | - | Ь | Е | У | - | Ш | Л | С |
| Т | И | Ь | З | Ы | Я | Е | М | - | О |
| - | Е | Ф | - | - | Р | О | - | С | М |

## 2.4 Шифры замены

Шифр, преобразования которого приводят к замене каждого символа открытого сообщения на другие символы — шифробозначения,

причём порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения, называется *шифром замены*.

**Задача 85. Стихотворение Тютчева.** Буквы фрагмента известного стихотворения Ф. И. Тютчева заменены некоторыми буквами так, что разным буквам соответствуют разные буквы, а одинаковым — одинаковые. Пробелы между словами и знаки препинания сохранены.

Гъюь Фюббшн эй яюэовл,  
Пфзщэюь юришь эй шчъйфшвл:  
Г эийщ юбюрийээпо бвпвл —  
С Фюббшн ьюцэю вюылъю сийфшвл.

Восстановите этот фрагмент.

**Задача 86. Определение языка.** Для зашифрования текстов каждую букву заменяли парой цифр. При этом разные буквы текста заменялись разными парами, а одинаковые — одинаковыми. Даны два зашифрованных текста:

79 92 38 98 95 91 34 95 73 77 96 92 78 95 73 98 92 96 92 72 98 96  
77 72 92 34 77 96 75 90 76 95 38 98 92 70 33 90 96 79 90 96 77 98  
95 90 38 77 70 70 90 98 74 92 96 98 96 77 72 92 34 77 96 75 73 77  
96 92 98 74 92 79 96 90 79 92 96 98 94 90 76 98 74 92 95 96 96 92  
73 79 92 33 98 95 32 92 90 93 38 92 96 73 94 90 91 96 91 73 92 98  
74 95 73 33 72 96 90 34 95 73 73 91 36 71 92 33 98 98 90 77 38 92  
38 72 91 73 92 96 70 95 33 92 38 33 92

71 75 74 39 74 73 74 72 30 73 74 78 33 79 98 94 78 36 79 97 72 29  
78 74 96 74 92 30 38 79 70 72 94 78 79 22 92 92 79 98 37 70 92 74  
94 77 74 93 31 78 74 70 39 79 71 75 94 98 70 39 97 92 72 22 23 39  
78 94 70 74 76 78 94 78 78 30 77 39 94 74 75 94 39 79 38 94 70 73  
79 77 79 78 39 94 75 94 70 73 75 74 76 94 39 74 96 74 76 78 74 96  
79 94 39 79 71 30 27 39 79 32 71 75 74 39 74 73 74 72 74 92 71 75  
94 98 35 22 92 72 22 23 39

Известно, что один из них соответствует сообщению на русском языке, а другой — на английском (в текстах строчные и заглавные буквы не различались, а пробелы и знаки препинания опускались).

Определите, какой шифрованный текст соответствует сообщению на русском языке.

**Задача 87. Первое слово.** Зашифрование сообщения состоит в замене букв исходного текста на пары цифр в соответствии с некоторой (известной только отправителю и получателю) таблицей, в которой разным буквам алфавита соответствуют разные пары цифр. Криптографу дали задание восстановить зашифрованный текст. В каком случае ему будет легче выполнить задание: если известно, что первое слово второй строки — «термометр», или что первое слово третьей строки — «ремонт»? Обоснуйте свой ответ. Предполагается, что таблица зашифрования криптографу неизвестна.

**Задача 88. Пословица.** Разгадайте пословицу

77.61.91.55.16.00.77.61.91.55.16.55.00.87.81.31.81.73.00.81.21.31.55.47.34.16.55.10

**Задача 89. Знаки на доске.** На доске было написано несколько натуральных чисел, причём разность любых двух соседних чисел равна одному и тому же числу. Коля заменил в этой записи разные цифры разными буквами, а одинаковые цифры — одинаковыми буквами. Восстановите исходные числа, если на доске написано Т, ЕЛ, ЕК, ЛА, СС.

**Задача 90. Поиск слова.** При зашифровании текста на русском языке (в текстах строчные и заглавные буквы не различались, а пробелы и знаки препинания опускались) каждую букву заменяли парой цифр. При этом разные буквы текста заменялись разными парами, а одинаковые — одинаковыми. Найдите все возможные места расположения слова ПОДЪЕЗД в исходном тексте по шифрованному тексту:

92 97 36 72 97 92 70 73 97 90 97 72 38 39 74 76 97 34 79 78 97 70 76 74  
72 74 73 74 76 70 70 97 76 74 96 74 37 39 75 97 70 39 74 79 39 37 71 74  
98 35 94 90 98 97 94 96 74 98 74 76 97

**Задача 91. Шифр «Два квадрата».** Для зашифрования сообщения на английском языке составляются две таблицы размера  $5 \times 5$ . В клетки каждой таблицы в неизвестном порядке вписаны буквы укороченного английского алфавита (*v* и *w* отождествлены), так что

каждая буква алфавита встречается в каждой таблице один раз. Букву, расположенную в  $i$ -ой строке и  $j$ -м столбце первой таблицы обозначим через  $a_{ij}$ , а букву второй таблицы — через  $b_{ij}$ . При зашифровании сообщение разбивается на пары подряд идущих букв. Пара вида  $a_{ij}b_{\ell m}$  заменяется при  $i \neq \ell$  парой  $b_{im}a_{\ell j}$ , а при  $i = \ell$  — парой  $b_{\ell j}a_{im}$ . В результате зашифрования сообщения

с r u p t o g r a p h i c a l g o r i t h m

был получен один из следующих шифртекстов:

p a b d g l i u r c a v t h o t u e a d s p,  
d s z q u p h s b q i j d b m h p s j u i n.

Определите, какой именно? Ответ обоснуйте.

### Задача 92. Четверостишие. Криптограмма

12 2 24 5 3 21 6 29 28 2 20 18 20 21 5 10 27 17 2 11 2 16 —  
19 2 27 5 8 29 12 31 22 2 16, 19 2 19 5 17 29 8 29 6 29 16:  
8 2 19 19 29 10 19 29 14 19 29 29 19 10 2 24 2 11 2 16  
10 14 18 21 17 2 20 2 28 29 16 21 29 28 6 29 16.

получена заменой букв на числа (от 1 до 32) так, что разным буквам соответствуют разные числа. Отдельные слова разделены несколькими пробелами, буквы — одним пробелом, знаки препинания сохранены. Буквы «е» и «ё» не различаются. Прочтите четверостишие В. Высоцкого.

**Задача 93. Простая замена.** Шифрпреобразование простой замены в алфавите  $A = \{a_1, a_2, \dots, a_n\}$ , состоящем из  $n$  различных букв, заключается в замене каждой буквы шифруемого текста буквой того же алфавита, причём разные буквы заменяются разными. Ключом шифра простой замены называется таблица, в которой указано, какой буквой надо заменить каждую букву алфавита  $A$ . Если слово СРОЧНО зашифровать простой заменой с помощью ключа

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П |
| Ч | Я | Ю | Э | Ы | Ь | Щ | Ш | Ц | Х | Ф | У | Б | Д | Т |
| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Ь | Э | Ю | Я |
| З | В | Р | П | М | Л | К | А | И | О | Ж | Е | С | Г | Н |

,

то получится слово ВЗДАБД. Зашифровав полученное слово с помощью того же ключа ещё раз, получим слово ЮШЧЯ. Сколько всего различных слов можно получить, если указанный процесс шифрования продолжать неограниченно?

**Задача 94. «Криптография».** Сообщение, зашифрованное в пункте А шифром простой замены в алфавите из букв русского языка и знака пробела (-) между словами, передаётся в пункт Б отрезками по 12 символов. При передаче очередного отрезка сначала передаются символы, стоящие на чётных местах в порядке возрастания их номеров, начиная со второго, а затем — символы, стоящие на нечётных местах (также в порядке возрастания их номеров), начиная с первого. В пункте Б полученное шифрованное сообщение дополнительно шифруется с помощью некоторого другого шифра простой замены в том же алфавите, а затем таким же образом, как и из пункта А, передаётся в пункт В. По перехваченным в пункте В отрезкам:

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| С | О | - | Г | Ж | Т | П | Н | Б | Л | Ж | О |
| Р | С | Т | К | Д | К | С | П | Х | Е | У | Б |
| - | Е | - | П | Ф | П | У | Б | - | Ю | О | Б |
| С | П | - | Е | О | К | Ж | У | У | Л | Ж | Л |
| С | М | Ц | Х | Б | Э | К | Г | О | Щ | П | Ы |
| У | Л | К | Л | - | И | К | Н | Т | Л | Ж | Г |

восстановите исходное сообщение, зная, что в одном из переданных отрезков зашифровано слово КРИПТОГРАФИЯ.

**Задача 95. Группы цифр.** Цифры 0, 1, ..., 9 разбиты на несколько непересекающихся групп. Из цифр каждой группы составляются все возможные числа, для записи каждого из которых все цифры группы используются ровно один раз (учитываются и записи, начинающиеся с нуля). Все полученные числа расположили в порядке возрастания и  $k$ -ому числу поставили в соответствие  $k$ -ю букву алфавита:

А В В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ч Ш Щ Ы Ъ Э Ю Я

Оказалось, что каждой букве соответствует число и каждому числу соответствует некоторая буква. Шифрование сообщения осуществляется заменой каждой буквы соответствующим ей числом. Если

ненулевое число начинается с нуля, то при шифровании этот нуль не выписывается. Восстановите сообщение 873146507381 и укажите таблицу замены букв числами.

## 2.5 Комбинированные шифры

Часто встречаются комбинации замены и перестановки. Причины такого подхода ясны, такой шифр сложнее вскрыть, чем шифр замены или шифр перестановки.

**Задача 96.** Замена и перестановка. Текст

А М И М О П Р А С Т Е Т И Р А С И С П Д  
И С А Ф Е И И Б О Е Т К Ж Р Г Л Е О Л О  
И Ш И С А Н Н С Й С А О О Л Т Л Е Я Т У  
И Ц В Ы И П И Я Д П И щ П Ъ П С Е Ю Я Я

получен из исходного сообщения перестановкой его букв. Текст

У щ Ф М щ П д Р Е ц Ч Е щ ю щ Ч д А к Е  
Ч м д в к щ б Е Е Ч д Ф Э П й щ Г щ Ф щ  
Ц Е ю щ Ф П М Е Ч П М Е Р щ М Е О Ф Ч щ  
Х Е щ Р Т Г д И Ф Р С я й л К д Ф Ф Е Е

получен из того же исходного сообщения заменой каждой буквы на другую букву так, что разные буквы заменены разными, а одинаковые — одинаковыми. Восстановите исходное сообщение.

**Задача 97. Две последовательности.** Во фрагменте литературного произведения известного автора, записанном без пробелов и знаков препинания, заменили буквы. При этом разные буквы заменили разными, а одинаковые — одинаковыми. В результате получили некоторую последовательность букв. Тот же фрагмент был разбит на целое число подряд идущих участков, состоящих из одинакового числа букв. В каждом участке буквы одинаково переставили между собой. В результате получили другую последовательность. Восстановите исходный фрагмент по двум полученным последовательностям:

МЗОБВЕСИАВЛИЕВСОДВОВМОНИОНЧЛГЕЕОТИЕПОРЗАНДСОТЮВИСЧОНЕВИЛОО  
РИЖХУВМРЭЭШБЯВРРЖШВЭРВУЧМЖЬВЕЖЭКВЖАЛЬЯСВХВТРВШАВЕЬГЭШВМВРЖЭ

**Задача 98. Перепутанные проводки.** Для передачи сообщений по телеграфу каждая буква русского алфавита (буквы Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б — 00001, буква Ч — 10111, буква Я — 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоичный разряд передается поциальному проводу. При приёме сообщения Криптоша перепутал провода, поэтому вместо переданного слова получен набор букв ЭАВЩОЩИ. Найдите переданное слово.

**Задача 99.** Сообщение на русском языке состоит из 6 строк. В каждой строке (кроме последней) ровно 18 букв (буквы в строках стоят точно друг под другом). Для зашифрования сообщения каждую его букву заменили парой цифр в соответствии с её порядковым номером в алфавите (А — на 01, Б — на 02, ..., Я — на 33). В результате получилась таблица цифр, в которой 36 столбцов. Затем эту таблицу разделили на вертикальные полосы: по три столбца в каждой. После чего полосы переставили в неизвестном порядке. Получили вот что:

|     |     |     |     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 316 | 001 | 190 | 014 | 013 | 150 | 171 | 240 | 120 | 131 | 105 | 614 |
| 010 | 810 | 050 | 610 | 012 | 161 | 121 | 200 | 614 | 120 | 401 | 117 |
| 619 | 501 | 172 | 327 | 171 | 041 | 061 | 221 | 010 | 033 | 801 | 016 |
| 115 | 313 | 192 | 312 | 030 | 130 | 160 | 103 | 210 | 013 | 620 | 016 |
| 512 |     | 060 |     | 061 | 250 |     | 061 | 825 | 16  | 103 | 310 |

Какой текст был зашифрован?

**Задача 100. Двустшие.** Для зашифрования сообщения используют последовательность неотрицательных целых чисел  $x_1, x_2, \dots$ , удовлетворяющую соотношению  $x_{k+3} = x_k + x_{k+2}$ ,  $k \geq 1$ . Две строки известного стихотворения, последние 5 букв которых совпадают, зашифровали следующим образом. Первую букву заменили числом согласно таблице

|      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|
| А 0  | Б 1  | В 2  | Г 3  | Д 4  | Е 5  | Ж 6  | З 7  | И 8  | К 9  | Л 10 |
| М 11 | Н 12 | О 13 | П 14 | Р 15 | С 16 | Т 17 | У 18 | Ф 19 | Х 20 | Ц 21 |
| Ч 22 | Ш 23 | Щ 24 | Ђ 25 | Ѡ 26 | Ѡ 27 | Ѡ 28 | Ѡ 29 | Ѡ 30 |      |      |

и сложили с  $x_1$ , вторую заменили и сложили с  $x_2$  и т. д. Затем все суммы заменили остатками от деления на 31, а остатки заменили буквами согласно таблице. Получили текст

СЕЗНПБКЪЛЧЕЮЩТНИЭЛЬЩБШЕЮ  
ЛУАЕЧЖЪЭШЛЪЩХЧЩДЮВЫЮИД.

Восстановите три буквы, соответствующие в таблице числам  $x_1, x_2, x_3$ , и прочитайте двустишие.

**Задача 101. Кубик Рубика.** Для зашифрования фразы был взят кубик Рубика с нанесёнными на гранях русскими буквами. Развёртка кубика показана на рисунке.

Три его грани повернули по часовой стрелке на  $90^\circ$ . При этом грань с меньшим номером поворачивалась раньше, чем грань с большим номером. Затем каждая буква фразы отыскивалась на грани кубика и заменялась буквой этой же грани, следующей за ней по часовой стрелке (например, на рисунке буква А перейдет в букву Б, буква П в С). Буквы, находящиеся в центре грани, не заменялись.

Известно, что перед шифрованием запятая во фразе была заменена на ЗПТ, точка — на ТЧК, пробелы пропускались. В результате получилась строка

ЕПОЕЬРИТСГХЖЗТЯПСТАПДСБИСТЧК.

Прочтите исходное сообщение.

**Задача 102. Телетайп.** Для проверки телетайпа, печатающего буквами русского алфавита

АБВГДЕЖЗИЙКЛМНОРСТУФХЦЧЩЬЫЭЮЯ

передан набор из 9 слов, содержащий все 33 буквы алфавита. В результате неисправности телетайпа на приёмном конце получены слова:

ГъЙ АЭЕ БПРК ЕЖЩЮ НМЬЧ СЫЛЗ ЩДУ ЦХОТ ЯФВИ.

Восстановите исходный текст, если известно, что характер неисправности таков, что каждая буква заменяется буквой, отстоящей от неё в указанном алфавите не дальше, чем на две буквы. Например, буква Б может перейти в одну из букв {А, Б, В, Г}.



## 2.6 «Восстановите секретное сообщение...»

**Задача 103. Шифр Виженёра.** Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например **мир**. Для изменения первой буквы шифруемого сообщения создается следующая таблица:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
| М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ы | Ь |
| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |   |
| Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л |   |

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова М оказалась под буквой А. Буква открытого текста (например П) отыскивается в верхней строке и заменяется стоящей под ней буквой (для П это Ъ). Для зашифрования второй буквы аналогичным образом используется буква И, третьей — Р, четвёртой — вновь М и т. д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

МХЛЩЛИФЦБДЮГИШСПТАИВПБДЮОЛДЬУЭЮЙЕМХЛ

Восстановите исходное сообщение и ключевое слово.

**Задача 104. Секретная дата.** Сообщение зашифровано следующим образом. Над буквами сообщения надписывается числовая последовательность, образованная периодическим повторением 6 цифр, образующих дату. Например, 181107 отвечает дате 18 ноября 2007 года. После этого каждая буква сообщения заменяется буквой алфавита, циклически отстоящей от неё справа на число букв, указанное цифрой над ней. Можно ли прочитать зашифрованное таким образом сообщение:

Т П И Ё Р Ж Е М А А С Ф С Г Ъ О Г Х Ж П Н,

если неизвестна дата его написания?

**Задача 105. Шифр Bifid.** В качестве ключа используется квадратная таблица, в которой в некотором порядке записаны буквы английского алфавита (буквы I и J отождествлены):

|   |   |   |   |   |
|---|---|---|---|---|
| C | O | D | E | A |
| B | F | G | H | I |
| K | L | M | N | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

Результатом зашифрования фразы SIXTY EIGHT MILES на приведенном ключе является «фраза» RYXXT OFTXT LKSWS. Зашифруйте на том же ключе фразу ENTER OTHER LEVEL.

**Задача 106. Фраза на латыни.** Зашифрование фразы на латинском языке осуществлено в два этапа. На первом этапе каждая буква текста заменяется на следующую в алфавитном порядке (последняя Z заменяется на первую A). На втором этапе применяется шифр простой замены с неизвестным ключом. Его применение заключается в замене каждой буквы шифруемого текста буквой того же алфавита, при этом разные буквы заменяются разными буквами. Ключом такого шифра является таблица, в которой указано, какой буквой надо заменить каждую букву алфавита. По данному шифртексту:

OSZJX FXRE YOQJSZ RAYFJ

восстановите открытое сообщение, если известно, что для использованного (неизвестного) ключа результат шифрования не зависит от порядка выполнения указанных этапов для любого открытого сообщения. Пробелы в тексте разделяют слова. Латинский алфавит состоит из следующих 24 букв:

A B C D E F G H I J L M N O P Q R S T U V X Y Z.

**Задача 107. Крылатые фразы.** При передаче сообщений используется некоторый шифр. Пусть известно, что каждому из трёх шифрованных текстов:

ЙМЫВОТСЪЛКЪГВЦАЯ  
УКМАПОЧСРКЩВЗАХ  
ШМФЭОГЧСИЙКФЬВYEАКК

соответствовало исходное сообщение МОСКВА. Попробуйте расшифровать три текста:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ  
ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЕП  
РТПАИОМВСВТИЕОБПРОЕННИГЬКЕАМТАЛВТДСОУМЧШСЕОНШИАЯК

при условии, что двум из них соответствует одно и то же сообщение. Сообщениями являются известные крылатые фразы.

**Задача 108. Шифровка в Центр.** В адрес олимпиады пришло зашифрованное сообщение:

## Ф В М Е Ж Т И В Ф Ю

Найдите исходное сообщение, если известно, что шифр преобразование заключалось в следующем. Пусть  $x_1$ ,  $x_2$  — корни трёхчлена  $x^2 + 3x + 1$ . К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена  $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$ , вычисленное либо при  $x = x_1$ , либо при  $x = x_2$  (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.

**Задача 109. Коммерсант.** Исходное цифровое сообщение коммерсант шифрует и передает. Для этого он делит последовательность цифр исходного сообщения на группы по 5 цифр в каждой и после двух последовательных групп приписывает ещё две последние цифры суммы чисел, изображённых этими двумя группами. Затем к каждой цифре полученной последовательности он прибавляет соответствующий по номеру член некоторой целочисленной арифметической прогрессии, заменяя результат сложения остатком от деления его на 10.

Найдите исходное цифровое сообщение по шифрованному сообщению:

4 2 3 4 6 1 4 0 5 3 1 3.

### Задача 110. Корабли. Сообщение, записанное в алфавите

АБВГДЕЖЗИКЛМНОРСТУФХЦЧЩЬЫЭЮЯ,

зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении её порядкового номера в алфавите с порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфавита, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Восстановите два исходных сообщения, каждое из которых содержит слово КОРАБЛИ, если результат их зашифрования при помощи одной и той же шифрующей последовательности известен:

ЮПТЦАРГШАЛЖЕВЦЩЫРВУУ и ЮПЯТЬНЩМСДТЛЖГПСГХСЦЦ.

**Задача 111.** Буквы русского алфавита занумерованы в соответствии с таблицей:

|      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|
| А 1  | Б 2  | В 3  | Г 4  | Д 5  | Е 6  | Ж 7  | З 8  | И 9  | К 10 | Л 11 |
| М 12 | Н 13 | О 14 | П 15 | Р 16 | С 17 | Т 18 | У 19 | Ф 20 | Х 21 | Ц 22 |
| Ч 23 | Щ 24 | Ц 25 | Ы 26 | Ь 27 | Э 28 | Ю 29 | Я 30 |      |      |      |

Для зашифрования сообщения, состоящего из  $n$  букв, выбирается ключ  $K$  — некоторая последовательность из  $n$  букв приведённого выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении её номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Прочтите шифрованное сообщение

РБЫНТСИТСРРЕЗОХ,

если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.

**Задача 112.** Исходное сообщение, состоящее из букв русского алфавита и знака пробела (-) между словами, преобразуется в цифровое сообщение заменой каждого его символа парой цифр согласно следующей таблице:

|      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|
| А 1  | Б 2  | В 3  | Г 4  | Д 5  | Е 6  | Ж 7  | З 8  | И 9  | К 10 | Л 11 |
| М 12 | Н 13 | О 14 | П 15 | Р 16 | С 17 | Т 18 | У 19 | Ф 20 | Х 21 | Ц 22 |
| Ч 23 | Щ 24 | Ц 25 | Ы 26 | Ь 27 | Э 28 | Ю 29 | Я 30 |      |      |      |

Для зашифрования полученного цифрового сообщения используется отрезок последовательности из задачи 43, начинающийся с некоторого члена  $C_k$ . При зашифровании каждая цифра сообщения складывается с соответствующей цифрой отрезка и заменяется последней цифрой полученной суммы. Восстановите сообщение

2339867216458160670617315588.

**Задача 113.** Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

|      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|
| А 00 | Б 01 | В 02 | Г 03 | Д 04 | Е 05 | Ж 06 | З 07 | И 08 | К 09 | Л 10 |
| М 11 | Н 12 | О 13 | П 14 | Р 15 | С 16 | Т 17 | У 18 | Ф 19 | Х 20 | Ц 21 |
| Ч 22 | Ш 23 | Щ 24 | Ы 25 | Ь 26 | Э 27 | Ю 28 | Я 29 |      |      |      |

Для зашифрования полученного числового сообщения используется шифрующий отрезок последовательности  $A_1, A_2, \dots$  подходящей длины, начинающейся с  $A_{100}$ .

При зашифровании каждое число числового сообщения складывается с соответствующим числом шифрующего отрезка. Затем вычисляется остаток от деления полученной суммы на 30, который по данной таблице заменяется буквой. Восстановите сообщение

КЕНЗЭРЕ,

если шифрующий отрезок взят из последовательности, в которой  $A_1 = 3$  и  $A_{k+1} = A_k + 3(k^2 + k + 1)$  для любого натурального  $k$ .

**Задача 114. Пароль в сеть.** В компьютерной сети используются пароли, состоящие из цифр. Для того чтобы избежать хищения паролей, их хранят на диске в зашифрованном виде. При необходимости использования происходит однозначное расшифрование соответствующего пароля. Зашифрование пароля происходит посимвольно одним и тем же преобразованием. Первая цифра остается без изменения, а результат зашифрования каждой следующей цифры зависит только от неё и от предыдущей цифры.

Известен список зашифрованных паролей:

4249188780319, 4245133784397, 5393511, 428540012393,  
4262271910365, 4252370031465, 4245133784735

и два пароля 4208212275831 и 4242592823026, имеющиеся в зашифрованном виде в этом списке. Можно ли определить какие-либо другие пароли? Если да, то восстановите их.

**Задача 115. По секрету.** В результате перестановки букв сообщения получена криптограмма

БТИПЧЬЛОЯЧЫТотпунтнонзлажачоътуниухнипполовъчоелолс.

Прочтите исходное сообщение, если известно, что оно было разбито на отрезки одинаковой длины  $r$ , в каждом из которых буквы представлены одинаково по следующему правилу. Буква отрезка, имеющая порядковый номер  $x$  ( $x = 1, 2, \dots, r$ ), в соответствующем отрезке криптограммы имеет порядковый номер  $f(x) = ax \oplus b$ , где  $a$  и  $b$  — некоторые натуральные числа,  $ax \oplus b$  равно остатку от деления суммы  $ax + b$  на  $r$ , если остаток не равен нулю, и равно  $r$ , если остаток равен нулю.

## 2.7 Задачи последних олимпиад ИКСИ

Задачи олимпиады ИКСИ рассчитаны на учащихся 8–11 классов, но в олимпиаде могут принять участие и более юные школьники. Предлагаются три варианта, разделённые по классам, т. е. для 8–9, для 10 и для 11 классов. Обычно в варианте содержится 6 или более задач.

Ниже приведены варианты XX, XXI, XXII и XXIII олимпиад, которые проходили в 2010, 2011, 2012 и 2013 годах соответственно.

### 8–9 классы. 2010 год

В XX олимпиаде было по шесть задач в каждом варианте, но некоторые совпадали с задачами из других вариантов.

**Задача 116. Чат.** Ниже приведена переписка двух абонентов в чате.

**Godzilla:** Привет. Как дела? Пришли пароль для почты.

**Фунтик:** И усцрмс щюульсэ ц Яспар-Дюрюмгцмт пс вцю плювючж.  
Дсмычз: Гщмтщпвжи.

**Godzilla:** Когда доберешься до Питера, позвони.

Фунтик отвечает Godzill'e и для конспирации каждую букву заменяет другой буквой (при этом разные буквы заменяются разными, а одинаковые — одинаковыми). Восстановите зашифрованное сообщение и пароль.

**Задача 117. Модель нейрона.** Для прохода в учреждение необходимо предъявить пятизначную комбинацию, состоящую из нулей и единиц. Устройство распознавания представляет собой упрощённую модель нейрона — клетки головного мозга. Пятизначная комбинация  $x_1, x_2, x_3, x_4, x_5$  по пяти каналам поступает в клетку, где её компоненты умножаются на фиксированные целые числа  $a_1, a_2, a_3, a_4, a_5$ , и вычисляется сумма  $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5$ . Проход в учреждение открывается, только если  $S \geq c$ , где  $c$  — некоторое фиксированное целое число. Известно, что при предъявлении комбинаций  $(1,0,1,1,0)$ ,  $(1,1,0,1,0)$ ,  $(1,1,1,1)$  проход открывается, а при предъявлении комбинаций  $(1,0,1,0,0)$ ,  $(0,0,1,1,0)$ ,  $(1,1,0,1,1)$ ,  $(1,0,1,1,1)$  проход остаётся закрытым. Найдите ещё одну комбинацию, открывающую проход в учреждение.

## 10 класс. 2010 год

**Задача 118. Пароли.** На клавиатуре мобильного телефона каждой кнопке сопоставлено по несколько букв: кнопке 2 соответствуют буквы ABC, 3 — DEF, 4 — GHI, 5 — JKL, 6 — MNO, 7 — PQRS, 8 — TUV, 9 — WXYZ. Выбор нужной буквы определяется числом нажатий на кнопку. Например, нажав на кнопку 4 один раз, получим букву G, а два нажатия на кнопку 4 дадут или букву H (если нажимать быстро) или две буквы G (если нажимать с паузой). Известно, что при наборе пароля из 10 букв были нажаты последовательно кнопки 777255899999. Определите число возможных вариантов паролей.

**Задача 119. Подземелье.** Для открытия подземелья в волшебной стране надо правильно назвать три целых числа  $a, b, c$ , служащих коэффициентами квадратичной функции  $f(x) = ax^2 + bx + c$ . Представителям четырёх рас были переданы следующие значения функции: троллям — значение  $f(21)$ , эльфам —  $f(24)$ , гномам —  $f(25)$ , оркам —  $f(28)$ . Когда представители рас встретились, чтобы совместно найти  $a, b, c$  и открыть подземелье, один из представителей, чтобы сорвать

мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 273, эльфы — 357, гномы — 391, орки — 497.

## 11 класс. 2010 год

**Задача 120. Граф.** Для зашифрования натурального числа  $m$  используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединённые друг с другом, называют соседними. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна  $m$ . Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число  $m$ . Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования указан на рис. 3. На рис. 4 приведён результат зашифрования некоторого числа. Найдите его.

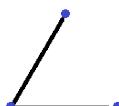


Рис. 1

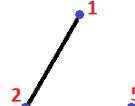


Рис. 2

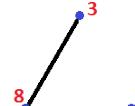


Рис. 3

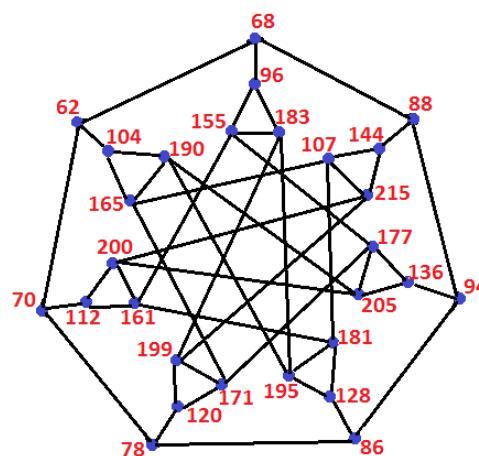


Рис. 4

**Задача 121. Окружность.** В концах диаметра окружности расположены числа 1 и 5, разбивающие окружность на две дуги. Совершим по окружности  $n$  оборотов по часовой стрелке, приняв за начало обхода один из концов диаметра. После прохождения каждой имеющейся на данный момент дуги делим её пополам и в середине записываем число  $(3x + 3y)/2$ , где  $x$  и  $y$  — числа, стоящие на концах пройденной дуги, взятые в порядке направления обхода. Найдите сумму всех записанных чисел после  $n$  оборотов.

**Задача 122. Нейрокомпьютер.** В нейрокомпьютере используется упрощённая модель нейрона — клетки головного мозга. По четырём каналам  $x_1, x_2, x_3, x_4$  в клетку поступают нули и единицы, из которых внутри неё формируется сумма  $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4$  ( $a_1, a_2, a_3, a_4$  — целые числа). Затем  $S$  сравнивается с некоторым целым параметром  $c$ , и если  $S \geq c$ , то на выходе клетки формируется значение  $y = 1$ , иначе —  $y = 0$ . Найдите какие-либо целые параметры  $a_1, a_2, a_3, a_4, c$  такого нейрона, чтобы  $y = 1$  на наборах  $(1,0,1,0)$ ,  $(1,1,1,0)$ ,  $(0,0,1,0)$ ,  $(1,0,0,1)$ ,  $(1,0,1,1)$ ,  $(0,0,1,1)$ ,  $(1,1,1,1)$  и  $y = 0$  — на остальных наборах.

**Задача 123.** В текстовом сообщении на русском языке, записанном без знаков препинания и пробелов, переставили буквы:

нкбакморолаентоиеб.

Затем первую букву заменили буквой, следующей за ней через некоторое число позиций в алфавите, расположенном на круге. Вторую букву заменили буквой, которая следует за ней через другое число позиций в алфавите и так далее. При этом одинаковые буквы могут перейти в разные, а разные — в одинаковые. После этого получили:

иклмноиклмноиклмност.

И наконец, буквы в этой строке выстроили в исходном порядке (т. е., если, например, первую букву исходного сообщения поставили на третье место, то теперь третью букву поставили на первое):

икоокмтисонилнлкмлмн.

Восстановите исходное сообщение.

**Задача 124.** Известно, что число 14197777 равно остатку от деления на 56887111 некоторого числа  $x$ , возведённого в куб. Числа  $x$  и 56887111 имеют общий делитель, отличный от 1, а число 56887111 является произведением двух простых чисел. Найдите хотя бы одно такое число  $x$ .

**Задача 125. Светофильтры.** Крокодил Гена и Чебурашка могут связываться двумя способами: по радиоканалу и оптическому каналу. Используя эти каналы, они хотят договориться о кодовой комбинации сейфа, составленной из 20 букв К, З, С или Ч. Для этого Гена по оптическому каналу передаёт случайную комбинацию из 20 вспышек, причём каждая вспышка может быть красного (К), синего (С) или зелёного (З) цвета. Для каждой вспышки Чебурашка наугад выбирает светофильтр. Если его цвет совпадает с переданным цветом, то срабатывает датчик, а если не совпадает, то цвет вспышки остаётся для Чебурашки неизвестным. После замера всех вспышек Чебурашка по радиоканалу сообщает, какие светофильтры он выбрал. В результате Гена узнаёт номера вспышек, цвет которых Чебурашка определил. Гена устанавливает комбинацию на сейфе так: если цвет очередной вспышки Чебурашке определить удалось, то выбирается буква, соответствующая цвету вспышки (К, З либо С), если нет — выбирается Ч.

Шапокляк прослушивает радиоканал и «встроилась» в оптический канал. На пути передаваемых вспышек она выставляла свои светофильтры: ККЗЗЗСКСКСЗЗСКСКСКЗК — и одновременно передавала вспышки соответствующих цветов Чебурашке. Срабатывание датчика у неё произошло на 6, 10, 11, 14, 17 и 19 вспышках. Чебурашка, не зная о вмешательстве, сообщил по радиоканалу свои цвета: СКЗКККЗЗККСККЗСЗСК. Учитывая собранную Шапокляк информацию определите число кодовых комбинаций, которые гарантированно не откроют сейф.

## 8–9 классы. 2011 год

**Задача 126. Шестерёнки I.** Для шифрования сообщения использовалось устройство из трёх последовательно зацепленных шестерёнок с 5, 30 и 6 зубцами. На зубцах первой шестерёнки записаны по

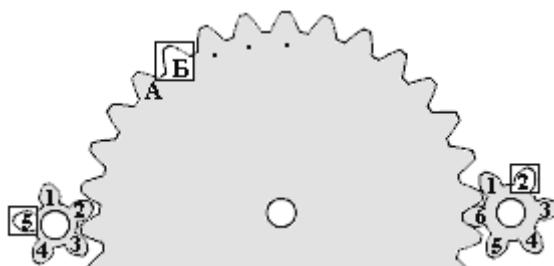
часовой стрелке цифры от 1 до 5, на третьей — от 1 до 6. На второй шестерёнке также по часовой стрелке записан 32-буквенный алфавит:

АВВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЬЭЮЯ.

Для каждой шестерёнки выделено окошко (на рисунке оно изображено квадратиком), в котором видна лишь одна буква или цифра. Сообщение шифровалось побуквенно: вторая шестерёнка вращалась по часовой стрелке, пока в окошке не появится первая буква сообщения. Затем выписывалась пара цифр, открывшихся в окошках первой и третьей шестерёнок. Далее продолжали вращать вторую шестерёнку до появления второй буквы сообщения, выписывали пару цифр из окошек и т. д. Так, для случая, приведённого на рисунке, буква Б заменяется парой 52 (подчеркнём, что рисунок лишь поясняет принцип работы устройства, и на самом деле букве Б может соответствовать другая пара цифр). Начальное взаимное расположение шестерёнок неизвестно. Найдите по известным выписанным парам цифр

11 55 16 53 21 16 31 15 52 14 16 44 46

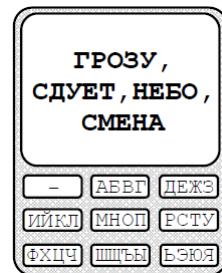
какое сообщение было зашифровано (пробелы в тексте сохранены).



**Задача 127.** Для шифрования передаваемых сообщений Катя и Юра используют следующий способ. Юра заранее выбрал набор коэффициентов  $(2, 5, 8, 16)$ , натуральное число  $u$  и сообщил их Кате. Для шифрования сообщения  $(x_1, x_2, x_3, x_4)$ , состоящего из нулей и единиц, Катя вычисляет сумму  $S = 2x_1 + 5x_2 + 8x_3 + 16x_4$ , а затем находит остаток  $S'$  от деления произведения  $Su$  на 32 и отсылает  $S'$  Юре. Помогите Юре расшифровать сообщение  $S' = 11$ , т. е. найти соответствующую ему строку  $(x_1, x_2, x_3, x_4)$ , если известно, что остаток от деления числа  $7u$  на 32 равен 1.

**Задача 128. Города I.** Когда число городов в Криптоландии достигло  $4^4$ , власти решили провести территориальную реформу, создав 4 провинции по  $4^3$  городов в каждой. В качестве названий городам планировалось присвоить различные обозначения  $(a_1, \dots, a_4)$  — наборы из четырёх целых чисел, в которых  $a_i$  принимают значения от 0 до 3. При этом обозначения каждой пары городов из одной провинции должны были отличаться не менее чем в двух позициях. Укажите какой-либо способ построения такой системы названий.

**Задача 129. Режим Т9 I.** Для шифрования SMS-сообщений использовался следующий способ. Выбиралось секретное осмысленное трёхбуквенное слово. Каждый пробел в сообщении заменялся очередной буквой секретного слова: первый — на первую, второй — на вторую, третий — на третью, четвёртый — снова на первую и т. д. Затем полученная цепочка букв набиралась на клавиатуре с использованием интеллектуального ввода (по типу Т9). При этом при вводе каждой буквы осуществлялось лишь однократное нажатие соответствующей клавиши, а программа интеллектуального ввода выбирала слово из словаря по следующему принципу: первая буква слова выбиралась с первой нажатой клавиши, вторая — со второй и т. д. Полученные таким образом осмысленные слова разделялись запятыми и передавались. Найдите исходное сообщение, соответствующее написанному на экране.



**Задача 130. Радиоканал.** Крокодил Гена посыпает Чебурашке по радиоканалу сообщение, заменяя буквы наборами из нулей и единиц согласно таблице (другие буквы не встретились)

|                   |                   |                   |                   |
|-------------------|-------------------|-------------------|-------------------|
| А (0,0,0,0,0,0,0) | В (1,1,1,0,0,0,1) | Г (1,0,1,0,0,1,0) | Д (0,1,0,0,0,1,1) |
| Е (0,1,1,0,1,0,0) | И (1,0,0,0,1,0,1) | М (1,1,0,0,1,1,0) | О (0,0,1,0,1,1,1) |
| Р (1,1,0,1,0,0,0) | С (0,0,1,1,0,0,1) | Т (0,1,1,1,0,1,0) | У (1,0,0,1,0,1,1) |
| Х (1,0,1,1,1,0,0) | Ч (0,1,0,1,1,0,1) | Ы (0,0,0,1,1,1,0) | Я (1,1,1,1,1,1,1) |

Из-за помех некоторые биты искажились, но не более двух в одном наборе. Определите, какое сообщение отправил крокодил Гена, если Чебурашка получил:

$$\begin{aligned}
 & (1,0,0,1,0,1,1) \quad (0,1,0,0,0,1,1) \quad (0,0,1,0,0,0,0) \quad (1,1,0,1,0,0,0) \\
 & (1,0,1,0,1,1,0) \quad (0,0,0,0,0,0,0) \quad (0,0,1,1,0,0,0) \quad (0,1,1,1,0,1,0) \\
 & (0,0,1,0,1,0,0) \quad (1,1,0,1,0,0,0) \quad (0,0,0,0,0,0,1) \quad (1,0,1,1,0,0,0) \\
 & (0,1,1,1,0,1,0) \quad (0,0,1,0,1,1,0) \quad (1,0,0,0,1,0,1) \quad (0,1,1,0,0,1,0) \\
 & (0,1,1,1,0,1,0) \quad (1,0,0,1,1,1,0) \quad (0,0,1,1,0,0,1) \quad (1,1,1,0,1,1,1) \\
 & (0,1,0,1,1,0,1) \quad (1,0,0,0,0,0,1) \quad (0,1,0,0,0,1,1) \quad (1,1,0,1,0,1,1) \\
 & (1,0,0,1,0,1,1) \quad (1,0,1,0,0,0,0) \quad (1,0,0,0,1,0,1) \quad (1,0,1,1,1,0,0) \\
 & (1,0,0,0,0,1,0) \quad (0,1,0,0,0,1,1) \quad (1,0,0,0,0,1,0) \quad (1,1,0,1,0,0,0) \\
 & (0,0,0,0,1,1,1) \quad (1,0,0,0,0,0,1).
 \end{aligned}$$

**Задача 131.** Милла и Стелла разговаривают по телефону и хотят выбрать секретное число так, чтобы оно осталось неизвестным постороннему, возможно, подслушивающему разговор. Для этого Милла подбирает натуральное число  $a \leq 256$  такое, что числа  $r_{257}(a^i)$  различны при всех  $1 \leq i \leq 256$  и  $r_{257}(a^{256}) = 1$ , где  $r_{257}(t)$  — остаток от деления числа  $t$  на 257. Затем Милла загадывает натуральное число  $x \leq 256$ , а Стелла — натуральное число  $y \leq 256$ . После этого Милла сообщает числа  $a$  и  $r_{257}(a^x)$  Стелле, а Стелла ей — число  $r_{257}(a^y)$ . Теперь они обе вычисляют их секретное число  $r_{257}(a^{xy})$ . Найдите его, если известно, что  $r_{257}(a^x) = 9$ ,  $r_{257}(a^y) = 256$ .

## 10 класс. 2011 год

**Задача 132. Шестерёнки II.** Для шифрования сообщения использовалось устройство из трёх последовательно зацепленных шестерёнок с 5, 30 и 6 зубцами. На зубцах первой шестерёнки записаны по часовой стрелке цифры от 1 до 5, на третьей — от 1 до 6. На второй шестерёнке также по часовой стрелке записан 32-буквенный алфавит:

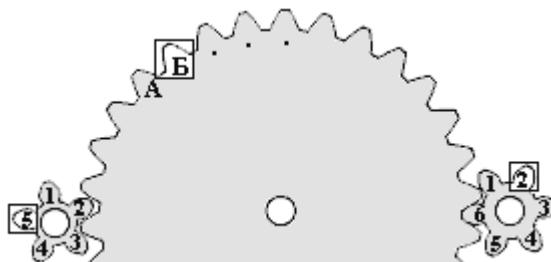
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЬЭЮЯ.

Для каждой шестерёнки выделено окошко (на рисунке оно изображено квадратиком), в котором видна лишь одна буква или цифра. Сообщение шифровалось побуквенно: вторая шестерёнка вращалась по часовой стрелке, пока в окошке не появится первая буква сообщения. Затем выписывалась пара цифр, открывшихся в окошках первой и третьей шестерёнок. Далее продолжали вращать вторую шестерёнку до появления второй буквы сообщения, выписывали пару цифр из

окошечек и т. д. Так, для случая, приведённого на рисунке, буква Б заменяется парой 52 (подчеркнём, что рисунок лишь поясняет принцип работы устройства, и на самом деле букве Б может соответствовать другая пара цифр). Найдите по известным выписанным парам цифр

$$\begin{array}{ccccccccc} 43 & 33 & 55 & 11 & 11 & 31 & 42 & 24 & 32 \\ & & & & & & & 45 & 56 \\ & & & & & & & 13 & 44 \\ & & & & & & & 31 & \\ 55 & 16 & & 23 & 55 & 22 & 15 & 56 & 33 \\ & & & & & & & 56 & 15 \end{array}$$

какое сообщение было зашифровано (пробелы в тексте сохранены).



**Задача 133.** Милла и Стелла разговаривают по телефону и хотят выбрать секретное число так, чтобы оно осталось неизвестным постороннему, возможно, подслушивающему разговор. Для этого Милла подбирает натуральное число  $a \leq 256$  такое, что числа  $r_{257}(a^i)$  различны при всех  $1 \leq i \leq 256$  и  $r_{257}(a^{256}) = 1$ , где  $r_{257}(t)$  — остаток от деления числа  $t$  на 257. Затем Милла загадывает натуральное число  $x \leq 256$ , а Стелла — натуральное число  $y \leq 256$ . После этого Милла сообщает числа  $a$  и  $r_{257}(a^x)$  Стелле, а Стелла ей — число  $r_{257}(a^y)$ . Теперь они обе вычисляют их секретное число  $r_{257}(a^{xy})$ . Найдите его, если известно, что  $a = 6$ ,  $r_{257}(a^x) = 4$ ,  $r_{257}(a^y) = 251$ .

**Задача 134. Города II.** Когда число городов в Криптоландии достигло  $5^4$ , власти решили провести территориальную реформу, создав 5 провинций по  $5^3$  городов в каждой. В качестве названий городам планировалось присвоить различные обозначения  $(a_1, \dots, a_4)$  — наборы из четырёх целых чисел, в которых  $a_i$  принимают значения от 0 до 4. При этом обозначения каждой пары городов из одной провинции должны были отличаться не менее, чем в двух позициях. Укажите какой-либо способ построения такой системы названий.

**Задача 135. Режим Т9 II.** Для шифрования SMS-сообщений использовался следующий способ. Первоначально каждый пробел в исходном сообщении заменялся некоторым трёхбуквенным словом. Затем полученная цепочка букв набиралась на клавиатуре с использованием интеллектуального ввода (по типу Т9). При этом при вводе каждой буквы осуществлялась лишь однократное нажатие соответствующей клавиши, а программа интеллектуального ввода выбирала слово из словаря по следующему принципу: первая буква слова выбиралась с первой нажатой клавиши, вторая — со второй и т. д. Полученные таким образом осмысленные слова разделялись запятыми и передавались. Найдите исходное сообщение, соответствующее написанному на экране.



**Задача 136.** Для шифрования передаваемых сообщений Катя и Юра используют следующий способ. Юра заранее выбрал набор коэффициентов (4, 6, 13, 25), натуральное число  $u$  и сообщил их Кате. Для шифрования сообщения  $(x_1, x_2, x_3, x_4)$ , состоящего из нулей и единиц, Катя вычисляет сумму  $S = 4x_1 + 6x_2 + 13x_3 + 25x_4$ , а затем находит остаток  $S'$  от деления произведения  $Su$  на 49 и отсылает  $S'$  Юре. Помогите Юре расшифровать сообщение  $S' = 47$ , т. е. найти соответствующую ему строку  $(x_1, x_2, x_3, x_4)$ , если известно, что остаток от деления числа  $13u$  на 49 равен 1.

**Задача 137.** В треугольнике  $ABC$  известно:  $BC = 2$ ,  $AC = 3$ , угол  $ACB$  равен  $60^\circ$ . Точки  $M$  и  $K$  удовлетворяют условиям:  $AM : MC = 1 : 2$ ,  $BK : CK = 1 : 2$ . Найдите максимально возможное расстояние между точками  $M$  и  $K$ .

## 11 класс. 2011 год

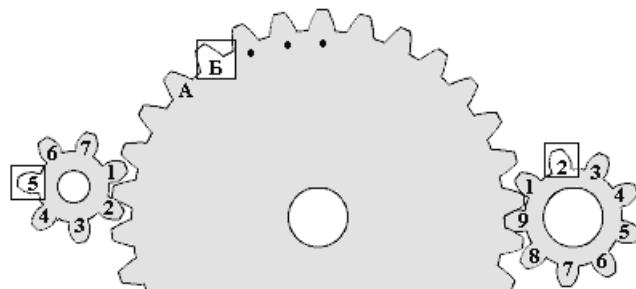
**Задача 138. Шестерёнки III.** Для шифрования сообщения использовалось устройство из трёх последовательно зацепленных шестерёнок с 7, 30 и 9 зубцами. На зубцах первой шестерёнки по часовой записи записаны цифры от 1 до 7, на третьей — от 1 до 9. На второй шестерёнке также по часовой стрелке записан 32-буквенный алфавит:

АБВГДЕЖЗИЙКЛМНОРСТУФХЦЧШЫЬЭЮЯ.

Для каждой шестерёнки выделено окошко (на рисунке оно изображено квадратиком), в котором видна лишь одна буква или цифра. Сообщение шифровалось побуквенно: вторая шестерёнка вращалась по часовой стрелке, пока в окошке не появится первая буква сообщения. Затем выписывалась пара цифр, открывшихся в окошках первой и третьей шестерёнок. Далее продолжали вращать вторую шестерёнку до появления второй буквы сообщения, выписывали пару цифр из окошек и т. д. Так, для случая, приведённого на рисунке, буква Б заменяется парой 52 (подчеркнём, что рисунок лишь поясняет принцип работы устройства, и на самом деле букве Б может соответствовать другая пара цифр). Найдите по известным выписанным парам цифр

11 64 12 46 66 75 56 65    29 42 71 12    23 67 76 28 52,

какое сообщение было зашифровано (пробелы в тексте сохранены).



**Задача 139.** Милла и Стелла разговаривают по телефону и хотят выбрать секретное число так, чтобы оно осталось неизвестным постороннему, возможно подслушивающему разговор. Для этого Милла подбирает натуральное число  $a \leq 256$  такое, что числа  $r_{257}(a^i)$  различны при всех  $1 \leq i \leq 256$  и  $r_{257}(a^{256}) = 1$ , например 3, 5, 6, 7, 10, 12, где  $r_{257}(t)$  — остаток от деления числа  $t$  на 257. Затем Милла загадывает натуральное число  $x \leq 256$ , а Стелла — натуральное число  $y \leq 256$ . После этого Милла сообщает числа  $a$  и  $r_{257}(a^x)$  Стелле, а Стелла ей — число  $r_{257}(a^y)$ . Теперь они обе вычисляют их секретное число  $r_{257}(a^{xy+1})$ . Найдите его, если известно, что  $a = 5$ ,  $r_{257}(a^x) = 16$ ,  $r_{257}(a^y) = 248$ .

**Задача 140.** Каждое из чисел  $x_1, x_2, x_3, x_4, x_5, x_6$  принимает значение либо 0, либо 1. Известно, что числа  $x_1x_2 + x_2x_3 + x_1x_4$ ,  $x_1x_2x_4 + x_5x_6 + x_4$ ,  $x_2x_6 + x_4 + x_5$ ,  $x_1x_2x_4 + x_4x_6 + x_2x_3$ ,  $x_1x_4 + x_2x_6 + x_3$  чётны, а число  $x_1x_4 + x_4x_6 + x_4$  нечётно. Найдите все варианты для  $x_1, x_2, x_3, x_4, x_5, x_6$ .

**Задача 141. Режим Т9 III.** Для шифрования SMS-сообщений использовался следующий способ. Выбиралось секретное осмысленное трёхбуквенное слово. Каждый пробел в сообщении заменялся очередной буквой секретного слова: первый — на первую, второй — на вторую, третий — на третью, четвёртый — снова на первую и т. д. Затем полученная цепочка букв набиралась на клавиатуре с использованием интеллектуального ввода (по типу Т9). При этом при вводе каждой буквы осуществлялось лишь однократное нажатие соответствующей клавиши, а программа интеллектуального ввода выбирала слово из словаря по следующему принципу: первая буква слова выбиралась с первой нажатой клавиши, вторая — со второй и т. д. Полученные таким образом осмысленные слова разделялись запятыми и передавались. Найдите исходное сообщение, соответствующее написанному на экране.



**Задача 142. Пароль.** Перед записью в память сервера пароли пользователей системы преобразуются. Сначала обрабатывается первая и вторая буква пароля, затем вторая и третья и т. д. Пара букв представляется набором, состоящим из двенадцати битов  $x_1, \dots, x_{12}$ , первые шесть из которых соответствуют первой букве, а вторые шесть — второй согласно таблице:

Биты получившегося набора подаются на четыре одинаковых логических элемента. На вход каждого из них поступает три бита, а на выходе формируется значение  $f(x, y, z)$ , равное 1, если среди битов  $x, y, z$  больше единиц, чем нулей, иначе формируется значение 0. В память сервера для каждой пары букв записывают четыре бита:  $(f(x_1, x_2, x_3), f(x_4, x_5, x_6), f(x_7, 1 - x_8, x_9), f(x_{10}, 1 - x_{11}, x_{12}))$ . Определите осмыслиенный пароль, если в памяти компьютера он хранится в следующем сжатом виде:  $(0,1,1,0), (0,0,1,0), (1,0,1,0), (0,0,1,0), (0,0,1,0), (0,0,1,1), (0,0,0,0), (0,1,1,0), (0,0,0,1)$ .

**Задача 143.** В треугольнике  $ABC$  известно:  $BC = 2$ ,  $AC = 3$ , угол  $ACB$  равен  $60^\circ$ . Точки  $M$  и  $K$  удовлетворяют условиям:  $AM : MC = 1 : 2$ ,  $BK : CK = 2 : 3$ . Найдите максимально возможное расстояние между точками  $M$  и  $K$ .

## 9 класс. 2012 год

**Задача 144.** Известно, что 20-значное число  $A$  делится нацело на 143,  $A = 2013x2013x2013x2013x$ . Найдите все возможные значения цифры  $x$ . Решение обоснуйте.

**Задача 145. Вышивка крестиком I.** Ксюша вышивала крестиком. Внутри вышивки размером 27 на 50 клеточек она скрыла послание Серёже. В сообщении она заменила каждую букву парой цифр, соответствующих их номерам в алфавите: А = 01, Б = 02, ..., Я = 33, и пронумеровала полученные цифры (слева направо): 1, 2, 3, ... Затем выбрала натуральное число  $p$ . Для каждой цифры послания с номером  $k$  крестик нужного цвета вышивался в клетке с номером  $pk$ . Нужный цвет определялся по таблице:

|       |   |   |   |   |   |   |   |   |   |   |
|-------|---|---|---|---|---|---|---|---|---|---|
| Цифры | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| Цвета | x | . | & | : | * | > | < | s | = | ж |

Клетки в схеме нумеруются слева направо снизу вверх (например, левая нижняя клетка имеет номер 1, а клетка над ней — 51). Затем Ксюша почти завершила оставшуюся часть картинки, не успев вышить две нижние строки. Прочитайте скрытое послание.

```

. . < . . . . > x x s x x s x x = * x x s x = * > = s x s x x s x x x s x x s x = x s > > . . . < .
. . . < . < > s x s x s x s = x x = . x = x x x > s s x x x x s = = * < > x x x s x x * . . . . < .
. . . . . < s x s s s x x x x s = x = = x x = x & x x * x * x s x * > * = x x x x x . . . . < .
. . . . . : . x s x x = s x s * x s x x x x x x x x s s x : < * = * > < = = x x x x : . . . . .
. . . . . : * s x x & = x = x x s s s x x x s x . s x x x * = x = = = < * x = x x . . . < .
. . . . . > x x s s s x s s s x s s x x x x x = x x * x s x * x s x = * s x s x = . . . .
< . . . . . s x x x x < : . x x s x x x x s x x x s x = s s > x s s s x s x x x s x = < . . . .
. . . . . * s x & & & > < < x & x s x s x s x s x s x s x s x x x s x = < . . . .
< . > . . > x & x = x & x > . . . x s x s x s x s x s x s x x x = x = . . < & x x x . . . .
. . . > x x x x : . < = s & x s x . . . x & x x x s s x s * > x x x x . . . x & x x s * < . . .
. < > = x x & x s s * < = s & & & x x s s s x x x s x & x x x < . x s s . . x s s = : x x x * : . . .
. > * x s x x x s x x = : = * x x x x x x x x & & s s x x x < . . . s x x = > < = > x x x s * x .
< > s s x < x & x s x s = = = * = s & & & & & & & & x s & & x x s & & x * = x s x = x x x s s : .
x x x < > x : x x = x s s : < . . > x & & & & & & & & & x x = x x x x x x & s * = s x : .
> = x s : * x x & x x s s x x : . . & & & & & & & & x . . : = = s x x & x x = x x > .
x & x x x = = s x & & x s x x : . . & & & & & & & & x . < = x x s x x x x x = x > x s .
: * & & x s x x = x x & & & x & s s s & & & & & & & & & < : x x x s x & x = s = * = = s x
= x x x s x & x s x s x x x x & x & & & & & & & & & x s x & & & & x s x = : x x > x s x
x s : x & x s * = x s x s x x s x x & x & & & & & & & & x s s = s x x x x x x s s
. = x & x : > > * > s x s = x x x s * > x & & & > & & & & & x s s x * * = * x s x x s s x x & s =
. < = x * > * x = * x x x s s = = x * x x & & & & & x x > s x * x x x s x x x s * > > x s .
< > x s x * s x x x = x x x x x x & & x s s x x x x & & x s = x x x s s x x x = * * : < * x s
: * x x > x & x x x x = x x : * & x x x x = x = s x x x x & x x x x x x & s x x x x s = . s x
> s x x * x x x x s s s x < . * x x s x x x = x x x x & x x x s x x x x x x x s s x s * s x > * x
> s x = x s * x s x x x = x s x s s x x x = x x s & x s x s x s s s x > x x x x = x x < x

```

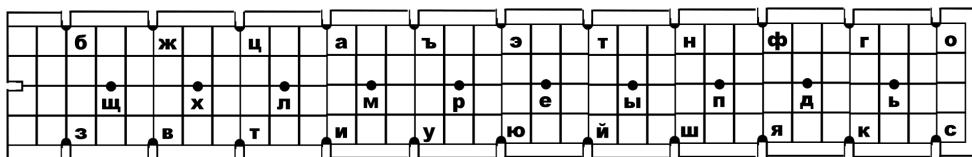
**Задача 146.** Для записи текста используются только заглавные буквы, пробелы, точки и запятые — всего различных 36 символов. При *зашифровании* каждый символ заменили числом от 0 до 35, в соответствии с порядком в «расширенном» алфавите. Затем полученную последовательность чисел разбили на пары, а каждую пару заменили по правилу: пару  $(a_1, a_2)$  заменили на пару  $(r_{36}(a_1 \cdot n), r_{36}(a_1 \cdot k + a_2 \cdot m))$ , где  $r_{36}(x)$  — остаток от деления числа  $x$  на 36, а  $n, k$  и  $m$  — заранее выбранные целые числа от 0 до 35. Найдите все наборы чисел  $n, k$  и  $m$ , при которых разные пары переходят в разные (это необходимо для возможности *расшифрования* текста). Сформулируйте правило расшифрования для случая  $n = k = m = 17$ . Решение обоснуйте.

**Задача 147. Криптохауз I.** Помещения здания «Криптохауз» открываются пластиковыми карточками, на которых записаны кодовые комбинации из нулей и единиц длины 8. Коды для помещений на первом этаже имеют вид  $(10****0*)$ , на втором —  $(**1*1***)$ , на третьем —  $(1****0**)$ . На местах, помеченных символом  $*$ , может

быть и 0, и 1. Каждый из 45 работников «Криптохауза» имеет ровно по одному ключу. Найдите количество работников, имеющих доступ ровно на один этаж, если получена информация о наличии ключей существующих типов:

| Тип        | Кол-во |
|------------|--------|
| (101*1*0*) | 6      |
| (1*1*10**) | 9      |
| (10***00*) | 9      |
| (101*100*) | 2      |

**Задача 148. Линейка и нить I.** При осмотре логова древних хакеров археологами были обнаружены следующие предметы, вероятно использовавшиеся для шифрования информации: линейка (см. рис.); и катушка с белой нитью, на которую были нанесены черные метки. Расстояния между последовательными метками, измеренные в единицах деления линейки, равны 74,5; 85; 90; 90; 86; 18. Прочитайте сообщение, зашифрованное хакерами.



## 10 класс. 2012 год

**Задача 149.** Известно, что 10-значное число  $A = 2013x2013y$  делится нацело на 121. Найдите все возможные пары цифр  $(x, y)$ . Решение обоснуйте.

**Задача 150.** При передаче сообщения по факсу, произошел сбой. В результате на листе было напечатано (изображение увеличено):



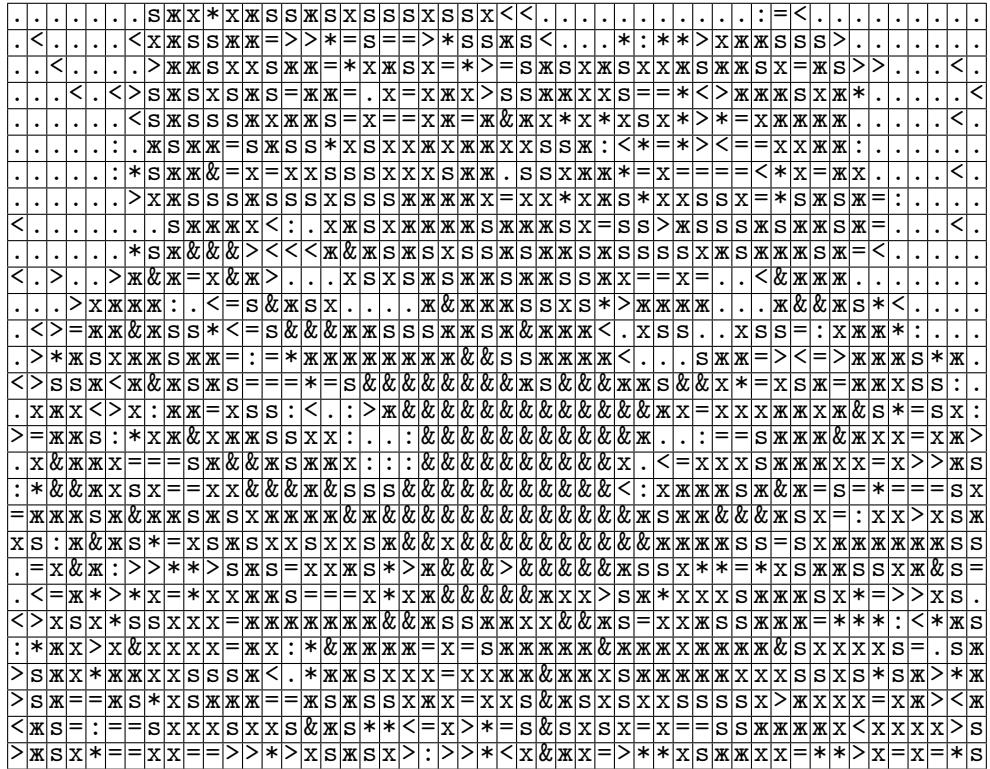
Восстановите текст (ответ обоснуйте). Известно, что исходный шрифт выглядел так:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ъ Э Ю Я.

**Задача 151. Вышивка крестиком II.** В картинке, вышитой «крестиком», Ксюша скрыла послание Серёже. Буквы она заменила парами цифр в соответствии с алфавитным порядком: А = 01, Б = 02, ..., Я = 33. Затем Ксюша выбрала простое число  $p$ . Для цифры послания с номером  $k$  крестик нужного цвета вышивался в клетке с номером  $pk$ . Нужный цвет определялся по следующей таблице:

|       |   |   |   |   |   |   |   |   |   |   |
|-------|---|---|---|---|---|---|---|---|---|---|
| Цифры | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| Цвета | х | . | & | : | * | > | < | s | = | ж |

Клетки в схеме нумеруются слева направо снизу вверх (например, левая нижняя клетка имеет номер 1, а клетка над ней — 51). Затем Ксюша завершила оставшуюся часть картинки. Прочтите скрытое послание.



**Задача 152.** Пусть  $a_{i,j}$  — число, стоящее в строке с номером  $i$  и столбце с номером  $j$  в квадратной таблице  $A$ :

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 6 | 7 | 8 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 5 | 8 | 7 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 8 | 5 | 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 7 | 6 | 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 9 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 9 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 9 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 4 | 2 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 2 | 3 |

По таблице  $A$  построена таблица  $B$ , в строке с номером  $i$  и столбце с номером  $j$  которой стоит выражение  $x^{2^{a_{ij}}}$ . Набор из десяти клеток таблицы будем называть «правильным», если в нём присутствуют ровно по одной клетке из каждого столбца и каждой строки. Вычисляются произведения элементов, входящих в правильные наборы. Результатом являются выражения вида  $x^n$ . Такое  $n$  будем называть степенью правильного набора. Найдите наибольшую возможную степень правильного набора и число правильных наборов степени 1023.

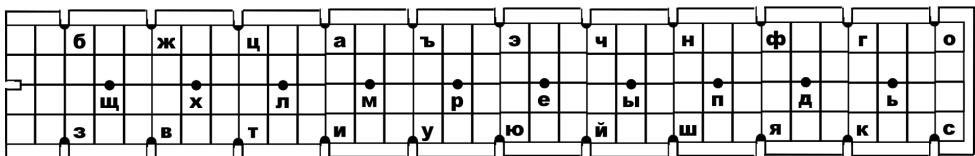
**Задача 153. «Рукопожатие» I.** При установке соединения между компьютерами  $A$  и  $B$  используется следующий вариант «процедуры рукопожатия»:

- 1)  $A$  выбирает натуральное число  $x$ , не большее 5250, и пересылает  $B$  значение функции  $F(x)$ , а затем  $B$  пересылает  $A$  число  $F(x+1)$ ;
- 2) теперь  $B$  выбирает натуральное число  $y$ , не большее 5250, и пересылает  $A$  число  $F(y)$ ,  $A$  пересылает в ответ  $F(y+1)$ . При этом,  $F(t) = r_{5251}(t^3)$ , где  $r_{5251}(t)$  — остаток от деления целого числа  $t$  на число 5251.

Найдите числа  $x$  и  $y$ , если в сети последовательно наблюдались числа: 506, 519, 229 и 231. Замечание: известно, что в компьютерах  $A$  и  $B$  реализована процедура, решающая уравнение  $r_{5251}(x^3) = a$ , где  $x$  — неизвестное целое число,  $0 \leq x \leq 5250$ , и число 5251 выбрано так, что это уравнение имеет единственное решение.

**Задача 154. Линейка и нить II.** При осмотре логова варваров-хакеров сотрудниками информационной полиции были обнаружены

следующие предметы, использовавшиеся для шифрования информации: линейка (см. рис.) и катушка с белой нитью, на которую были нанесены чёрные метки. Расстояния между последовательными метками, измеренные в единицах деления линейки, равны 72; 87,5; 65,5; 51,5; 65,5; 108. Прочитайте сообщение, зашифрованное хакерами.



## 11 класс. 2012 год

**Задача 155.** Докажите, что среди любых пяти натуральных чисел найдутся три, сумма которых делится на три, а среди любых 25 — девять, сумма которых делится на девять.

**Задача 156. «Рукопожатие» II.** При установке TCP/IP соединения между компьютерами А и В

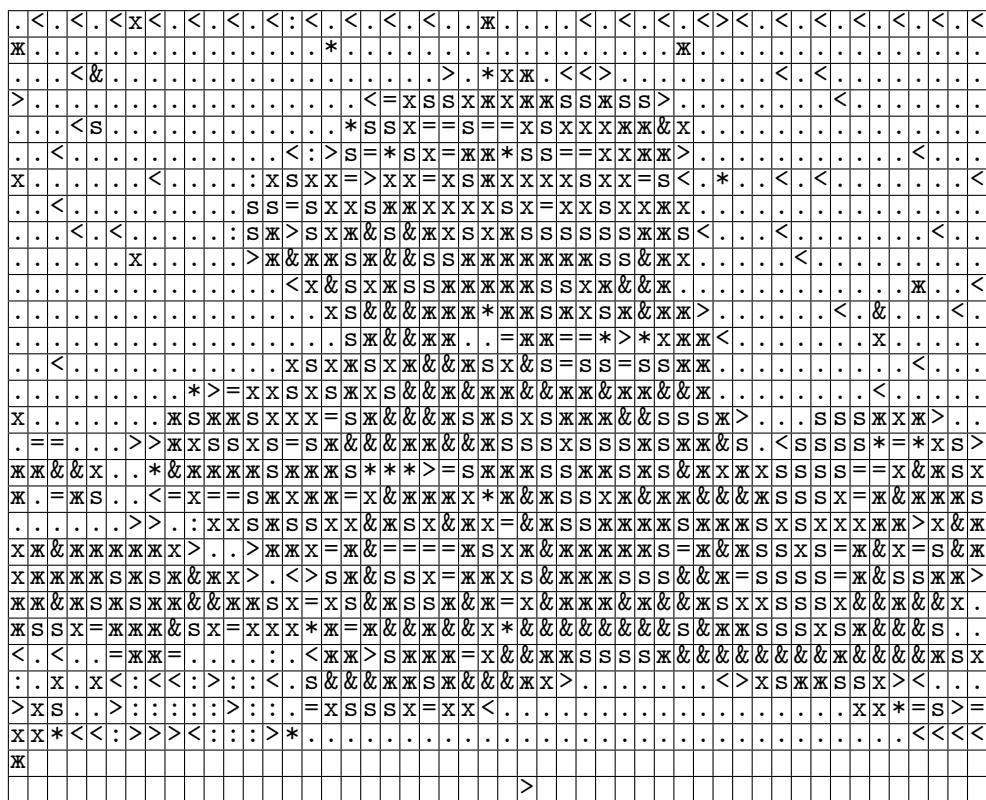
- 1) А выбирает натуральное число  $x$ , не большее 5988, и передает В значение функции  $F(x)$ , а В отвечает А числом  $F(x + 1)$ ;
- 2) В выбирает натуральное число  $y$ , не большее 5988, и передает А число  $F(y)$ , при этом А отвечает В числом  $F(y + 1)$ .

Значение функции  $F$  равно остатку от деления на 5989 значения аргумента, возведённого в третью степень. Найдите числа  $x$  и  $y$ , если в сети последовательно наблюдались числа: 1369, 1421, 2795 и 2804. Примечание: число 5989 выбрано так, что значение аргумента определяется по значению функции  $F$  однозначно.

**Задача 157. Вышивка крестиком III.** Ксюша вышивала крестиком. Внутри вышивки она скрыла послание Серёже. Для этого она представила русские буквы парами цифр в соответствии с их номерами в алфавите: А = 01, Б = 02, ..., Я = 33, а затем цифры — цветами (в таблице ниже представлены условные обозначения использованных цветов).

|       |   |   |   |   |   |   |   |   |   |   |
|-------|---|---|---|---|---|---|---|---|---|---|
| Цифры | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| Цвета | x | . | & | : | * | > | < | s | = | ж |

Сначала она вышила само послание. При этом крестик, соответствующий цифре послания с номером  $k$ , она вышивала в позиции с номером  $k^2 + ak + b$ . Позиции нумеруются слева направо, сверху вниз (например, левая верхняя клетка имеет номер 1, а клетка под ней — номер 51). Затем Ксюша стала заполнять оставшуюся часть картички, но последние две строчки вышить не успела. Прочитайте спрятанное послание.



**Задача 158. Криптохауз II.** Номера гостиницы «Криптохауз» открываются магнитными карточками, на которых записаны ключевые последовательности из нулей и единиц длины 8. Чтобы карточка открыла номер класса «эконом», необходимо, чтобы на ней был записан ключ вида  $(10****0*)$ , номер «стандарт» — ключ вида  $(**1*1***)$ , «люкс» —  $(1****0**)$ . На местах, помеченных символом  $*$ , может быть любой из двух символов. Каждый из 174 работников «Криптохауза» имеет ровно по 9 различных ключей и может использовать

только их. Известно, что любой из существующих ключей изготовлен ровно в 27 экземплярах и находится в пользовании. Найдите минимальное число работников, открывающих номера класса «эконом», если получена информация о наличии ключей существующих видов:

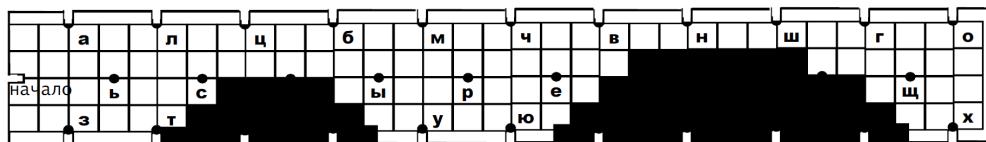
| Вид         | Кол-во |
|-------------|--------|
| (**1*1****) | 21     |
| (1****0**)  | 23     |
| (101*10**)  | 4      |
| (1*1*10**)  | 5      |
| (10***00*)  | 4      |
| (101*100*)  | 1      |

**Задача 159.** В клетках таблицы записаны числа, являющиеся степенями числа 2.

|     |     |     |     |     |     |     |   |   |   |
|-----|-----|-----|-----|-----|-----|-----|---|---|---|
| 16  | 32  | 64  | 128 | 1   | 1   | 1   | 1 | 1 | 1 |
| 32  | 16  | 128 | 64  | 1   | 1   | 1   | 1 | 1 | 1 |
| 64  | 128 | 16  | 32  | 1   | 1   | 1   | 1 | 1 | 1 |
| 128 | 64  | 32  | 16  | 1   | 1   | 1   | 1 | 1 | 1 |
| 1   | 1   | 1   | 1   | 256 | 512 | 1   | 1 | 1 | 1 |
| 1   | 1   | 1   | 1   | 512 | 1   | 256 | 1 | 1 | 1 |
| 1   | 1   | 1   | 1   | 1   | 256 | 512 | 1 | 1 | 1 |
| 1   | 1   | 1   | 1   | 1   | 1   | 1   | 2 | 4 | 8 |
| 1   | 1   | 1   | 1   | 1   | 1   | 1   | 4 | 8 | 2 |
| 1   | 1   | 1   | 1   | 1   | 1   | 1   | 8 | 2 | 4 |

Набор из десяти клеток таблицы будем называть «правильным», если в нём присутствуют ровно по одной клетке каждого столбца и каждой строки. Найдите наибольшую возможную сумму чисел в клетках правильного набора и число правильных наборов с суммой 1023.

**Задача 160. Линейка и нить III.** При раскопках стоянки первобытных хакеров были обнаружены приспособления, предположительно использовавшиеся для шифрования паролей: частично повреждённая фигурная линейка (см. рис.) и катушка с белой нитью, на которую нанесены одинаковые чёрные метки. Расстояния между последовательно идущими метками измерены в единицах деления найденной линейки и равны: 29,5; 24,5; 90; 29,5; 40; 32. Прочитайте пароль, зашифрованный хакерами.



### 8–9 классы. 2013 год

**Задача 161. Беговые роботы I.** На соревнованиях беговых роботов было представлено некоторое количество механизмов. Роботов выпускали на одну и ту же дистанцию попарно. В протоколе фиксировались разности времен финиша победителя и побежденного в каждом из забегов. Все они оказались разными: 1 сек., 2 сек., 3 сек., 4 сек., 5 сек., 6 сек. Известно, что в ходе бегов каждый робот соревновался с каждым ровно один раз, и что каждый робот всегда бегал с одной и той же скоростью. Определите число представленных на бегах механизмов, а также время прохождения дистанции каждым из них, если лучшее время прохождения дистанции было равно 30 секундам.

**Задача 162.** В таблицу, состоящую из  $n$  строк и  $m$  столбцов, записаны числа так, что сумма элементов в каждой строке равна 790, а сумма элементов в каждом столбце равна 1422. Найдите числа  $n$  и  $m$ , при которых выражение  $3n - 4m$  принимает наименьшее возможное натуральное значение. При найденных параметрах  $n$  и  $m$  приведите пример указанной таблицы, в которой не все элементы одинаковы.

**Задача 163. Многократное шифрование I.** Стёпа и Миша разработали следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задаётся таблицей.

|   |   |   |   |   |   |   |   |    |    |
|---|---|---|---|---|---|---|---|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9  | 10 |
| 7 | 9 | 2 | 8 | 6 | 5 | 1 | 3 | 10 | 4  |

То есть, первая буква каждой части ставится на 7 место, вторая — на 9 место и т. д. Однажды Стёпа собрался отправить сообщение Мише. Он его зашифровал, а потом, для пущей надежности, зашифровал

полученный текст еще раз. Подумал, и зашифровал его еще 75 раз. В результате Миша получил вот такое сообщение:

ыновтекнафтеамошьек.

Помогите Мише его прочитать.

**Задача 164.** Функции  $f_0(x), f_1(x), \dots, f_6(x)$  с областью определения  $\{0, 1, 2, 3\}$  и областью значений  $\{0, 1, 2, 3\}$  заданы таблицей.

| $x$ | $f_0(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | $f_4(x)$ | $f_5(x)$ | $f_6(x)$ |
|-----|----------|----------|----------|----------|----------|----------|----------|
| 0   | 0        | 1        | 3        | 2        | 0        | 0        | 0        |
| 1   | 1        | 0        | 2        | 3        | 2        | 2        | 1        |
| 2   | 2        | 3        | 0        | 1        | 1        | 3        | 3        |
| 3   | 3        | 2        | 1        | 0        | 3        | 1        | 2        |

а) Для функции  $f(x)$ , заданной равенствами  $f(0) = 1, f(1) = 2, f(2) = 0, f(3) = 3$  подберите различные числа  $a, b, c \in \{0, 1, \dots, 6\}$  такие, чтобы соотношение

$$f(x) = f_c(f_b(f_a(x))) \quad (2.1)$$

выполнялось для всех  $x = 0, 1, 2, 3$ .

б) Докажите, что для любой функции  $f(x)$  с областью определения  $\{0, 1, 2, 3\}$  и областью значений  $\{0, 1, 2, 3\}$  переводящей разные элементы в разные, найдутся числа  $a, b, c \in \{0, 1, \dots, 6\}$  (не обязательно различные) при которых выполнено равенство (2.1).

**Задача 165. Коммуникатор I.** Разблокировка коммуникатора осуществляется вводом 4-значного числового кода на сенсорном экране. На клавиатуре первоначальная расстановка цифр после ввода кода меняется в зависимости от случайного простого числа  $k$  от 7 до 2017, и на месте цифры  $i$  отображается значение  $a_i$ , равное последней цифре числа  $i \cdot k$ . Пользователь вводит цифры из левой колонки левой рукой, а остальные правой. Восстановите код блокировки, если известно, что при наборе кода пользователь вводил цифры следующим образом:

- при  $a_3 = 3$  : левой, правой, правой, правой;
- при  $a_3 = 9$  : правой, правой, левой, левой;
- при  $a_3 = 1$  : левой, левой, правой, правой;
- при  $a_3 = 7$  : правой, правой, левой, правой.

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline 7 & 8 & 9 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline a_1 & a_2 & a_3 \\ \hline a_4 & a_5 & a_6 \\ \hline a_7 & a_8 & a_9 \\ \hline \end{array}$$

**Задача 166. Пошаговое шифрование I.** Для зашифрования слова из 5 букв на русском языке его:

- 1) преобразовали следующим образом



в цепочку чисел  $x_1, x_2, x_3, x_4, x_5$ ,

- 2) выбрали (секретное) натуральное число  $k_1$  и дописали сумму  $x_6 = x_1 + x_2 + x_3 + x_4 + x_5 + k_1$  к цепочке справа,

3) в расширенной цепочке  $x_1, x_2, x_3, x_4, x_5, x_6$  числа  $x_i$  заменили числами  $y_i$  по формулам:  $y_i = 2x_i + x_{i+1} + k_2$ , если  $i$  нечётное;  $y_i = x_{i-1} + x_i + k_1$ , если  $i$  чётное, где  $k_2$  еще одно (секретное) натуральное число и, наконец,

4) каждое  $y_i$  заменили его остатком от деления на 31.

В результате получили вот что:

10 класс. 2019 год

**Задача 167. Всегда работы 11.** На соревнованиях остовых роботов было представлено некоторое количество механизмов. Роботов выпускали на одну и ту же дистанцию попарно. В протоколе фиксировались разности времен финиша победителя и побежденного в

каждом из забегов. Все они оказались разными: 1 сек., 2 сек., 3 сек., 4 сек., 5 сек., 7 сек. Известно, что в ходе бегов каждый робот соревновался с каждым ровно один раз, и что каждый робот всегда бегал с одной и той же скоростью. Определите число представленных на бегах механизмов, а также время прохождения дистанции каждым из них, если лучшее время прохождения дистанции было равно 30 секундам.

**Задача 168.** В таблицу, состоящую из  $n$  строк и  $m$  столбцов, записаны числа так, что сумма элементов в каждой строке равна 1284, а сумма элементов в каждом столбце равна 1070. Найдите числа  $n$  и  $m$ , при которых выражение  $3n - 4m$  принимает наименьшее возможное натуральное значение. При найденных параметрах  $n$  и  $m$  приведите пример указанной таблицы, в которой не все элементы одинаковы.

**Задача 169. Многократное шифрование II.** Винтик и Шпунтик используют следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задаётся таблицей.

|   |   |   |   |   |   |   |    |   |    |
|---|---|---|---|---|---|---|----|---|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8  | 9 | 10 |
| 7 | 9 | 8 | 1 | 3 | 2 | 4 | 10 | 6 | 5  |

То есть, первая буква каждой части ставится на 7 место, вторая — на 9 место и т. д. Однажды Винтик собрался отправить сообщение Шпунтику. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 333 раза. В результате Шпунтику получил вот такое сообщение:

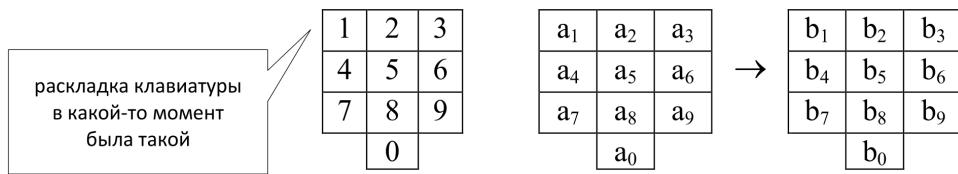
сътуемнсеяиклеонкасо.

Помогите Шпунтику его прочитать.

**Задача 170. Коммуникатор II.** Разблокировка коммуникатора осуществляется вводом 4-значного числового кода на сенсорном экране. При каждом последующем включении устройства, цифры на клавиатуре появляются по закону: на месте цифры  $a_i$  из предыдущего включения появляется цифра  $b_i$ , равная последней цифре числа  $3a_i + 1$ .

Пользователь вводит цифры из левой колонки левой рукой, а остальные правой. Определите возможные коды блокировки, если известно, что при наборе кода при четырёх последовательных включениях коммуникатора, пользователь вводил цифры следующим образом:

- правой, правой, правой, левой;
- левой, правой, левой, правой;
- правой, левой, левой, левой;
- левой, левой, правой, правой.



**Задача 171.** Функции  $f_0(x), f_1(x), \dots, f_6(x)$  с областью определения  $\{0, 1, 2, 3\}$  и областью значений  $\{0, 1, 2, 3\}$  заданы таблицей.

| $x$ | $f_0(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | $f_4(x)$ | $f_5(x)$ | $f_6(x)$ |
|-----|----------|----------|----------|----------|----------|----------|----------|
| 0   | 0        | 1        | 3        | 2        | 0        | 0        | 0        |
| 1   | 1        | 0        | 2        | 3        | 2        | 2        | 1        |
| 2   | 2        | 3        | 0        | 1        | 1        | 3        | 3        |
| 3   | 3        | 2        | 1        | 0        | 3        | 1        | 2        |

а) Для функции  $f(x)$ , заданной равенствами  $f(0) = 3, f(1) = 1, f(2) = 2, f(3) = 0$  подберите различные числа  $a, b, c \in \{0, 1, \dots, 6\}$  такие, чтобы соотношение

$$f(x) = f_c(f_b(f_a(x))) \quad (2.2)$$

выполнялось для всех  $x = 0, 1, 2, 3$ .

б) Докажите, что для любой функции  $f(x)$  с областью определения  $\{0, 1, 2, 3\}$  и областью значений  $\{0, 1, 2, 3\}$  переводящей разные элементы в разные, найдутся числа  $a, b, c \in \{0, 1, \dots, 6\}$  (не обязательно различные) при которых выполнено равенство (2.2).

**Задача 172. Пошаговое шифрование II.** Для зашифрования слова из 9 букв на русском языке его:

- 1) преобразовали следующим образом



в цепочку чисел  $x_1, x_2, \dots, x_9$ ,

2) выбрали (секретное) натуральное число  $k_1$  и дописали сумму  $x_{10} = x_1 + x_2 + \dots + x_9 + k_1$  к цепочке справа,

3) в расширенной цепочке  $x_1, x_2, \dots, x_9, x_{10}$  числа  $x_i$  заменили числами  $y_i$  по формулам:  $y_i = 2x_i + x_{i+1} + (-1)^{\frac{i+1}{2}}k_1$ , если  $i$  нечётное;  $y_i = x_{i-1} + x_i + (-1)^{\frac{i}{2}}k_2$ , если  $i$  чётное, где  $k_2$  еще одно (секретное) натуральное число и, наконец,

4) каждое  $y_i$  заменили его остатком от деления на 32.

В результате получили вот что:

9, 8, 7, 12, 28, 29, 31, 8, 25, 8.

Найдите исходное сообщение.

## 11 класс. 2013 год

**Задача 173. Многократное шифрование III.** Пончик и Незнайка используют следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается на части по 15 букв. В каждой части буквы нумеруются слева направо от 1 до 15 и затем переставляются по правилу, которое задаётся таблицей.

|    |   |   |    |    |   |   |   |    |    |    |    |    |    |    |
|----|---|---|----|----|---|---|---|----|----|----|----|----|----|----|
| 1  | 2 | 3 | 4  | 5  | 6 | 7 | 8 | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| 14 | 5 | 9 | 15 | 10 | 4 | 3 | 7 | 12 | 11 | 13 | 6  | 1  | 2  | 8  |

То есть, первая буква каждой части ставится на 14 место, вторая — на 5 место и т. д. Однажды Незнайка собрался отправить сообщение Пончику. Он зашифровал его, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его

еще 2013 раз. В результате Пончик получил вот такое сообщение:

яттзоелотисспосоамвъртсачсаве.

Помогите Пончику его прочитать.

**Задача 174. Беговые роботы III.** На соревнованиях беговых роботов было представлено некоторое количество механизмов. Роботов выпускали на одну и ту же дистанцию попарно. В протоколе фиксировались разности времен финиша победителя и побежденного в каждом из забегов. Все они оказались разными: 1 сек., 2 сек., 3 сек., 4 сек., 5 сек., 6 сек., 7 сек., 10 сек., 11 сек., 13 сек. Известно, что в ходе бегов каждый робот соревновался с каждым ровно один раз, и что каждый робот всегда бегал с одной и той же скоростью. Определите число представленных на бегах механизмов, а также время прохождения дистанции каждым из них, если лучшее время прохождения дистанции было равно 50 секундам.

**Задача 175.** В таблицу, состоящую из  $n$  строк и  $m$  столбцов, записали числа (не обязательно целые) так, что сумма элементов в каждой строке равна 408, а сумма элементов в каждом столбце равна 340. После чего к таблице приписали  $k$  столбцов, сумма элементов в каждом из которых равна 476, и столбец, сумма элементов в котором равна 272. Получили таблицу, в которой сумма элементов в каждой строке равна 544. Найдите числа  $n$ ,  $m$  и  $k$ , при которых выражение  $2n - 3m + 6k$  принимает наименьшее возможное натуральное значение. При найденных параметрах  $n$ ,  $m$  и  $k$  приведите пример указанной таблицы.

**Задача 176.** Для хранения пароля, записанного в 32-х буквенному алфавите, каждая его буква представляется порядковым номером — парой цифр (т. е. А — 1, Б — 2 и т. д. как в задаче 172). Получается последовательность цифр  $y_1, y_2, y_3, \dots$  Одновременно по правилу  $x_{i+1} = r_{10}(ax_i + b)$ ,  $i \in \mathbb{N}$ , вырабатывается последовательность десятичных цифр ( $x_i$ ), минимальный период которой равен 10, где  $r_{10}(x)$  — остаток от деления  $x$  на 10,  $a$  и  $b$  — натуральные числа. После чего по правилу  $c_i = r_{10}(x_i + y_i)$  вычисляется последовательность ( $c_i$ ), которая и сохраняется в памяти компьютера. Вася выбрал для

пароля очень короткое слово, поэтому при вводе был вынужден повторить его дважды. Помогите ему восстановить забытый пароль, если сохраненная последовательность  $(c_i)$  имеет вид:

3584388279287226.

**Задача 177.** Функции  $f_0(x), f_1(x), \dots, f_{10}(x)$  с областью определения  $\{0, 1, 2, 3, 4\}$  и областью значений  $\{0, 1, 2, 3, 4\}$  заданы следующей таблицей:

| $x$ | $f_0(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | $f_4(x)$ | $f_5(x)$ | $f_6(x)$ | $f_7(x)$ | $f_8(x)$ | $f_9(x)$ | $f_{10}(x)$ |
|-----|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|-------------|
| 0   | 0        | 3        | 4        | 3        | 2        | 0        | 0        | 0        | 0        | 0        | 0           |
| 1   | 1        | 0        | 2        | 4        | 3        | 3        | 4        | 3        | 1        | 1        | 1           |
| 2   | 2        | 1        | 0        | 1        | 4        | 1        | 2        | 4        | 4        | 3        | 2           |
| 3   | 3        | 2        | 1        | 0        | 1        | 4        | 1        | 2        | 2        | 4        | 4           |
| 4   | 4        | 4        | 3        | 2        | 0        | 2        | 3        | 1        | 3        | 2        | 3           |

a) Для функции  $f(x)$ , заданной равенствами  $f(0) = 1, f(1) = 2, f(2) = 4, f(3) = 0, f(4) = 3$ , найдите различные числа  $a, b, c, d \in \{0, 1, \dots, 10\}$  так, чтобы соотношение

$$f(x) = f_d(f_c(f_b(f_a(x)))) \quad (2.3)$$

выполнялось для всех  $x = 0, 1, 2, 3, 4$ .

б) Докажите, что для любой функции  $f(x)$  с областью определения  $\{0, 1, 2, 3, 4\}$  и областью значений  $\{0, 1, 2, 3, 4\}$ , переводящей разные элементы в разные, найдутся числа  $a, b, c, d \in \{0, 1, \dots, 10\}$  (не обязательно различные) при которых равенство (2.3) выполняется для всех  $x = 0, 1, 2, 3, 4$ .

**Задача 178. Пошаговое шифрование III.** Для зашифрования слова из 9 букв на русском языке его:

1) преобразовали следующим образом



в цепочку чисел  $x_1, x_2, \dots, x_{13}$ ,

2) выбрали (секретное) натуральное число  $k_1$  и дописали сумму  $x_{10} = x_1 + x_2 + \dots + x_{13} + k_1$  к цепочке справа,

3) в расширенной цепочке  $x_1, x_2, \dots, x_{13}, x_{14}$  числа  $x_i$  заменили числами  $y_i$  по формулам:  $y_i = 2x_i + x_{i+1} + (-1)^{\frac{i+1}{2}}k_1$ , если  $i$  нечётное;  $y_i = x_{i-1} + x_i + (-1)^{\frac{i}{2}}k_2$ , если  $i$  чётное, где  $k_2$  еще одно (секретное) натуральное число и, наконец,

4) каждое  $y_i$  заменили его остатком от деления на 32.

В результате получили вот что:

$$20, 31, 12, 11, 6, 9, 5, 9, 14, 27, 9, 10, 11, 16.$$

Найдите исходное сообщение.

## 2.8 Задачи олимпиады по компьютерной безопасности

В данном разделе приводится несколько задач из числа тех, которые предлагались школьникам на олимпиаде по информатике и компьютерной безопасности в 2013 году ([www.cryptolymp.ru/olmp\\_it/](http://www.cryptolymp.ru/olmp_it/)).

**Задача 179. Задача о компьютерном вирусе.** Перед группой хакеров стоит задача по выводу из строя компьютеров конкурирующей фирмы. Они создали вредоносное программное обеспечение, распространяющееся в сети. В силу особенностей разработки вирус при распространении с зараженного компьютера всегда поражает либо 4, либо 6 ещё не зараженных. В случае если такого количества незараженных компьютеров нет, то он не имеет возможности распространяться. В сети фирмы зарегистрировано 258 компьютеров. Удастся ли злоумышленникам вывести из строя все компьютеры фирмы при условии, что изначально заражается один компьютер.

**Задача 180. Системы счисления.** При каком основании системы счисления имеет решение следующий ребус:

$$\begin{array}{r} & \text{WZYX} \\ + & \underline{\text{WZXYX}} \\ & \text{YXWZX} \end{array}$$

**Задача 181. Доступ к секретным документам.** В 44 отдельных комнатах хранились секретные документы, по одному в каждой комнате. Все комнаты располагаются так, что их можно обходить по кругу по или против часовой стрелки. Чтобы запутать потенциальных шпионов, два документа из каких-то двух комнат перекладывались в другую соседнюю комнату, следуя по часовой стрелке, а два других — против часовой. Может ли такая схема привести к тому, что все документы соберутся в одной комнате?

**Задача 182. Образ пароля.** Чтобы защитить операционную систему, её разработчики реализовали вход пользователей с использованием пароля. При этом в системе хранится не сам пароль, а его образ, который формируется по следующему принципу. Каждой букве алфавита ставится в соответствие определённое число ( $A = 1$ ,  $B = 2$ ,  $V = 3$  и т. д.). Когда пользователь выбирает себе пароль,  $ABAK$ , то буквам пароля ставятся в соответствие следующие числа:  $A = 1$ ,  $B = 2$ ,  $K = 11$ , а затем вычисляется следующая сумма:  $1 + 2 + 1 + 11 = 15$ . Это число и хранится в системе. Будет ли такая система формирования образа надёжной?

**Задача 183. Закодированное сообщение.** Сообщение содержит 36 групп символов по 6 символов в группе. Оно было представлено файлом объёмом 81 байт (в байте 8 бит). Определите число символов в алфавите, в котором было закодировано сообщение.

## 2.9 Задачи Белорусского государственного университета

НИИ прикладных проблем математики и информатики БГУ открыл на своем сайте (<http://apmi.bsu.by/resources/tasks.html>) задачник. Время от времени здесь появляются очередные задачи по криптографии или смежным областям математики. С разрешения авторов мы приводим эти непростые и весьма любопытные задачи в данном разделе. Сразу предупредим, что для их решения вам потребуются базовые знания криптографии и криптоанализа, комбинаторики, теории чисел, алгебры (конечных полей), теории вероятностей

и программирования. Часть этих знаний вы можете почерпнуть в следующих главах данного пособия (предлагаем заглядывать в них по ходу решения), часть стоит освоить самостоятельно из классических учебников по соответствующим дисциплинам.

## Математические задачи

В задачах участвуют:

**Алиса.** Любит разговаривать по открытым каналам связи. Забывает пароли и вложения к электронным письмам.

**Боб.** Любит разговаривать с Алисой. Читает «Искусство программирования» и «Искусство войны».

**Трент.** Ему доверяют Алиса и Боб. Делает то, что должен делать. Делает это хорошо. Не делает ничего лишнего. Надёжен. Проложил к Алисе и Бобу секретные каналы связи.

**Виктор.** Интересуется всем. В особенности перепиской Алисы и Боба. Владеет искусством перевоплощения.

**Задача 184. (\*\*)** **Первая цифра.** Код сейфа представляет собой последовательность цифр от 1 до 9. Алиса и Боб хотят сгенерировать случайный контрольный код. Каждая из сторон желает влиять на результат генерации. Алиса и Боб договорились, что для генерации каждой цифры кода они будут действовать следующим образом:

1. Алиса выбирает наудачу натуральное  $A$ , не кратное 10;
2. Боб выбирает наудачу натуральное  $B$ ;
3. В качестве цифры кода выбирается первая слева десятичная цифра числа  $A^B$ ;
4.  $A$  и  $B$  уничтожаются.

Виктор обрадован. Почему?

**Задача 185. (\*\*)** **Временной замок.** Боб передает Алисе ключ  $K$  так, чтобы им можно было воспользоваться не сразу, а по истечении определенного времени. Боб выбрал простое  $p = 2^{128} - 159$  и в течение месяца рассчитывал последовательность Фибоначчи по модулю  $p$ :

$$u_0 = 0, \quad u_1 = 1, \quad u_n = (u_{n-1} + u_{n-2}) \bmod p, \quad n = 2, 3, \dots, 2^{64} - 1.$$

Последний элемент последовательности Боб использовал в качестве ключа. Компьютеры Алисы уступают компьютерам Боба и поэтому Боб считает, что для определения ключа Алисе потребуется не меньше месяца. Помогите Алисе найти ключ  $K$  раньше.

**Задача 186. (\*\*)** **Период последовательности.** В качестве гаммы поточного шифра Алиса использует ненулевую двоичную последовательность  $(s_t)$ , заданную следующим рекуррентным соотношением:  $s_{t+128} = (s_{t+1} \oplus 1) \cdot (s_{t+2} \oplus 1) \cdots (s_{t+127} \oplus 1) \oplus s_t \oplus s_{t+1} \oplus s_{t+2} \oplus s_{t+7}$ , где сложение выполняется по модулю 2. Найдите период этой последовательности.

**Последняя теорема Ферма.** Для любого натурального числа  $n > 2$  уравнение  $a^n + b^n = c^n$  не имеет решений в целых ненулевых числах  $a, b, c$ .

**Задача 187. (\*\*)** **Последняя теорема Ферма.** Виктор утверждает, что найденное Уайлсом доказательство последней теоремы Ферма содержит ошибку. Виктор присыпает в математический журнал Selanna показатель  $n > 2$ , для которого он знает (?) решение уравнения  $x^n + y^n = z^n$  в натуральных числах. Трент, который редактирует журнал, просит Виктора предъявить решение. Но Виктор отказывается это сделать, предлагая Тренту сначала анонсировать его открытие. Трент находится в затруднительном положении.

Предложите криптографический протокол, который, с одной стороны, доказывал бы Тренту, что Виктор действительно знает решение, и, с другой стороны, не раскрывал бы это решение.

**Задача 188. (\*\*)** **Цифры.** Трент реализовал в шифровальной машине Amgine алгоритм *Digit*, который берёт на вход вещественное  $x$  и натуральное  $n$  и возвращает  $n$ -й после запятой десятичный знак  $x$ . В качестве  $x$  можно использовать любое аналитически заданное выражение. Например,  $Digit(\pi, 1) = 1$ ,  $Digit(\pi, 2) = 4$ . Алиса и Боб получили Amgine и решили воспользоваться её возможностями следующим образом:

1. Стороны по секретному каналу договариваются об общем ключе  $k$  — большом натуральном числе.
2. Алиса выбирает натуральное  $n$  и вырабатывает гамму  $Digit(a^k, n), Digit(a^k, n + 1), \dots$ , где  $a = 1 + 2\cos(\pi/9)$ .

3. Символы гаммы суммируются с символами открытого текста. Полученный шифртекст отправляется вместе с  $n$ .

Виктор обрадован. Почему?

**Задача 189. (\*) Генерация ключа.** Бобу требуется сгенерировать ключ, который обладает свойствами  $C_1, \dots, C_m$ . Боб выбирает ключ наудачу и проверяет его свойства. Как только одно из свойств не выполняется, Боб генерирует новый ключ, проверяет его и так далее, до тех пор пока не будет найден ключ, обладающий всеми свойствами. Известно, что случайный ключ обладает свойством  $C_i$  с вероятностью  $p_i$  независимо от других свойств. Известно также, что для проверки свойства  $C_i$  требуется время  $t_i$ . В какой очередности Боб должен проверять свойства, чтобы среднее время генерации ключа было минимальным?

**Задача 190. (\*) Отпечатки пальцев.** Боб использует в качестве пароля случайную двоичную строку длины  $n$ . Пароль вводится на сенсорном устройстве Dapi. Виктор может разглядеть отпечатки пальцев Боба и узнать, сколько в пароле единиц и сколько нулей. Виктор может воспользоваться наблюдениями и уменьшить число паролей, которые требуется проверить. Если, например, Виктор знает, что в пароле ровно одна единица, то ему требуется проверить не  $2^n$ , а только  $n$  паролей. Во сколько раз уменьшается среднее число паролей, которые требуется проверить Виктору?

**Задача 191. Поиск вирусов.** Боб проверяет заражение программ на своем компьютере вирусами  $V_1, \dots, V_n$ . Как только в проверяемой программе обнаружена сигнатура некоторого из вирусов, Боб помещает эту программу в карантин и переходит к следующей программе. Известно, что программа заражена вирусом  $V_i$  с вероятностью  $p_i$  независимо от других вирусов. Известно также, что для проверки заражения  $V_i$  требуется время  $t_i$ . В какой очередности Боб должен проверять сигнатуры вирусов, чтобы среднее время проверки было минимальным?

**Задача 192. Протокол аутентификации.** Алиса и Боб проводят взаимную аутентификацию, которая состоит в проверке знания общего секретного ключа  $\mu$ . На этом ключе стороны выполняют шиф-

рование пар 16-байтовых блоков. Используются алгоритмы шифрования в режиме сцепления блоков [СТБ 34.101.31](#). При шифровании выбираются нулевые синхропосылки. Аутентификация проводится по следующему протоколу:

1. Боб выбирает случайный блок  $X_B$  и посыпает его Алисе.
2. Алиса выбирает случайный блок  $X_A$  и посыпает Бобу зашифрованную пару  $(X_A, X_B)$ .
3. Боб выполняет расшифрование принятого сообщения, получая  $(X'_A, X'_B)$ , а затем сравнивает  $X'_B$  с  $X_B$ . Если блоки отличаются, то Боб завершает протокол с ошибкой. В противном случае Боб признаёт подлинность Алисы и отсылает ей зашифрованную пару  $(X_B, X_A)$ .
4. Алиса выполняет расшифрование принятого сообщения, получая  $(X''_B, X''_A)$ , а затем сравнивает  $X''_A$  с  $X_A$ . Если блоки отличаются, то Алиса завершает протокол с ошибкой. В противном случае Алиса признаёт подлинность Боба.

Покажите как Виктор, который не знает  $\mu$ , может ввести Алису в заблуждение, выдав себя за Боба.

**Задача 193. (\*\* Матрицы.** В рассматриваемой системе используется протокол Диффи-Хэллмана. Выбран простой модуль  $p = 2^{127} - 1$  и найден первообразный корень  $g$  по модулю  $p$ . Алиса, Боб, ... выбирают наудачу личные ключи  $a, b, \dots \in \{1, 2, \dots, p - 1\}$  и записывают их на собственные сверхзащищённые носители Dractrams. Для связи друг с другом Алиса и Боб, а также другие пары абонентов, обмениваются открытыми ключами  $g^a, g^b$  и определяют общий ключ  $K = (g^a)^b = (g^b)^a$  (приведение  $\bmod p$  опускается). Трент обратил внимание на то, что вырабатываемый парами ключ  $K$  будет всегда одним и тем же. Это может использовать Виктор, который непрестанно прослушивает каналы связи. Абоненты понимают озабоченность Трента, но не хотят менять надёжно защищенные личные ключи. Выход предложил Боб:

1. Публикуется детерминированный алгоритм, который по номеру сеанса строит матрицу  $M$  порядка 127 над полем из двух элементов. Матрица  $M$  обратима и строится как псевдослучайная.

2. Числа от 0 до  $2^{127} - 1$  отождествляются с двоичными векторами размерности 127. Личный ключ  $k$  (как вектор) умножается на матрицу  $M$  и произведение (как число) обозначается через  $M(k)$ .

3. Алиса определяет сеансовую матрицу  $M$  и посыпает Бобу одноразовый открытый ключ  $g^{M(a)}$ .

4. Боб определяет сеансовую матрицу  $M$  и посыпает Алисе одноразовый открытый ключ  $g^{M(b)}$ .

5. Алиса и Боб вычисляют общий сеансовый секретный ключ  $K_M = g^{M(a)M(b)}$ .

Виктор утверждает, что сможет определить личные ключи Алисы и Боба, перехватив данные 130 сеансов связи. Прав ли Виктор?

**Задача 194. (\*\*)** **Серийное производство.** Трент наладил серийное производство шифровальных машин Amgine и выпустил первую серию из  $n$  машин. Производственные ресурсы Трента практически неограничены, и Виктор не может сделать никаких априорных выводов об объёме серии. Однако известно, что машины снабжены последовательными серийными номерами от 1 до  $n$  и выдаются абонентам в случайном порядке. Виктор узнал, что Алиса получила машину с номером 539, Боб — с номером 734, а Глеб — с номером 222. Помогите Виктору оценить  $n$ .

**Задача 195. (\*\*)** **Генерация простых.** Боб генерирует простые числа, используя теорему Диемитко: если  $q$  — нечётное простое,  $R$  — чётное,  $R < 4(q+1)$ ,  $n = qR + 1$  и для некоторого целого  $a$  выполняются условия:

- 1)  $n$  делит  $a^{qR} - 1$ ;
- 2)  $n$  не делит  $a^R - 1$ ,

то  $n$  — простое. Для построения простого  $n$  битовой длины  $k$  ( $2^{k-1} < n < 2^k$ ) Боб находит  $\lfloor k/2 \rfloor$ -битовое простое  $q$  (выбирает малое простое или генерирует  $q$  снова с помощью теоремы Диемитко). Затем Боб выбирает чётное  $R$  так, что  $n = qR + 1$  имеет нужную длину  $k$  и проверяет условия 1) и 2) для случайного  $a$ . Алгоритм Боба содержит ошибку. Найдите составное  $n$ , которое Боб может признать простым.

**Задача 196. (\*) Социальная сеть.** Алиса и Боб зарегистрировались в социальной сети и вошли в группу любителей рок-группы The Group. Группа секретная, все её члены, и только они, знают секретный ключ  $K$ . Ключ используется в алгоритмах шифрования СТБ 34.101.31 (режим гаммирования с обратной связью). С помощью  $K$  члены группы проверяют друг друга, а также обмениваются продуктами творчества The Group. Пользователь социальной сети, который хочет получить некоторый продукт, обращается с запросом к предполагаемому члену группы. В ответ ему отправляется письмо со случайной синхропосылкой и предлагается зашифровать имя отправителя, используя  $K$  и эту синхропосылку. Если имя зашифровано корректно, то далее высыпается запрошенный продукт, зашифрованный на  $K$ . При шифровании снова используется случайная синхропосылка, которая отправляется вместе с данными. Виктор не входит в группу, не знает  $K$ , он знает только, что Алиса и Боб уже который год разыскивают треки песен «Alice goes to Franc» и «Bronze goes to Bob». Виктор, в свою очередь, желает получить слова секретной песни «Navajo know». Помогите Виктору.

**Задача 197. (\*) Матрицы Belt.** В алгоритме выработки имитовставки стандарта СТБ 34.101.31 (Belt) используются две матрицы над полем  $GF(2)$ :

$$M_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Вместе с единичной матрицей  $M_0$  они образуют множество  $S$ , которое обладает следующим свойством: сумма любого числа любых различных элементов  $S$  является обратимой матрицей. Найдите ещё одну матрицу  $M_3$ , после добавления которой к  $S$  свойство останется справедливым.

**Задача 198. (\*) Истинно-истинно случайные буквы.** Трент подарил Бобу истинно-истинно случайный кубик с шестью гранями, результаты бросков которого независимы и равновероятны. Бросая кубик, Боб генерирует истинно-истинно случайные буквы русского

алфавита. Верно ли, что для генерации отдельной буквы (одной из 33) Боб может использовать менее  $\sqrt{5}$  бросков кубика в среднем? Верно ли, что для генерации отдельной буквы английского алфавита (одной из 26) потребуется больше  $\sqrt{5}$  бросков в среднем? Изменятся ли ответы на предыдущие вопросы при замене  $\sqrt{5}$  на  $21163/9721$ ?

**Задача 199. (\*) Простые делители.** Боб продолжает разрабатывать программу генерации простых чисел  $p > 2^{512}$  для крипtosистемы RSA. Для защиты от некоторых методов факторизации модуля RSA требуется генерировать такие  $p$ , что числа  $p \pm 1$  имеют максимально большие простые делители. Пусть

$$D(p) = \frac{p-1}{q_0} + \frac{p+1}{q_1},$$

где  $q_0$  — максимальный простой делитель  $p - 1$ , а  $q_1$  — максимальный простой делитель  $p + 1$ . Какое минимальное значение может принимать  $D(p)$ ?

**Задача 200. (\*\* Программа EulerPhi.** Бобу требуется написать программу, которая определяет количество различных простых делителей заданного натурального числа  $n$ . Число  $n$  может быть очень большим, его факторизация затруднена. Однако Боб может воспользоваться программой *EulerPhi*, которая выполняется на суперкомпьютере Трента и за приемлемое время находит значение функции Эйлера от  $n$ .

Помогите Бобу, используя следующие дополнительные данные: число простых делителей нечётно и все они имеют вид  $2^s r + 1$ , где  $s$  — натуральное число, общее для всех делителей,  $r$  — нечётное число.

**Задача 201. (\*\* PIN-код.** У Боба все больше пластиковых карточек. Для каждой карточки требуется помнить PIN-код — число  $x$  от 0 до 9999. Как обычно, при трёх попытках ввода неверного PIN карточка блокируется. Боб не может запомнить  $x$  наверняка. Тем не менее, при предъявлении 7 или 8 PIN-кодов конкретной карточки Боб всегда может выбрать из них тройку, в которой обязательно окажется  $x$ . Боб решил действовать следующим образом:

1. Выбирается ключ  $k$  — натуральное число. Ключ записывается в очень защищённый блокнот.

2. PIN  $x$  зашифровывается, ему ставится в соответствие число  $y = (x+1)^k \bmod 10009$ . Шифртекст  $y$  сохраняется в другом, не очень защищённом блокноте.

Боб хочет организовать всё так, чтобы каждому  $y$  соответствовало 7 или 8 вариантов  $x$ . Тогда Боб сможет отобрать три из них, включая правильный, и наверняка пройти аутентификацию с трёх попыток. А вот Виктору, даже если он завладел двумя блокнотами, придётся проверять не менее 7 вариантов. Как Боб должен выбирать  $k$  и как должно быть организовано расшифрование  $y$ ?

**Задача 202. (\*) Связь между филиалами.** Компания Tenhtam является молодой и динамично развивающейся. Приём на работу в Tenhtam идёт по всему миру. Для того, чтобы стать сотрудником требуется ответить всего на один вопрос: каким будет следующий элемент последовательности

$$\frac{4}{10}, \frac{25}{100}, \frac{168}{1000}, \frac{1229}{10000}?$$

Бобу поручено наладить защищённое взаимодействие между филиалами компании. Боб организовал в каждом филиале закрытую корпоративную сеть и установил шифровальную машину Amgine. На Amgine попадает вся исходящая корреспонденция филиала и, наоборот, Amgine доставляет сотрудникам филиала всю адресованную им корреспонденцию. Данные, передаваемые между машинами различных филиалов, зашифровываются на общем парном секретном ключе этих филиалов. Объём передаваемых данных быстро растёт. Боб опасается, что Виктор, который контролирует открытые каналы связи, может накопить много шифрматериала и определить парный ключ. Поэтому каждое утро парный ключ меняется: новый парный ключ является результатом расшифрования текущей даты на старом ключе. Помогите Виктору найти парный ключ.

**Задача 203. (\*) Секретные материалы.** Активист Нед Вонс разместил в Интернете секретные материалы, зашифрованные с помощью AES-256. Каждый месяц Нед рассыпает в редакции газет всего мира ключ, на котором был зашифрован очередной секретный документ, делая его содержимое общедоступным. Документы Неда

производят фурор, все редакции пытаются первыми опубликовать выдержки из них. Уже второй раз подряд в газету Gnutiez приходят письма Виктора. Виктор утверждает, что умеет атаковать AES-256 и в качестве доказательства указывает первый байт следующего ключа, который будет раскрыт Недом. Этот прогноз каждый раз оказывается верным! В третьем письме Виктор предлагает заплатить за предсказание всех следующих ключей. Трент, который редактирует газету, отказывается платить, утверждая, что Виктор — мошенник. Почему Трент так считает?

## Задачи с элементами программирования

**Задача 204. (\*) Трудность обращения хэш-функции.** Функция хэширования FNV обрабатывает сообщение `msg` из `size` байт следующим образом:

```
uint32 fnv32(const uint8* msg, size_t size)
{
    uint32 hash = 2166136261;
    while (size--)
        hash ^= *msg++,
        hash *= 16777619;
    return hash;
}
```

Найдите сообщение `msg`, которое имеет нулевое хэш-значение.

В данном разделе многочлены задаются двоичными словами по следующим правилам. Байту  $u = u_1u_2\dots u_8$  ставится в соответствие многочлен  $u(x) = u_1x^7 + u_2x^6 + \dots + u_8$ . Многочлен ставится в соответствие также любому непустому двоичному слову из целого числа байт. Первому байту соответствует многочлен  $u_1(x)$ , второму —  $x^8u_2(x)$ , третьему —  $x^{16}u_3(x)$  и так далее.

**Задача 205. (\*) Умножение многочленов.** Боб реализует умножение многочленов над полем из двух элементов. Боб утверждает, что при определенном заполнении массивов `log1`, `log2`, `crt1`, `crt2` следующая программа на языке C++ реализует умножение многочлена `a` на многочлен `b`:

```

uint16 mul8x8(uint8 a, uint8 b)
{
    static const uint8 log1[256] = {???};
    static const uint8 log2[256] = {???};
    static const uint16 crt1[256] = {???};
    static const uint16 crt2[256] = {???};

    if (a == 0 || b == 0)
        return 0;

    uint16 d1, d2;
    if (((d1 = log1[a]) += log1[b]) > 255)
        d1 -= 255;
    if (((d2 = log2[a]) += log2[b]) > 255)
        d2 -= 255;

    return crt2[d1] ^ crt1[d2];
}

```

Восстановите заполнение массивов.

**Задача 206. (\*) Деление многочленов.** Боб реализует деление многочленов над полем из двух элементов. Боб написал программу на языке C++, в которой многочлен, заданный строкой байтов `poly`, нацело делится на многочлен  $g(x)$ . Найдите  $g(x)$ .

```

void polyDiv(uint8* poly, size_t n)
{
    uint8 a = 0;
    for (int i = 0; i < n; i++)
    {
        a ^= poly[i];
        a ^= a << 2;
        a ^= a << 4;
        poly[i] = a;
        a >= 6;
    }
}

```

## Непростые навыки программирования

**Задача 207. Программа умножения.** Алиса написала для Amgine программу умножения больших чисел. Программа написана на языке С. Найдите ошибку в программе.

```

typedef unsigned long word;
typedef unsigned long long dword;
void mul(word c[16], const word a[8], const word b
         [8])
{
    size_t i, j;
    word carry;
    dword mul;
    for (i = 0; i < 16; c[i++] = 0);
    for (i = 0; i < 8; ++i)
    {
        for (j = 0, carry = 0; j < 8; ++j)
            ((mul = b[i]) *= a[j]) += carry + c[i + j],
            c[i + j] = mul,
            carry = mul >> sizeof(word) * 8;
        c[i + j] = carry;
    }
}

```

**Задача 208. (\*) Регулярное сложение.** Боб узнал, что если в криптографических программах имеются условные переходы и условия переходов определяются обрабатываемыми данными (но не их размерностями), то эти программы подвержены атакам, основанным на замерах времени или питания. Боб решил переписать программы шифровальной машины Amgine так, чтобы все вычисления были регулярными, т. е. не содержали бы небезопасных условных переходов. Помогите Бобу переписать следующую функцию, реализующую сложение больших чисел:

```

word zzAdd(word c[], const word a[], const word b[],
           size_t n) {
    register word carry = 0;
    register word w;
    size_t i;
    for (i = 0; i < n; ++i) {
        w = a[i] + carry;

```

```

    if (w < carry)
        c[i] = b[i];
    else
        w += b[i], carry = w < b[i], c[i] = w;
}
w = 0;
return carry;
}

```

Функция написана на языке С. Большие числа задаются массивами из  $n$  машинных слов. Буферы  $a$  и  $c$ ,  $b$  и  $c$  либо не пересекаются, либо совпадают.

**Задача 209. (\*) Деление на малые простые.** Боб разрабатывает программу генерации простых чисел для крипtosистемы RSA. Первым этапом теста простоты большого натурального числа  $a$ , заданного  $n$  32-разрядными словами,  $n \geq 8$ , является проверка его делимости на малые простые  $\text{val}$ . Для этого Боб использует следующую функцию языка С, которая находит остаток  $a \bmod \text{val}$ :

```

uint32 zzModVal(const uint32 a[], size_t n, uint32 val)
{
    uint32 r = 0;
    uint64 divisor;
    while (n--)
        divisor = r,
        divisor <= 32,
        divisor += a[n],
        r = (uint32)(divisor % val);
    return r;
}

```

Для определения остатка требуется выполнить  $n$  делений  $\text{uint64} \% \text{uint32}$  и еще  $2n$  сложений и сдвигов. Программа Боба будет использоваться в шифровальной машине Amgine. Деление на этой машине выполняется неэффективно, в 8–10 раз медленнее умножения. Переопишите функцию  $\text{zzModVal}$  так, чтобы в ней использовалось не более 4 делений  $\text{uint32 \% uint32}$ , не более  $2n$  умножений  $\text{uint32 * uint32}$ , а суммарное число сложений и сдвигов увеличилось не более, чем в 2 раза.

# ГЛАВА 3. КОМБИНАТОРНЫЕ ЗАДАЧИ

Эта глава посвящена методам комбинаторики, знание которых очень полезно при решении математических задач криптографии.

Для углублённого изучения комбинаторных методов, применяемых в криптографии, рекомендуем вам учебник В. Н. Сачкова [27].

## 3.1 Сочетания и перестановки

### Биномиальные коэффициенты

Пусть  $A$  — произвольное конечное множество из  $n$  элементов. Число его различных  $k$ -элементных подмножеств называется *числом сочетаний из  $n$  по  $k$*  или просто *биномиальным коэффициентом* и обозначается  $C_n^k$  или  $\binom{n}{k}$ .

**Задача 210.** Докажите, что  $C_n^k = \frac{n!}{k!(n-k)!}$  при  $0 \leq k \leq n$ .

**Задача 211.** Докажите, что  $C_n^0 + C_n^1 + C_n^2 + \dots + C_n^n = \sum_{k=0}^n C_n^k = 2^n$ .

Данное равенство показывает, как легко вычислить число *всех* различных подмножеств множества  $A$ . Эту задачу умели решать в Индии ещё во II веке до н. э.

**Задача 212. Правило Паскаля.** Докажите, что  $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ . Определите, каким образом строится следующий треугольник, называемый *треугольником Паскаля*, и как наглядно пояснить с помощью него правило Паскаля:

$$\begin{array}{ccccccc} n=0 & & & & 1 \\ n=1 & & 1 & & 1 \\ n=2 & & 1 & 2 & & 1 \\ n=3 & & 1 & 3 & 3 & & 1 \\ n=4 & & 1 & 4 & 6 & 4 & 1 \\ n=5 & 1 & 5 & 10 & 10 & 5 & 1 \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

**Задача 213. Биномиальная формула.** Докажите, что для любых чисел  $a, b$  и любого натурального  $n$  справедлива формула

$$(a + b)^n = \sum_{i=0}^n C_n^i a^i b^{n-i},$$

которая уже была, по-видимому, известна персидскому поэту, математику и философи Омару Хайяму (1048–1131).

**Задача 214.** Найдите чему равны выражения:

- а)  $C_n^0 - C_n^1 + C_n^2 - \dots + (-1)^n C_n^n;$
- б)  $C_n^0 + C_n^2 + C_n^4 + \dots;$
- в)  $C_n^1 + C_n^3 + C_n^5 + \dots.$

**Задача 215.** Докажите, что если  $n$  фиксировано, то  $C_n^k$  возрастает по  $k$  при  $k \leq \lfloor n/2 \rfloor$  и убывает при  $k > \lceil n/2 \rceil$ , где запись  $\lfloor x \rfloor$  означает ближайшее целое число к  $x$  снизу, а запись  $\lceil x \rceil$  — ближайшее целое к  $x$  сверху (например,  $\lfloor 3,14 \rfloor = 3$ ,  $\lceil 3,14 \rceil = 4$ ).

**Задача 216. О кодовом замке.** На входных дверях Алисы и Боба стоят кодовые замки. Код — это комбинация различных цифр  $0, 1, \dots, 9$ , которая нажимается одновременно. Известно, что код на двери у Алисы состоит из трёх цифр, у Боба — из двух. Злоумышленник Ева на проверку одной комбинации на кодовом замке тратит 2 секунды. Сколько времени ей понадобится, чтобы подобрать код Алисы и проникнуть в дом? А код Боба? Прежде чем решать, попробуйте предложить свой интуитивный ответ на этот вопрос (хватит ли Еве недели? суток? часа? 10 минут? минуты?), а потом проверьте себя. Сколько цифр должен содержать самый надёжный дверной код? Что изменится, если в кодовой комбинации учитывать порядок цифр (т. е. нажимать их последовательно)?

**Задача 217.** В классе учатся  $n$  девушек и  $m$  юношей. Сколькими способами можно выбрать пару из одной девушки и одного юноши, чтобы назначить их дежурными? А выбрать группу из  $k$  девушек и  $\ell$  юношей для участия в соревнованиях?

**Задача 218. О шахматном городе.** Город — это  $m \times n$  прямоугольных кварталов, раздёлённых  $(n - 1)$  горизонтальными и  $(m - 1)$  вертикальными улицами. Каждому перекрёстку отвечает пара координат  $(i, j)$ . Чему равно число различных кратчайших путей из точки  $(0, 0)$  в точку  $(m, n)$ ?

**Задача 219. Идея на прогулке.** Как, размышляя о шахматном городе, доказать, что  $C_{2n}^n = (C_n^0)^2 + (C_n^1)^2 + \dots + (C_n^n)^2$ ?

**Задача 220. О прямых.** На плоскости проведено  $n$  прямых так, что никакие две из них не параллельны и никакие три не пересекаются в одной точке.

- а) Чему равно число точек пересечения этих прямых?
- б) Сколько различных треугольников образуют прямые?
- в) На сколько частей эти прямые делят плоскость?
- г) Сколько среди этих частей ограниченных и неограниченных?

## Полиномиальные коэффициенты

Полиномиальные коэффициенты возникают, когда мы имеем дело с задачей разбиения множества на части. А именно, пусть  $n = k_1 + k_2 + \dots + k_m$ . Сколькими способами можно разбить  $n$ -элементное множество  $A$  на  $m$  подмножеств  $B_1, \dots, B_m$  так, что  $|B_1| = k_1, \dots, |B_m| = k_m$ ? Это число называется *полиномиальным коэффициентом* и обозначается через  $C_n(k_1, \dots, k_m)$ .

**Задача 221.** Докажите, что  $C_n(k_1, \dots, k_m) = \frac{n!}{k_1!k_2! \cdot \dots \cdot k_m!}$ .

**Задача 222.** Сколько различных слов можно составить, переставляя буквы слова «МАМА»?, слова «МАТЕМАТИКА»?

Решив эту задачу, несложно понять, почему полиномиальный коэффициент называется также *числом перестановок из  $n$  элементов с повторениями*.

## Упорядоченные множества

Множество называется *упорядоченным*, если некоторым образом упорядочены его элементы. И этот порядок важен. Например, упорядоченные множества  $A = \{a, b, c\}$  и  $B = \{b, c, a\}$  различны. Хотя без учёта порядка это одно и то же множество. Нетрудно понять, что существует ровно  $n!$  различных упорядоченных множеств из одних и тех же  $n$  элементов.

**Задача 223.** Сколькими способами можно упорядочить множество  $\{1, 2, \dots, 2n\}$  так, чтобы каждое чётное число имело чётный номер?

**Задача 224. О ладьях.** Сколькими способами можно расположить на шахматной доске 8 ладей так, чтобы они не били друг друга?

**Задача 225.** Сколькими способами можно упорядочить множество  $\{1, 2, \dots, n\}$  так, чтобы числа 1, 2, 3 стояли рядом и в порядке возрастания?

**Задача 226. Гости за круглым столом.** Сколькими способами можно рассадить  $n$  гостей за круглым столом? (Способы считаются одинаковыми, если один можно получить из другого циклической перестановкой.)

## Сочетания с повторениями

Конечному множеству из  $n$  элементов можно придать такой смысл: пусть каждый его элемент обозначает некоторый *тип* предмета. Считаем, что предметов каждого типа существует бесконечно много и между собой они неразличимы. Сколькими способами можно выбрать  $k$  предметов так, что предметы одного типа могут повторяться, но порядок элементов не имеет значения? Это число называется числом *сочетаний из  $n$  элементов по  $k$  с повторениями*.

**Задача 227.** Сколькими способами можно выбрать 7 одинаковых или разных пирожных в кондитерской, в которой есть 12 разных сортов пирожных?

**Задача 228.** Докажите, что число сочетаний из  $n$  элементов по  $k$  с повторениями равно  $C_{n+k-1}^k$ .

**Задача 229.** Сколько различных костей домино можно сделать, используя числа  $0, 1, 2, \dots, n$ ?

## Друзья Боба

В этом небольшом подразделе собраны комбинаторные задачи разных типов.

**Задача 230. Книжная полка.** На полке стоят 12 книг. Сколькими способами можно выбрать 5 книг, не стоящих рядом?

**Задача 231. Домино.** Кости домино сделаны с использованием чисел  $0, 1, 2, 3, 4, 5, 6$ . Сколькими способами можно выбрать пару домино так, чтобы их можно было приложить друг к другу?

**Задача 232.** Сколько различных матриц  $m \times n$ , заполненных элементами 0 и 1, можно составить? Сколько среди них матриц с попарно различными строками?

**Задача 233. Друзья Боба.** У Боба 6 друзей и ежедневно в течение 18 дней он приглашает к себе в гости троих из них так, что компания ни разу не повторяется. Сколькими способами он может это сделать?

**Задача 234. Треугольники.** Сколько существует треугольников, у которых длина каждой стороны принимает одно из четырёх значений  $4, 5, 6, 7$ ?

**Задача 235. Векторы.** Сколько существует различных векторов длины 20 таких, что каждый вектор содержит

- 5 нулей, 4 единицы, 7 двоек, а остальные — тройки?
- в сумме 5 нулей и единиц; 4 двойки, 7 троек, а остальные — четвёрки или пятёрки?

**Задача 236. (\*) Враждующие рыцари.** За круглым столом собрались 12 рыцарей. Каждые два соседних рыцаря враждуют между

собой. Сколькими способами можно выбрать 5 попарно невраждующих друг с другом рыцарей? (Способы рассадки считаются одинаковыми, если один можно получить из другого циклической перестановкой.)

## 3.2 Метод включения и исключения

Пусть  $A_1, \dots, A_m$  — некоторые подмножества  $n$ -элементного множества  $A$ . Определим  $n_0$  — число элементов множества  $A$ , не принадлежащих ни одному из подмножеств. Для этого вычислим значения:

$b_i$  — число элементов, принадлежащих множеству  $A_i$ ;

$b_{i_1, i_2}$  — число элементов, принадлежащих множеству  $A_{i_1} \cap A_{i_2}$ ;

...

$b_{i_1, \dots, i_k}$  — число элементов в множестве  $A_{i_1} \cap \dots \cap A_{i_k}$ ;

После этого вычислим:

$n_1 = b_1 + \dots + b_m$  (сумма всех  $b$  с одним индексом);

$n_2 = \sum b_{i_1, i_2}$  (сумма всех  $b$  с двумя индексами);

...

$n_k = \sum b_{i_1, \dots, i_k}$  (сумма всех  $b$  с  $k$  индексами);

Тогда  $n_0 = n - n_1 + n_2 - n_3 + \dots + (-1)^m n_m$ .

Можно понимать задачу так. Есть набор из  $n$  элементов. Есть  $m$  определённых свойств. Каждый элемент может обладать какими-то из них, а может и не обладать. Удобно считать, что элемент обладает  $i$ -м свойством, если и только если он принадлежит множеству  $A_i$ . Тогда сколько элементов не обладают ни одним свойством? По методу включения и исключения это число равно  $n_0$ . А сколько элементов обладают хотя бы одним свойством? Всё просто:  $n - n_0$ .

**Задача 237. Полиглоты.** Из 100 студентов английский язык знают 28, немецкий — 30, итальянский — 42, английский и немецкий — 8, английский и итальянский — 10, немецкий и итальянский — 5, все три языка знают 3 студента, а декан факультета свободно говорит по-испански. Сколько студентов не знают ни одного языка?

**Задача 238. Ладьи на прогулке.** Сколькими способами можно разместить 8 ладей на шахматной доске так, чтобы они, во-первых,

не могли бить друг друга, а во-вторых, чтобы ни одна из ладей не стояла на белой главной диагонали?

**Задача 239. Ящики и предметы I.** Сколько способами можно разместить  $m$  различных предметов по  $n$  ящикам так, чтобы ни один ящик не был пуст?

**Задача 240. Ящики и предметы II.** Сколько способами можно разместить  $m$  различных предметов по  $n$  ящикам так, чтобы ровно  $\ell$  ящиков оказались пустыми?

**Задача 241. Ящики и предметы III.** Сколько способами можно разместить  $m$  различных предметов по  $n$  ящикам так, чтобы не менее  $\ell$  ящиков оказались пустыми?

**Задача 242. (\*) Перестановки цифр.** Сколько способами можно переставить в числе 12341234 цифры так, чтобы никакие две одинаковые цифры не шли друг за другом?

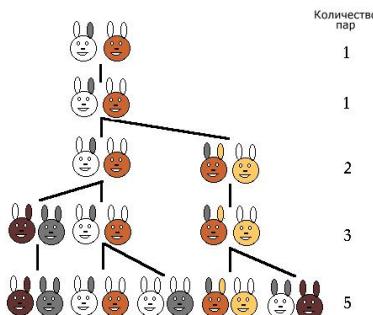


**Задача 243. (\*) Задача мажордома.** К обеду за круглым столом приглашены  $n$  пар враждующих рыцарей ( $n \geq 2$ ). Требуется рассадить их так, чтобы никакие два врага не сидели рядом. Докажите, что это можно сделать  $\sum_{k=0}^n (-1)^k C_n^k 2^k (2n - k - 1)!$  способами. (Способы считаются одинаковыми, если один можно получить из другого циклической перестановкой.)

**Задача 244. (\*) О беспорядках.** Беспорядок на  $n$  элементах — это перестановка чисел  $1, 2, \dots, n$  такая, что ни одно число не стоит на своём месте. Например,  $(34152)$  — беспорядок, а  $(34125)$  — нет. Чему равно число беспорядочных перестановок на  $n$  элементах?

### 3.3 Числа Фибоначчи

«Пара кроликов приносит раз в месяц приплод из двух крольчат (самки и самца), причём новорождённые крольчата через два месяца после рождения уже приносят приплод. Сколько пар кроликов появится через год, если в начале года была одна пара кроликов и ни одна пара за год не погибла?» — эта задача была сформулирована Леонардо Фибоначчи в его книге «*Liber Abaci*» в 1202 г.



Если число пар кроликов в начале  $i$ -го месяца обозначить за  $u_i$ , то мы придём к знаменитой *последовательности Фибоначчи*:

$$u_1 = 1, u_2 = 1, u_n = u_{n-1} + u_{n-2},$$

свойства которой предлагаются изучить, решая следующие задачи.

**Задача 245. Числа Фибоначчи и векторы.** Докажите, что число  $\ell(n)$  двоичных векторов длины  $n$  таких, что в каждом из них никакие две единицы не стоят рядом, равно  $u_{n+2}$ .

**Задача 246. Диагональ Паскаля.** Докажите, что  $\ell(n) = C_{n+1}^0 + C_n^1 + C_{n-1}^2 + \dots + C_{n-s+1}^s$ , где  $s = \lfloor (n+1)/2 \rfloor$ . Почему задаче дано такое название?

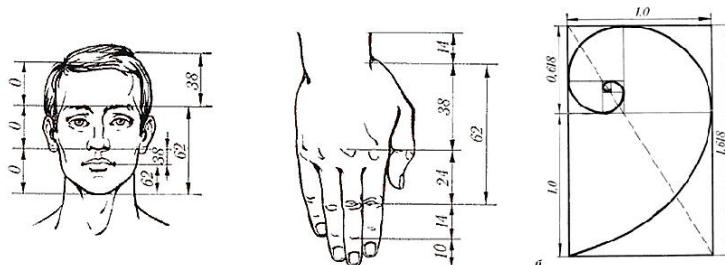
**Задача 247. Свойства чисел Фибоначчи.** Докажите формулы:

- $u_1 + u_2 + \dots + u_n = u_{n+2} - 1;$
- $u_1 + u_3 + \dots + u_{2n-1} = u_{2n};$
- $u_1^2 + u_2^2 + \dots + u_n^2 = u_n u_{n+1}.$

**Задача 248. (\*)** Докажите, что справедлива точная формула вычисления  $n$ -го члена последовательности Фибоначчи:

$$u_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right].$$

Любопытно, что в данной формуле возникает число  $\varphi = \frac{1+\sqrt{5}}{2} \approx 1,618$ . Если в таком отношении разделить отрезок на две части, то длина меньшей части будет относиться к длине большей так же, как длина большей части к длине всего отрезка. Такое отношение  $\varphi$  называется *золотым сечением* или *золотой пропорцией*.

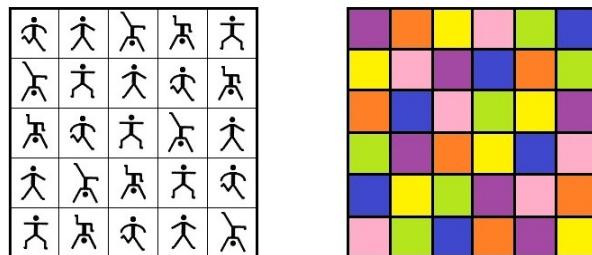


**Задача 249.** Определите, чему равен предел  $\lim_{n \rightarrow \infty} \frac{u_{n+1}}{u_n}$ .

**Задача 250. Золотая пропорция.** Найдите пять примеров золотой пропорции, которые вы наблюдали в жизни.

## 3.4 Латинские квадраты

Пусть у нас есть некоторое число символов. Пронумеруем их все по порядку от 1 до  $n$ . Вопрос: можно ли построить матрицу размера  $n \times n$ , составленную из символов 1, 2, ...,  $n$ , такую, что в каждом столбце и в каждой строке все символы были бы различны? Ответ: можно для любого натурального числа  $n$ . Такая матрица называется *латинским квадратом*. Примеры латинских квадратов  $5 \times 5$  и  $6 \times 6$ :



Аналогично можно определить *латинский куб*, т. е. куб размера  $n \times n \times n$ , заполненный символами от 1 до  $n$  так, что в каждой линии любого из трёх направлений все символы различны.

Пусть  $A = (a_{ij})_{i,j=1}^n$  и  $B = (b_{ij})_{i,j=1}^n$  — два латинских квадрата размера  $n \times n$ , где  $a_{ij}$  и  $b_{ij}$  — элементы, стоящие в строке  $i$  и столбце  $j$  квадратов  $A$  и  $B$  соответственно. Латинские квадраты  $A$  и  $B$  называются *ортогональными*, если различны все упорядоченные пары  $(a_{ij}, b_{ij})$ , где  $i = 1, \dots, n$  и  $j = 1, \dots, n$ .

Пусть  $N(n)$  — множество, состоящее из попарно ортогональных латинских квадратов размера  $n \times n$ . Какова его максимальная мощность при заданном  $n$ ? Ответ: меньше или равна  $n - 1$ . При этом, если достигается равенство, т. е.  $|N(n)| = n - 1$ , то такое множество попарно ортогональных латинских квадратов называется *полным*.

Два латинских квадрата *эквивалентны*, если один можно получить из другого перестановкой столбцов, перестановкой строк и/или перенаименованием элементов.

**Задача 251. Ортогональные латинские квадраты.** Постройте пару ортогональных латинских квадратов размера  $4 \times 4$ .

**Задача 252. Латинские кубы.** Постройте латинские кубы порядков 2, 3 и 4.

**Задача 253. Дважды нормализованные квадраты.** Для заданного  $n$ ,  $2 \leq n \leq 5$ , выполните следующее:

а) постройте все *дважды нормализованные* латинские квадраты размера  $n \times n$ , т. е. такие, что в первой строке и в первом столбцы символы расставлены попорядку от 1 до  $n$ ;

б) определите, сколько среди них неэквивалентных.

**Задача 254. Задача о 36 офицерах.** В 1779 г. Леонард Эйлер поставил следующую задачу. «Для участия в параде каждый из шести полков выделил по шесть офицеров, имеющих шесть различных воинских рангов. Этих офицеров нужно построить в каре так, чтобы ни в одной линии не было повторения ни рангов, ни названий полков.» Вам требуется решить эту задачу для  $n^2$  офицеров, где  $2 \leq n \leq 6$ . Всегда ли это можно сделать при таких  $n$ ?

Например, для  $n = 3$  может получиться результат:

$$\begin{array}{ccc} (1, 1) & (2, 2) & (3, 3) \\ (2, 3) & (3, 1) & (1, 2) \\ (3, 2) & (1, 3) & (2, 1) \end{array},$$

где элементу  $(x, y)$  отвечает офицер ранга  $x$  из полка  $y$ . Напомним, что пара соответствующих квадратов

$$\left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \right), \quad \left( \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array} \right),$$

составленных отдельно из компонент  $x$  и компонент  $y$  образует пару ортогональных латинских квадратов.

Напомним, что если  $A = (a_{ij})_{i,j=1}^n$ , то  $A^T = (a_{ji})_{i,j=1}^n$ .

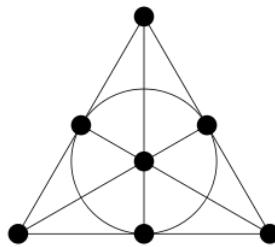
**Задача 255. Самоортогональные квадраты.** Латинский квадрат  $A$  называется *самоортогональным*, если  $A$  и  $A^T$  — ортогональные латинские квадраты. Найдите примеры само-ортогональных квадратов порядка  $n$ , где  $2 \leq n \leq 6$ .

**Задача 256. (\*) Полная система.** Пусть  $n = p^k$ , где  $p$  — простое число. Постройте полную систему ортогональных латинских квадратов при таком  $n$ .

## 3.5 Системы троек Штейнера

Пусть  $n$  — натуральное число. *Системой троек Штейнера* порядка  $n$  называется система трёхэлементных подмножеств  $n$ -элементного множества такая, что каждая неупорядоченная пара элементов встречается ровно в одном подмножестве системы (обозначается  $STS(n)$ ).

**Задача 257. Тройки Штейнера I.** Постройте систему троек Штейнера  $STS(7)$ . Покажите, как можно связать полученную систему со следующим изображением (плоскостью Фано):



**Задача 258. Тройки Штейнера II.** Пусть существует система троек Штейнера порядка  $n$ . Может ли  $n$  быть любым натуральным числом? Если нет, то каким?

**Задача 259. Тройки Штейнера III.** Достройте систему до  $STS(9)$ :  
 $(123), (145), (179), (249), (348), (369), (256), (467), (589), \dots$

# ГЛАВА 4. ЭЛЕМЕНТЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

Результаты алгебры и теории чисел лежат в основе многих криптографических систем с открытым ключом. В данной главе приводится серия избранных задач этой области. Результаты, с которыми мы познакомимся, будут использованы в других главах пособия.

Для основательного знакомства с теоретико-числовыми методами, применяющимися в криптографии, можно рекомендовать книги М. М. Глухова, И. А. Круглова, А. Б. Пичкура и А. В. Черёмушкина [13], Е. Б. Маховенко [21], А. В. Черёмушкина [36] и др.

## 4.1 Целые числа. Алгоритм Евклида

Введём следующие обозначения:

$\mathbb{N}$  — множество натуральных чисел  $\{1, 2, 3, \dots\}$ ;

$\mathbb{Z}$  — множество целых чисел  $\{0, \pm 1, \pm 2, \pm 3, \dots\}$ ;

$a, b, c$  — произвольные целые числа.

Если существует целое число  $q$  такое, что  $a = bq$ , то говорят, что  $b$  делит  $a$ , обозначается  $b|a$ . Наибольшим общим делителем чисел  $a$  и  $b$ , НОД( $a, b$ ), называется наибольшее целое число  $q$  такое, что  $q$  делит и  $a$ , и  $b$ . Наименьшим общим кратным чисел  $a$  и  $b$ , НОК( $a, b$ ), называется наименьшее целое число  $q$  такое, что  $a$  и  $b$  являются делителями  $q$ .

Приведём алгоритм Евклида нахождения НОД целых чисел  $a$  и  $b$ . Пусть  $a \geq b$ . Если  $a$  делится нацело на  $b$ , то  $\text{НОД}(a, b) = b$ . Иначе выполняем следующие шаги:

$$\begin{array}{lll} \text{шаг 1.} & a = bq_1 + r_1, & 0 < r_1 < b, \\ \text{шаг 2.} & b = r_1q_2 + r_2, & 0 < r_2 < r_1, \\ \text{шаг 3.} & r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2, \\ \dots & \dots & \dots \\ \text{шаг } n. & r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ \text{шаг } n+1. & r_{n-1} = r_nq_{n+1}. & \end{array}$$

Проделав все шаги алгоритма Евклида, получаем  $\text{НОД}(a, b) = r_n$ .

**Задача 260.** Пусть  $a, b, c \in \mathbb{Z}$ . Докажите свойства делимости:

- если  $a|b$ ,  $a|c$ , то  $a|(b \pm c)$ ;
- если  $a|b$ , то  $a|bc$  для любого  $c$ ;
- $a|b$ ,  $b|a$  тогда и только тогда, когда  $a = \pm b$ .

**Задача 261.** Пусть  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}$ . Докажите, что для  $a$  и  $b$  всегда существуют единственныe целые числа  $q$  и  $r$  такие, что  $a = bq + r$ ,  $0 \leq r < b$ .

**Задача 262.** Пусть  $n, r, s$  — целые числа такие, что  $n > 1$ ,  $r, s > 0$ . Докажите, что  $n^s - 1$  делит  $n^r - 1$  тогда и только тогда, когда  $s|r$ .

**Задача 263.** Докажите, что для любого натурального числа  $n$  число  $n!$  не делится нацело на  $2^n$ .

**Задача 264.** Пусть  $a, b \in \mathbb{Z}$ . Докажите свойства НОД:

- если  $b|a$ , то  $\text{НОД}(a, b) = b$ ;
- если  $a = bq + r$ , то  $\text{НОД}(a, b) = \text{НОД}(b, r)$ .

**Задача 265. Алгоритм Евклида.** Покажите корректность вычисления НОД двух целых чисел с помощью алгоритма Евклида.

**Задача 266.** С помощью алгоритма Евклида вычислите  $\text{НОД}(a, b)$ :

- |                                |                                 |
|--------------------------------|---------------------------------|
| а) $a = 589$ , $b = 343$ ;     | б) $a = 6188$ , $b = 4709$ ;    |
| в) $a = 12606$ , $b = 6494$ ;  | г) $a = 20989$ , $b = 2573$ ;   |
| д) $a = 135837$ , $b = 9009$ ; | е) $a = 132079$ , $b = 93881$ . |

**Задача 267.** Пусть  $a, b \in \mathbb{Z}$ . Докажите свойства НОК:

- если  $q$  — целое число такое, что  $a|q$  и  $b|q$ , то  $\text{НОК}(a, b)|q$ ;
- $\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a, b)}$ .

**Задача 268. «Хорошие» числа.** Назовём число *хорошим*, если оно делится на квадрат натурального числа большего 1. При каких  $N$  найдётся  $N$  последовательных хороших чисел?

## 4.2 Простые и взаимно простые числа

Целые числа  $a, b$  называются *взаимно простыми*, если  $\text{НОД}(a, b) = 1$ . Натуральное число  $p$ ,  $p > 1$ , называется *простым*, если его натуральными делителями являются только числа 1 и  $p$ ; в противном случае число называется *составным*.

Любое натуральное число  $n$ ,  $n > 1$ , представимо в виде произведения степеней простых чисел:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

где  $p_1, \dots, p_k$  — простые,  $\alpha_1, \dots, \alpha_k$  — целые положительные числа.

Пусть  $n$  — натуральное число. *Функцией Эйлера* числа  $n$  называется функция  $\varphi(n)$ , подсчитывающая количество натуральных чисел, не превышающих  $n$  и взаимно простых с  $n$ .

**Задача 269. Критерий взаимной простоты чисел.** Докажите, что целые числа  $a$  и  $b$  являются взаимно простыми тогда и только тогда, когда найдутся целые числа  $u$  и  $v$  такие, что  $au + bv = 1$ .

**Задача 270.** Докажите свойства взаимно простых чисел:

- а) если  $\text{НОД}(a, b) = 1$  и  $\text{НОД}(a, c) = 1$ , то  $\text{НОД}(a, bc) = 1$ ;
- б) если  $a$  делит  $bc$  и  $\text{НОД}(a, c) = 1$ , то  $a$  делит  $b$ ;
- в) если  $a$  делит  $c$ ,  $b$  делит  $c$ ,  $\text{НОД}(a, b) = 1$ , то  $ab$  делит  $c$ .

**Задача 271.** Определите, являются ли  $a$  и  $b$  взаимно простыми:

- а)  $a = 323$ ,  $b = 136$ ;
- б)  $a = 126$ ,  $b = 247$ ;
- в)  $a = 168$ ,  $b = 667$ .

**Задача 272.** Пусть целые числа  $a$  и  $b$  взаимно простые. Докажите, что  $\text{НОД}(a + b, a - b)$  равен либо 1, либо 2.

**Задача 273. Теорема Евклида.** Докажите, что простых чисел бесконечно много.

**Задача 274.** Докажите, что для любого натурального числа  $k$  найдётся натуральное число  $n$  такое, что числа  $n + 1, n + 2, \dots, n + k$  составные.

**Задача 275.** (\*) **Функция Эйлера.** Докажите следующие утверждения о функции Эйлера.

- Пусть  $p$  — простое число. Тогда  $\varphi(p) = p - 1$ .
- Пусть  $p$  — простое число. Тогда  $\varphi(p^k) = p^k - p^{k-1}$ .
- Пусть  $a, b$  — целые числа такие, что  $\text{НОД}(a, b) = 1$ . Докажите, что функция Эйлера *мультипликативна*, т. е. выполнено:

$$\varphi(ab) = \varphi(a)\varphi(b).$$

г) Пусть  $n$  — натуральное число, разложение которого на простые множители имеет вид  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , где  $p_1, p_2, \dots, p_k$  — простые числа. Докажите, что

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right).$$

**Задача 276.** Вычислите функцию Эйлера для следующих чисел:

- |                 |                 |                  |
|-----------------|-----------------|------------------|
| а) $n = 375$ ;  | б) $n = 720$ ;  | в) $n = 988$ ;   |
| г) $n = 1943$ ; | д) $n = 6369$ ; | е) $n = 33320$ . |

**Задача 277.** Пусть  $a$  — натуральное число, равное произведению двух простых чисел  $p$  и  $q$ , т. е.  $a = pq$ . Найдите число  $a$ , если известно, что  $\varphi(a) = 120$  и  $p - q = 2$ .

**Задача 278.** Пусть  $p$  — простое число. Докажите, что  $(2p - 1)! - p$  делится на  $p^2$ .

**Задача 279.** Пусть  $n > 2$  — натуральное число, и  $a_1, a_2, \dots, a_{\varphi(n)}$  — взаимно простые с  $n$  числа. Найдите формулу для вычисления суммы  $\sum_{i=1}^{\varphi(n)} a_i$  через функцию Эйлера.

### 4.3 Двоичное представление чисел

Любое натуральное число  $m$  может быть представлено в виде

$$m = \sum_{i=0}^{\ell} m_i 2^i,$$

где  $m_i \in \{0, 1\}$  и  $\ell$  — наибольшее подходящее целое число такое, что  $m_\ell = 1$ . Набор  $(m_\ell, \dots, m_0)$  называется *вектором двоичного представления* числа  $t$ . *Двоичным весом* числа  $t$  (обозначается  $wt(t)$ ) называется количество ненулевых коэффициентов среди  $m_0, \dots, m_\ell$ .

*Отношение предшествования* на множестве натуральных чисел определяется следующим образом:  $t \preceq t'$  (число  $t$  *предшествует* числу  $t'$ ), если для всех  $i$  выполнено  $m_i \leq m'_i$ . Если к тому же  $t \neq t'$ , то говорят, что предшествование *строгое* и пишут  $t < t'$ . Если среди двух чисел  $t$  и  $n$  ни одно не предшествует другому, то говорят, что числа  $t$  и  $n$  *не сравнимы*.

**Задача 280.** Найдите двоичные представления следующих чисел:

- а)  $n = 47$ ;      б)  $n = 283$ ;
- в)  $n = 682$ ;      г)  $n = 2063$ ;
- д)  $n = 2^k - 1$ , где  $k$  — произвольное натуральное число.

**Задача 281.** Определите, какие числа из приведённых связаны отношением предшествования, а какие не сравнимы между собой:

- а) 25, 2, 16;      б) 36, 68, 64;      в) 167, 255, 315.

**Задача 282. (\*)** Докажите, что биномиальный коэффициент  $C_n^k$  является нечётным числом только при  $k \preceq n$ .

## 4.4 Сравнение по модулю

Пусть  $a, b$  — целые числа,  $m$  — натуральное. Запись  $a = b \pmod m$  означает, что  $a$  равно остатку от деления  $b$  на  $m$ . Числа  $a$  и  $b$  называются *сравнимыми по модулю*  $m$ , если они имеют одинаковые остатки от деления на число  $m$ , что обозначается как  $a = b \pmod m$ . Сравнение по модулю  $m$  является отношением эквивалентности, поэтому множество всех целых чисел распадается на классы эквивалентности — *классы вычетов по модулю*  $m$ . Каждый класс вычетов по модулю  $m$  с представителем  $a$  состоит из всех целых чисел, сравнимых с  $a$  по модулю  $m$  и обозначается  $\bar{a}$ . Нетрудно понять, что всего имеется ровно  $m$  классов вычетов по модулю  $m$  с представителями  $0, 1, \dots, m-1$  соответственно. *Полной системой вычетов* по некоторому модулю называется система чисел, взятых по одному из каждого класса по этому модулю. *Приведённой системой вычетов* по

некоторому модулю  $m$  называется система чисел, взятых по одному из каждого класса, взаимно простого с модулем. (Говорят, что класс  $\bar{a}$  взаимно прост с модулем  $m$ , если само число  $a$  взаимно просто с  $m$ .)

**Задача 283.** Пусть  $a_1 = b_1 \pmod{m}$ ,  $a_2 = b_2 \pmod{m}$ . Докажите следующие свойства сравнений:

- а)  $a_1 + a_2 = b_1 + b_2 \pmod{m}$ , т. е. сравнения по одному модулю можно почленно складывать;
- б)  $a_1 a_2 = b_1 b_2 \pmod{m}$ , т. е. сравнения по одному модулю можно почленно перемножать.

**Задача 284.** Пусть  $a = b \pmod{m}$ . Докажите следующие свойства сравнений:

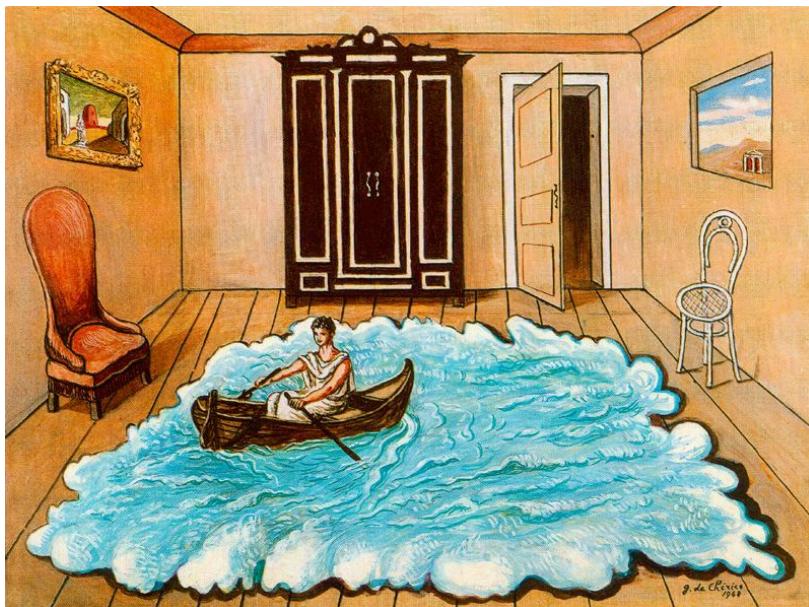
- а) для любого целого  $c$  верно, что  $a + c = b + c \pmod{m}$ , т. е. к обеим частям сравнения можно прибавлять любое целое число;
- б) для любого целого  $c$  верно, что  $ac = bc \pmod{m}$ , т. е. обе части сравнения можно умножать на одно и то же число;
- в) если  $\text{НОД}(a, b) = d$  и  $\text{НОД}(d, m) = 1$ , то  $a/d = b/d \pmod{m}$ ;
- г) если  $d$  — произвольный общий делитель чисел  $a$ ,  $b$  и  $m$ , то  $a/d = b/d \pmod{m/d}$ .

**Задача 285. Система вычетов.** Докажите, что если  $a$  взаимно просто с  $p$ , то числа  $1 \cdot a, \dots, (p - 1) \cdot a$  образуют приведённую систему вычетов по модулю  $p$ .

**Задача 286. Малая теорема Ферма.** Докажите, что если целое число  $a$  не делится на простое число  $p$ , то  $a^{p-1} = 1 \pmod{p}$ .

**Задача 287. Теорема Эйлера.** Докажите, что если целые числа  $a$  и  $m$  взаимно просты, то  $a^{\varphi(m)} = 1 \pmod{m}$ .

**Задача 288. Раскраска вершин.** Пусть  $p > 2$  — простое число. Сколько существует способов раскрасить вершины правильного  $p$ -угольника в  $a$  цветов? (Раскраски, которые можно совместить поворотом, считаются одинаковыми.) Получите формулу и выведите из неё малую теорему Ферма.



Результат следующей задачи имеет непосредственное приложение в криптосистеме RSA, см. подробнее раздел 5.3.

**Задача 289.** Пусть  $p$  и  $q$  — различные простые числа,  $a$  и  $k$  — произвольные целые числа. Докажите, что  $a^{k\varphi(pq)+1} = a \pmod{pq}$ .

**Задача 290. Нечётные делители.** Докажите, что если у числа  $m$  есть два различных нечётных простых делителя, то для числа  $a$  взаимно простого с  $m$  верно, что  $a^{\varphi(m)/2} = 1 \pmod{m}$ .

**Задача 291.** Как при помощи диофантовых уравнений найти число  $A$ , удовлетворяющее системе соотношений  $A = a_1 \pmod{m_1}$ ,  $A = a_2 \pmod{m_2}$  для взаимно простых чисел  $m_1, m_2$ ?

## 4.5 Обратный элемент и возвведение в степень

Обобщением задачи 269 о критерии взаимной простоты чисел является тот факт, что для любых натуральных чисел  $a$  и  $b$  существуют

целые числа  $u$  и  $v$  такие, что

$$au + bv = \text{НОД}(a, b).$$

*Обобщённый алгоритм Евклида* позволяет находить не только  $\text{НОД}(a, b)$ , но и числа  $u$  и  $v$ . Для чего это необходимо? Зачастую, например, в криптографических схемах с открытым ключом, для целого числа  $c$  требуется найти *обратный по модулю  $m$*  элемент — такое число  $d$ ,  $0 < d < m$ , (его обозначают  $c^{-1}$ ), что

$$cd = 1 \pmod{m},$$

при условии, что числа  $c$  и  $m$  взаимно простые.

Таким образом, в данной постановке задачи в качестве чисел  $a$  и  $b$  выступают числа  $m$  и  $c$  соответственно. Требуется найти подходящее число  $v$ , т. е. обратный элемент  $d$ , при условии, что  $\text{НОД}(m, c) = 1$ . Считаем далее, что  $m > c$ .

Опишем обобщённый алгоритм Евклида, адаптированный для нахождения обратного по модулю элемента:

$$\begin{array}{lll} \text{шаг 1.} & m = cq_1 + r_1, & 0 \leq r_1 < c, \\ & d_1 = 0 - q_1, & \\ \text{шаг 2.} & c = r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ & d_2 = 1 - q_2d_1, & \\ \text{шаг 3.} & r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2, \\ & d_3 = d_1 - q_3d_2, & \\ \dots & \dots & \dots \\ \text{шаг } n. & r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1}, \\ & d_n = d_{n-2} - q_nd_{n-1}, & \\ \text{шаг } n+1. & r_{n-1} = r_nq_{n+1}. & \end{array}$$

Проделав все шаги данного алгоритма, получаем, что обратным по модулю  $m$  элементом числа  $c$  является число  $d$ , равное  $d_n$  при  $d_n > 0$  и равное  $d_n + m$  при  $d_n < 0$ .

Очень удобно использовать краткую запись для вычислений алгоритма, предложенную в книге [26]. Запишем две строки 
$$\boxed{\begin{matrix} m & 0 \\ c & 1 \end{matrix}}.$$

Затем вычислим  $q_1$  и отнимем от первой строки вторую, умноженную на  $q_1$ . Результат запишем в третью строку. Далее аналогичные

действия производим со второй и третьей строкой и т. д. до тех пор, пока в очередной строке не получим первый элемент, равный нулю. Тогда второй элемент предпоследней строки будет искомым значением  $c^{-1}$ . Приведём два примера: найдём  $3^{-1} \pmod{5}$  и  $11^{-1} \pmod{53}$ .

|                      |                        |
|----------------------|------------------------|
| 5    0               | 53    0                |
| 3    1               | 11    1                |
| 2    -1 $q_1 = 1$    | 9    -4 $q_1 = 4$      |
| 1 <b>2</b> $q_2 = 1$ | 2    5 $q_2 = 1$       |
| 0    -5 $q_3 = 2$    | 1 <b>-24</b> $q_3 = 4$ |
|                      | 0    53 $q_4 = 2$      |

Таким образом,  $3^{-1} \pmod{5} = 2$ , а  $11^{-1} = -24 \pmod{53}$ , откуда заключаем, что  $11^{-1} \pmod{53} = -24 + 53 = 29$ .

**Задача 292.** С помощью обобщённого алгоритма Евклида найдите:

- а)  $7^{-1} \pmod{11}$ ;    б)  $5^{-1} \pmod{22}$ ;    в)  $17^{-1} \pmod{56}$ ;
- г)  $6^{-1} \pmod{32}$ ;    д)  $12^{-1} \pmod{221}$ ;    е)  $27^{-1} \pmod{611}$ .

**Задача 293.** Докажите корректность нахождения обратного по модулю элемента с помощью обобщённого алгоритма Евклида.

Другой важной задачей является возведение числа  $a$  в степень  $n$  по модулю  $m$ , т. е. нахождение значения  $a^n \pmod{m}$ . Возведение в степень по модулю также часто используется при построении криптографических схем с открытым ключом. Приведём *алгоритм возведения в степень*, позволяющий быстро вычислять  $a^n \pmod{m}$ :

- шаг 1. Найти вектор  $(n_\ell, \dots, n_1, n_0)$  двоичного представления числа  $n$ ;
- шаг 2. Вычислить значения  $a_0 = a \pmod{m}$ ,  $a_1 = a_0^2 \pmod{m}$ ,  
 $a_2 = a_1^2 \pmod{m}$ ,  $\dots$ ,  $a_\ell = a_{\ell-1}^2 \pmod{m}$ ;
- шаг 3. Вычислить значение  $b = a_0^{n_0} a_1^{n_1} \dots a_\ell^{n_\ell} \pmod{m}$ , последовательно выполняя операции умножения по модулю числа  $m$ .

Проделав все шаги данного алгоритма, получим, что искомое значение  $a^n \pmod{m}$  равно  $b$ .

Для примера вычислим  $3^{14} \pmod{5}$ :

- шаг 1.  $n = 14 = (1110)$ ;  
 шаг 2.  $a_0 = 3 \pmod{5}$ ,  $a_1 = 3^2 = 9 = 4 \pmod{5}$ ,  
 $a_2 = 4^2 = 16 = 1 \pmod{5}$ ,  $a_3 = 1^2 = 1 \pmod{5}$ ;  
 шаг 3.  $b = 3^0 \cdot 4^1 \cdot 1^1 \cdot 1^1 = 4 \pmod{5}$ .

Таким образом,  $3^{14} = b = 4 \pmod{5}$ .

**Задача 294.** С помощью алгоритма возвведения в степень найдите значения:

- а)  $5^{120} \pmod{31}$ ;      б)  $3^{84} \pmod{7}$ ;      в)  $7^{-10} \pmod{13}$ ;  
 г)  $19^{-15} \pmod{27}$ ;      д)  $13^{2013} \pmod{20}$ ;      е)  $11^{11111} \pmod{111}$ .

**Задача 295.** Докажите корректность вычислений с помощью алгоритма возвведения в степень.

## 4.6 Решение сравнений первой степени

Сравнением первой степени с одним неизвестным  $x$  называют сравнение

$$ax = b \pmod{m},$$

где  $a$ ,  $b$  — целые числа,  $m$  — натуральное.

**Теорема 1.** Сравнение  $ax = b \pmod{m}$  имеет решение тогда и только тогда, когда число  $b$  делится на  $\text{НОД}(a, m)$ .

**Теорема 2.** Пусть  $\text{НОД}(a, m) = d$  и  $b$  делится на  $d$ . Тогда множество решений сравнения  $ax = b \pmod{m}$  состоит ровно из  $d$  классов вычетов по модулю  $m$ , а именно, если  $x_0$  — решение сравнения, отвечающее некоторому классу вычетов, тогда остальные классы вычетов, являющиеся решениями, задаются числами  $x_0 + m_1, x_0 + 2m_1, \dots, x_0 + (d - 1)m_1$ , где  $m_1 = m/d$ .

Алгоритм решения сравнения  $ax = b \pmod{m}$  при  $\text{НОД}(a, m) = 1$ :

- шаг 1. С помощью обобщённого алгоритма Евклида найти обратный к  $a$  по модулю  $m$  элемент  $c$ , т. е. такой, что  $ac = 1 \pmod{m}$ .  
 шаг 2. Положить  $x$  равным  $cb \pmod{m}$ .

Алгоритм решения сравнения  $ax = b \pmod{m}$  при  $\text{НОД}(a, m) = d$ ,  $d > 1$ :

- шаг 1. Найти числа  $a_1$  и  $m_1$  такие, что  $a = a_1d$  и  $m = m_1d$ .  
Если  $b$  делится на  $d$ , то найти  $b_1 = b/d$  и перейти на шаг 2; иначе сказать, что решений сравнения нет, и выйти из алгоритма.
- шаг 2. С помощью алгоритма выше найти решение  $x_0$  сравнения  $a_1x = b_1 \pmod{m_1}$ .
- шаг 3. По теореме 2 найти оставшиеся  $d-1$  решений искомого сравнения.

Следующая теорема позволяет находить решение системы сравнений первой степени от одного неизвестного.

**Теорема 3. (Китайская теорема об остатках.)** Пусть  $n_1, n_2, \dots, n_s$  — попарно взаимно простые числа. Пусть  $M = n_1n_2\dots n_s$ . Тогда для любых целых чисел  $a_1, a_2, \dots, a_s$  система сравнений

$$\begin{cases} x = a_1 \pmod{n_1}, \\ x = a_2 \pmod{n_2}, \\ \dots \\ x = a_s \pmod{n_s} \end{cases}$$

имеет в интервале  $0 \leq x \leq M - 1$  единственное решение вида

$$x = \sum_{j=1}^s a_j \cdot N_j \cdot M_j \pmod{M},$$

где  $M_j = M/n_j$  и  $N_j = M_j^{-1} \pmod{n_j}$ .

**Задача 296.** Докажите теорему 1 о необходимом и достаточном условии для существования решения сравнения первой степени с одним неизвестным.

**Задача 297.** Докажите теорему 2 о множестве решений сравнения  $ax = b \pmod{m}$ .

**Задача 298.** Проверьте, имеют ли следующие сравнения решения:

- |                              |                                  |
|------------------------------|----------------------------------|
| а) $9x = 2 \pmod{18}$ ;      | б) $22x = 5 \pmod{36}$ ;         |
| в) $460x = 252 \pmod{884}$ ; | г) $1204x = 2782 \pmod{10062}$ . |

**Задача 299.** Найдите решения следующих сравнений:

- |                           |                              |
|---------------------------|------------------------------|
| а) $9x = 6 \pmod{12}$ ;   | б) $11x = 2 \pmod{15}$ ;     |
| в) $12x = 18 \pmod{22}$ ; | г) $22x = 10 \pmod{34}$ ;    |
| д) $12x = 4 \pmod{42}$ ;  | е) $256x = 179 \pmod{337}$ . |

**Задача 300.** Предложите способ решения сравнения  $ax = b \pmod{m}$  на основе теоремы Эйлера (см. задачу 287).

**Задача 301. (\*)** Докажите теорему 3 (китайскую теорему об остатках) о решении системы линейных сравнений от одного неизвестного.

**Задача 302.** С помощью китайской теоремы об остатках найдите решения следующих систем сравнений:

$$\text{а) } \begin{cases} x = 2 \pmod{5}, \\ x = 3 \pmod{6}, \\ x = 4 \pmod{7}. \end{cases} \quad \text{б) } \begin{cases} x = 2 \pmod{5}, \\ x = 3 \pmod{11}, \\ x = 4 \pmod{17}, \end{cases}$$

$$\text{в) } \begin{cases} x = 2 \pmod{3}, \\ x = 3 \pmod{4}, \\ x = 6 \pmod{7}, \\ x = 5 \pmod{11}. \end{cases} \quad \text{г) } \begin{cases} x = 1 \pmod{3}, \\ x = 4 \pmod{5}, \\ x = 2 \pmod{7}, \\ x = 9 \pmod{11}, \\ x = 3 \pmod{13}. \end{cases}$$

## 4.7 Цепные дроби

Цепной дробью  $[a_0, a_1, \dots, a_n, \dots]$  называется формальная сумма

$$a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{a_n + \dots}}},$$

где  $a_0$  — целое число, а все  $a_n$ ,  $n > 0$ , — натуральные числа, причём последнее, если оно существует, не равно 1.

Рациональные числа  $\delta_k = P_k/Q_k = [a_0, a_1, \dots, a_k]$ ,  $k \geq 0$ , называются подходящими дробями к цепной дроби  $[a_0, a_1, \dots, a_n, \dots]$ . Числа

$a_k$ ,  $k \geq 0$ , — неполные частные, а числа  $\alpha_k = [a_k, a_{k+1}, \dots]$ ,  $k \geq 0$ , — полные частные цепной дроби  $[a_0, a_1, \dots, a_n, \dots]$ .

**Задача 303.** Покажите, что верны следующие рекуррентные соотношения для цепной дроби  $[a_0, a_1, \dots, a_n, \dots]$  и её подходящих дробей  $\delta_k$ :

$$P_n = a_n P_{n-1} + P_{n-2}, \quad Q_n = a_n Q_{n-1} + Q_{n-2},$$

где формально определены начальные значения для  $n = -2, -1$ :

$$P_{-2} = 0, \quad P_{-1} = 1, \quad Q_{-2} = 1, \quad Q_{-1} = 0.$$

**Задача 304.** Вычислите значение цепных дробей:

- |                             |                                     |                           |
|-----------------------------|-------------------------------------|---------------------------|
| а) $[20, 1, 4]$ ;           | б) $[0, 8, 1, 6, 2, 2]$ ;           | в) $[1, 2, 3, 4, 5, 6]$   |
| г) $[-2, 3, 3, 10]$ ;       | д) $[1, (2)]$                       | е) $[(1)]$ ;              |
| ж) $[3, (1, 1, 1, 1, 6)]$ ; | з) $[-7, 1, 1, 1, 1, (2, 12, 1)]$ ; | и) $[6, 8, 8, 1, 2, 8]$ . |

**Задача 305.** Найдите представление числа в виде цепной дроби:

- |                             |                                 |                         |                                    |
|-----------------------------|---------------------------------|-------------------------|------------------------------------|
| а) $\frac{49}{9}$ ;         | б) $-\frac{69}{11}$ ;           | в) $\frac{1680}{391}$ ; | г) $\frac{1234}{567}$ ;            |
| д) $\frac{3 - \sqrt{5}}{2}$ | е) $\frac{2 + \sqrt{15}}{11}$ ; | ж) $\sqrt{31}$ ;        | з) $\frac{\sqrt{2210} - 13}{13}$ . |

## 4.8 Проверка простоты числа

В криптографических системах с открытым ключом широко используются простые числа. Поэтому важными задачами для криптографии являются генерация простых чисел и проверка простоты числа. Приведём несколько методов, позволяющих решить данные задачи.

### Решето Эратосфена

С помощью следующего алгоритма можно находить множество  $P_n$ , состоящее из всех простых чисел, не превышающих заданного натурального числа  $n$ :

- шаг 0. Выписать все натуральные числа от 2 до  $n$ . Положить  $p = 2$  и  $P_n = \{2\}$ .
- шаг 1. Вычеркнуть все числа от  $2p$  до  $n$ , которые кратны числу  $p$ .
- шаг 2. Положить  $p$  равным первому незачёркнутому числу, которое больше  $p$ , и добавить его в множество  $P_n$ .
- шаг 3. Если  $p^2 \leq n$ , то на переходим шаг 1, иначе — на шаг 4.
- шаг 4. Добавить в множество  $P_n$  все оставшиеся числа.

## Критерий Вильсона

Данный критерий формулирует необходимое и достаточное условие простоты числа.

**Теорема 4.** *Натуральное число  $n$  простое тогда и только тогда, когда  $(n - 1)! \equiv (-1) \pmod{n}$ .*

## Тест на основе малой теоремы Ферма

Данный критерий формулирует только необходимое условие простоты числа.

**Теорема 5.** *Если натуральное число  $n$  простое, тогда для любого числа  $a$ ,  $2 \leq a \leq n - 1$ , выполнено сравнение  $a^{n-1} \equiv 1 \pmod{n}$ .*

Тестирование заключается в проверке сравнения при случайному выборе числа  $a$ . Если сравнение не выполнено хотя бы для одного числа  $a$ , то число  $n$  составное.

Натуральное число  $n$  называется *псевдопростым по основанию  $a$* ,  $2 \leq a \leq n - 1$ ,  $\text{НОД}(a, n) = 1$ , если  $a^{n-1} \equiv 1 \pmod{n}$ . Если последнее сравнение выполнено для всех таких  $a$ , то  $n$  называется *псевдопростым*, или *числом Кармайкла*.

## Критерий Лукаса

Данный критерий формулирует необходимое и достаточное условие простоты числа.

**Теорема 6.** Натуральное число  $n$  простое тогда и только тогда, когда существует число  $a$  взаимно простое с  $n$  такое, что:

- (i)  $a^{n-1} \equiv 1 \pmod{n}$ ;
- (ii) для любого простого делителя  $p$  числа  $n - 1$  выполняется условие  $a^{\frac{n-1}{p}} \equiv 1 \pmod{n}$ .

**Задача 306. (\*) Критерий Вильсона.** Докажите справедливость теоремы 4 о критерии простоты числа.

**Задача 307.** Докажите справедливость теоремы 5 о необходимом условии простоты числа.

**Задача 308. Псевдопростые числа I.** Найдите все основания  $a$ , по которым число  $n$  является псевдопростым, если

- а)  $n = 15$ ;
- б)  $n = 21$ ;
- в)  $n = 527$ ;
- г)  $n = 629$ .

**Задача 309. Псевдопростые числа II.** Докажите, что если число  $n$  псевдопростое по основанию 2, то число  $2^n - 1$  также псевдопростое по основанию 2.

**Задача 310. (\*\* Числа Кармайкла (Критерий Корселта).** Докажите, что нечётное составное число  $n$  является числом Кармайкла тогда и только тогда, когда

- 1)  $n$  свободно от квадратов (т. е. оно не делится на квадрат никакого числа, кроме единицы);
- 2) если  $p$  — простой делитель  $n$ , то  $n - 1$  делится на  $p - 1$ .

**Задача 311. Числа Кармайкла.** Выполните следующее:

- а) найдите все числа Кармайкла меньше 10 000;
- б) докажите, что числа  $(12k + 5)(36k + 13)(48k + 17)$  и  $(30k + 7)(60k + 13)(150k + 31)$  являются числами Кармайкла, если все числа в скобках — простые числа.

**Задача 312. (\*) Критерий Лукаса.** Докажите справедливость теоремы 6 о критерии простоты числа.

**Задача 313. Проверка простоты числа.** Применяя любой из методов проверки простоты, определите, являются ли числа простыми:

- |                    |   |
|--------------------|---|
| а) 7 079;          | б) 12 827;                              |
| в) 50 819;         | г) 50 821;                              |
| д) 162 401;        | е) 252 601;                             |
| ж) 2 148 667 267;  | з) 1 111 111 111 111 111 111;           |
| и) 34 454 482 009; | к) 618 970 019 642 690 137 449 562 111. |

## 4.9 Поле Галуа

Основными объектами исследования алгебры являются алгебраические системы. Опишем две из них, которые будут необходимы нам для изучения криптографических основ.

**Определение 1.** *Группой* называется алгебраическая система  $(G, \cdot)$ , где  $G$  — некоторое множество с бинарной операцией  $\cdot$ , для которой выполнены следующие условия:

- 1) ассоциативность, т. е. для любых элементов  $a, b, c \in G$  верно:  
 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;
- 2) в  $G$  существует единичный элемент 1 такой, что для любого элемента  $a \in G$  выполнено:  $1 \cdot a = a \cdot 1$ ;
- 3) для любого  $a \in G$  существует обратный элемент  $a^{-1} \in G$  такой, что выполнено:  $a \cdot a^{-1} = a^{-1} \cdot a = 1$ .

Если к тому же в группе  $(G, \cdot)$  выполнен закон коммутативности, т. е. для любых  $a, b \in G$  верно, что  $a \cdot b = b \cdot a$ , то группа называется *абелевой* (*коммутативной*).

Группа  $(G, \cdot)$  называется *циклической*, если в множестве  $G$  существует элемент  $\alpha$  такой, что для любого элемента  $b \in G$  существует целое число  $k$ , что  $b = \underbrace{\alpha \cdot \dots \cdot \alpha}_{k \text{ раз}} = \alpha^k$ .

**Определение 2.** *Полем* называется алгебраическая система  $(F, +, \cdot)$ , где  $F$  — множество с двумя бинарными операциями  $+$  и  $\cdot$ , для которых выполнены следующие условия:

- 1) алгебраическая система  $(F, +)$  — абелева группа, т. е. для любых  $a, b, c \in F$  верно:  $a + (b + c) = (a + b) + c$ ;  $a + b = b + a$ ; существует элемент 0 такой, что  $a + 0 = 0 + a = a$ ; для любого  $a \in F$  существует  $-a$  такой, что  $a + (-a) = 0$ ;

2) алгебраическая система  $(F \setminus \{0\}, \cdot)$  — абелева группа, т. е. для любых  $a, b, c \in F$  верно:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;  $a \cdot b = b \cdot a$ ; существует элемент 1 такой, что  $a \cdot 1 = 1 \cdot a = a$ ; для любого  $a \in F \setminus \{0\}$  существует  $a^{-1}$  такой, что  $a \cdot a^{-1} = 1$ ;

3) выполнен закон дистрибутивности: для любых  $a, b, c \in F$  верно, что  $a \cdot (b + c) = a \cdot b + a \cdot c$ .

Для краткости записи вместо  $a \cdot b$  будем писать  $ab$ .

**Задача 314.** Докажите, что  $(ab)^{-1} = b^{-1}a^{-1}$  для любых элементов группы  $a, b$ .

**Задача 315.** Докажите, что в поле  $(F, +, \cdot)$  выполнено равенство  $a \cdot 0 = 0 \cdot a = 0$  для любого  $a \in F$ .

**Задача 316.** Докажите, что в поле  $(F, +, \cdot)$  нет делителей нуля, т. е. из равенства  $a \cdot b = 0$  следует, что  $a = 0$  или  $b = 0$ , где  $a, b \in F$ .

**Задача 317.** Проверьте, являются ли полями следующие системы:

- а) множество натуральных чисел с обычными операциями сложения и умножения;
- б) множество целых чисел с обычными операциями сложения и умножения;
- в) множество рациональных чисел с обычными операциями сложения и умножения.

Поле  $(F, +, \cdot)$  называется *конечным*, если множество  $F$  конечное. Через  $GF(q)$  обозначим конечное поле из  $q$  элементов (*поле Галуа*).

Основные теоремы о поле Галуа:

1. Конечное поле  $GF(q)$  существует тогда и только тогда, когда  $q = p^n$ , где  $p$  — простое число,  $n$  — натуральное число. Число  $p$  называется *характеристикой* поля и является наименьшим натуральным числом таким, что  $\underbrace{1 + \dots + 1}_{p \text{ раз}} = 0$ .
2. Поле  $GF(q)$  единственno с точностью до изоморфизма.
3. Любой элемент  $a \in GF(q)$  удовлетворяет равенству:  $a^q = a$ .

4. Множество  $GF^*(q) = GF(q) \setminus \{0\}$  образует циклическую мультипликативную группу порядка  $q-1$ , т. е. существует  $\alpha \in GF^*(q)$  такой, что  $GF^*(q) = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ , при этом  $\alpha^{q-1} = 1$ . Такой элемент  $\alpha$  называется *примитивным* элементом поля.
5. Множество автоморфизмов поля  $GF(p^n)$  над  $GF(p)$  образует циклическую группу порядка  $n$ , порождающим элементом которой является автоморфизм  $\phi : a \rightarrow a^p$ .

*Автоморфизмом* поля  $GF(p^n)$  над  $GF(p)$  называется взаимно-однозначное отображение  $\phi$  поля в себя, удовлетворяющее условиям:

- $\phi$  сохраняет операции в поле, т. е. для любых  $a, b \in GF(p^n)$  верно:  $\phi(a + b) = \phi(a) + \phi(b)$  и  $\phi(ab) = \phi(a)\phi(b)$ ;
- $\phi$  оставляет неподвижными элементы из  $GF(p)$ .

Для простоты и наглядности, а также в связи с широким применением в криптографии, далее рассматриваем конечное поле  $GF(2^n)$ .

Конструктивное описание поля  $GF(2^n)$ :

1. Каждый элемент  $c \in GF(2^n)$  представляем в виде многочлена от формального символа  $x$  степени  $n-1$  с коэффициентами из  $GF(2) = \{0, 1\} = \mathbb{Z}_2$ :

$$c(x) = c_1x^{n-1} + c_2x^{n-2} + \dots + c_{n-1}x + c_n, \text{ где } (c_1, \dots, c_n) \in \mathbb{Z}_2^n.$$

2. Операции  $+$  и  $\cdot$  определяются следующим образом:

$$\begin{aligned} c + c' &= d, & d(x) &= c(x) + c'(x), \\ c \cdot c' &= d, & d(x) &= c(x) \cdot c'(x) \bmod g(x), \end{aligned}$$

где под сложением многочленов понимаем их сложение над полем  $GF(2)$ , а  $g(x)$  — произвольный фиксированный *неприводимый* над  $GF(2)$  многочлен степени  $n$ , т. е. такой, что он не раскладывается на множители над полем  $GF(2)$ .

Используя следующий факт можно находить неприводимые над  $GF(2)$  многочлены: многочлен  $x^{2^n} + x$  равен произведению всех неприводимых над  $GF(2)$  многочленов, степени которых являются делителями числа  $n$ .

В конечном поле  $GF(2^n)$  функция *след*  $tr : GF(2^n) \rightarrow GF(2^n)$  определяется следующим образом:

$$tr(c) = c + c^2 + c^{2^2} + \dots + c^{2^{n-1}}, \text{ где } c \in GF(2^n).$$

**Задача 318.** Определите, являются ли неприводимыми над  $GF(2)$  следующие многочлены:

- |                            |                            |
|----------------------------|----------------------------|
| а) $f(x) = x^2 + 1;$       | б) $f(x) = x^2 + x + 1;$   |
| в) $f(x) = x^3 + 1;$       | г) $f(x) = x^3 + x^2 + 1;$ |
| д) $f(x) = x^4 + x^3 + 1;$ | е) $f(x) = x^5 + x^4 + 1;$ |

**Задача 319.** Постройте поле  $GF(2^n)$  с помощью неприводимого многочлена  $g(x)$ :

- |                                 |
|---------------------------------|
| а) $n = 3, g(x) = x^3 + x + 1;$ |
| б) $n = 4, g(x) = x^4 + x + 1.$ |

**Задача 320.** Найдите все неприводимые над  $GF(2)$  многочлены степени  $n = 2, 3, 4, 5$ .

**Задача 321.** Покажите, что для любых  $a, b \in GF(2^n)$  и любого натурального  $k$  выполняется равенство  $(a + b)^{2^k} = a^{2^k} + b^{2^k}$ .

**Задача 322.** Пусть  $a_j$  — произвольные (не обязательно различные, но не все одновременно равные нулю) элементы поля  $GF(q)$ , где  $j = 0, \dots, q - 1$ . Докажите, что найдётся элемент  $\beta \in GF(q)$  такой, что  $a_0\beta^0 + a_1\beta^1 + a_2\beta^2 + \dots + a_{q-1}\beta^{q-1} \neq 0$ .

**Задача 323. (\*) Примитивные элементы.** Определите число примитивных элементов поля  $GF(p^n)$ .

**Задача 324.** Докажите, что функция  $tr(c)$  принимает значения только из множества  $GF(2)$ .

**Задача 325. Линейность следа.** Докажите, что функция  $tr(c)$  линейна, т. е. для любых  $c', c''$  выполняется  $tr(c' + c'') = tr(c') + tr(c'')$ .

**Задача 326.** Докажите, что  $(\text{tr}(c))^2 = \text{tr}(c^2) = \text{tr}(c)$  для любого элемента  $c \in GF(2^n)$ .

**Задача 327. (\*)** Покажите, что существует  $c$  такой, что  $\text{tr}(c) = 1$ .

**Задача 328.** Покажите, что функция  $\text{tr}(c)$  принимает значения 0 и 1 одинаково часто.

**Задача 329. (\*) Сумма отображений.** Пусть  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  — произвольное взаимно однозначное отображение. Покажите, что его можно представить в виде суммы двух взаимно однозначных отображений  $G, H : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ , т. е. так, чтобы для всех  $x \in \mathbb{Z}_2^n$  выполнялось  $F(x) = G(x) \oplus H(x)$ , где  $\oplus$  обозначает побитовое сложение векторов.

**Задача 330. (\*)** Пусть  $a_1, \dots, a_m$  — произвольные ненулевые попарно различные элементы поля  $GF(2^n)$ ,  $\ell$  — целое число такое, что  $0 < \ell \leq m$  и  $r_1, \dots, r_\ell$  — целые числа. Рассмотрим следующую сумму:

$$A = \sum_{1 \leq i \leq m} a_i^{2^{r_1} + \dots + 2^{r_\ell}} + \sum_{1 \leq i < j \leq m} (a_i + a_j)^{2^{r_1} + \dots + 2^{r_\ell}} + \dots + (a_1 + \dots + a_m)^{2^{r_1} + \dots + 2^{r_\ell}}.$$

Докажите, что

- а) при  $\ell < m$  сумма  $A$  тождественно равна нулю;
- б) при  $\ell = m$  сумма  $A$  равна следующему выражению:

$$A = \sum_{\pi \in S_m} a_1^{2^{r_{1\pi}}} a_2^{2^{r_{2\pi}}} \dots a_m^{2^{r_{m\pi}}},$$

где  $\pi$  — элемент из группы перестановок  $S_m$ .

**Задача 331. (\*)** Докажите, что для произвольных элементов  $a_1, \dots, a_m$  поля  $GF(2^n)$  справедливо следующее равенство:

$$\sum_{\pi \in S_m} a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \dots a_m^{2^{m-m\pi}} = (a_1 + \dots + a_m) \prod_{1 \leq i_1 < \dots < i_{m-1} \leq m} (a_{i_1} + \dots + a_{i_{m-1}}) \dots \prod_{1 \leq i_1 < i_2 \leq m} (a_{i_1} + a_{i_2}) \prod_{1 \leq i \leq m} a_i.$$

# ГЛАВА 5. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

В данной главе мы рассмотрим основные криптосистемы с открытым ключом и решим ряд задач по их применению.



По сложившейся традиции будем называть абонентов, желающих обменяться секретными сообщениями, Алисой и Бобом, а злоумышленника — Евой. Приведём ряд криптосистем, которые позволяют передавать секретные сообщения по открытому каналу связи. Ева может легко перехватывать отправляемые сообщения, но при этом она не может их дешифровать без знания секретных ключей Алисы и Боба. Напомним, что в таких асимметричных системах у каждого абонента есть два ключа — открытый и секретный, первый из которых известен любому другому абоненту, а второй каждым абонентом хранится в секрете.

Основательно познакомиться с методами криптографии с открытым ключом (и не только) можно, прочитав книги Б. Я. Рябко и А. Н. Фионова [26], В. В. Ященко [39], Ю. С. Харина, В. И. Берника, Г. В. Матвеева, С. В. Агиевича [35], В. Мао [20] и др.

## 5.1 Протокол Диффи — Хеллмана

Протокол Диффи — Хеллмана стал первым алгоритмом, позволяющим по открытому каналу связи устанавливать двум абонентам

общий секретное число — некий ключ  $K$ . Далее они могут использовать ключ  $K$ , например, для дальнейшего обмена сообщения с помощью симметричной криптосистемы.

Группа абонентов открыто договаривается о большом простом числе  $p$  и числе  $1 < g < p - 1$ . Далее каждый абонент выбирает свой секретный ключ  $c$  и формирует открытый ключ  $d = g^c \bmod p$ .

|              | <b>Секретный ключ</b>           | <b>Открытый ключ</b>                                       |
|--------------|---------------------------------|--|
| <b>Алиса</b> | число $c_A$ , $1 < c_A < p - 1$ | числа $p$ и $g$ , а также число<br>$d_A = g^{c_A} \bmod p$ |
| <b>Боб</b>   | число $c_B$ , $1 < c_B < p - 1$ | числа $p$ и $g$ , а также число<br>$d_B = g^{c_B} \bmod p$ |

Протокол формирования общего ключа:

Шаг 3. Алиса, используя открытый ключ Боба, вычисляет  $K_{AB} = d_B^{c_A} \bmod p$ .

Шаг 4. Боб, используя открытый ключ Алисы, вычисляет  $K_{BA} = d_A^{c_B} \bmod p$ .

В результате работы протокола Диффи — Хеллмана Алиса и Боб получают общий секретный ключ  $K = K_{AB} = K_{BA}$ .

**Задача 332. Протокол Диффи — Хеллмана.** Докажите, что в результате работы протокола Алиса и Боб действительно устанавливают общий ключ, т. е. в обозначениях алгоритма  $K_{AB} = K_{BA}$ .

**Задача 333. Подруги.** Подруги Маша, Даша и Саша используют протокол Диффи — Хеллмана для формирования секретных ключей, с помощью которых далее они ведут переписку. В качестве параметров протокола они выбрали  $p = 23$  и  $g = 2$ , а в качестве своих секретных ключей —  $c_М = 5$ ,  $c_Д = 17$ ,  $c_С = 12$ . Определите открытые ключи каждой из подруг и определите общие секретные ключи пары —  $K_{МД}$ ,  $K_{МС}$ ,  $K_{ДС}$ .

**Задача 334. Миелофон.** Школьник Коля из XX века пытается сообщить Алисе место нахождения миелофона так, чтобы об этом не узнали космические пираты. Для этого он с помощью протокола Диффи — Хеллмана с параметрами  $p = 61$  и  $g = 3$  устанавливает

секретный ключ  $K$  с Алисой. Затем ключ  $K$  переводит в двоичную строку длины 6 и, дублируя её необходимое число раз, складывает побитово с сообщением. Сообщение представлено в виде двоичной строки: каждая буква русского сообщения («е» и «ё» отождествлены) кодируется двоичной строкой длины 5 соответствующей порядковому номеру буквы в алфавите (от 0 до 31).

- Помогите Алисе расшифровать сообщение УЭЙДГЙ, поступившее от Коли, если секретный ключ Алисы  $c_A = 37$ , а открытый ключ Коли  $d_K = 41$ .
- Как бы вы поступили на месте пиратов, зная алгоритм передачи сообщения?

## 5.2 Криптосистема Шамира

Пусть Алиса желает передать Бобу секретное сообщение  $m$ , где  $m$  — натуральное число. Для этого она выбирает достаточно большое случайное простое число  $p$ ,  $p > m$ , и открыто передает его Бобу. В качестве своего секретного ключа Алиса выбирает два числа  $c_A$  и  $d_A$  такие, что  $c_A d_A = 1 \pmod{p-1}$ .

Аналогичные действия проделывает Боб.

|              | Открытый ключ     | Секретный ключ  |
|--------------|-------------------|---|
| <b>Алиса</b> | простое число $p$ | числа $c_A$ и $d_A$ такие, что $c_A d_A = 1 \pmod{p-1}$ |
| <b>Боб</b>   | простое число $p$ | числа $c_B$ и $d_B$ такие, что $c_B d_B = 1 \pmod{p-1}$ |

Алгоритм передачи сообщения  $m$  от Алисы к Бобу:

Шаг 1. Алиса вычисляет  $x_1 = m^{c_A} \pmod{p}$  и отправляет его Бобу.

Шаг 2. Боб, получив число  $x_1$ , вычисляет число  $x_2 = x_1^{c_B} \pmod{p}$  и отправляет его Алисе.

Шаг 3. Алиса вычисляет  $x_3 = x_2^{d_A} \pmod{p}$  и отправляет его Бобу.

Шаг 4. Боб вычисляет число  $x_4 = x_3^{d_B} \pmod{p}$ .

В результате передачи сообщений  $x_1, x_2, x_3$  между Алисой и Бобом на последнем шаге Боб вычисляет сообщение  $x_4$ , которое и равно исходному секретному сообщению  $m$ .

**Задача 335. Крипtosистема Шамира.** Докажите, что в результате работы алгоритма Боб действительно получает от Алисы секретное сообщение  $m$ , т. е. в обозначениях алгоритма  $x_4 = m$ .

**Задача 336.** Для обмена сообщениями Алиса и Боб используют крипtosистему Шамира. В качестве открытого ключа ими выбрано число  $p = 23$ . В качестве своих секретных ключей они выбрали  $c_A = 7$ ,  $c_B = 5$ .

- а) Определите полностью секретные ключи Алисы и Боба.
- б) Алиса отправила Бобу сообщение  $m$ . Первое, что получил Боб, было 14. Обмениваясь дальше по алгоритму крипtosистемы, помогите Бобу определить секретное сообщение.

**Задача 337. Злоумышленник.** Абоненты сети для тайной переписки используют крипtosистему Шамира. Злоумышленник перехватил три подряд идущих сообщения между двумя абонентами: 2, 9, 15. Сможет ли злоумышленник узнать содержание секретного сообщения  $m$ , если известен открытый ключ  $p = 17$ ? Если да, найдите его.

**Задача 338. Пароль.** Алиса хочет сообщить Бобу пароль из букв русского алфавита (буквы «е» и «ё» отождествлены) для входа в секретный дом. Для этого они используют следующий алгоритм. Каждая буква сообщения кодируется двоичным вектором длины 5, который соответствует порядковому номеру буквы в алфавите (от 0 до 31). Далее двоичные вектора записываются последовательно друг за другом. Полученная длинная двоичная строка преобразуется в соответствующее ей десятичное число. Затем десятичное число разбивается слева направо на двузначные числа (последнее может состоять из одной цифры), каждое из которых далее последовательно передаётся с помощью крипtosистемы Шамира. Например, «КОТ» преобразуется так:

$$\text{КОТ} \rightarrow (01010 \ 01110 \ 10010) \rightarrow 10706 \rightarrow 10, 70, 6.$$

Определите пароль, переданный Алисой Бобу, если известно, что они используют открытый ключ  $p = 101$  и секретные ключи  $c_A = 11$ ,  $c_B = 13$ , и в каждом из пяти сеансов обмена сообщениями первыми Боб получил следующие: 29, 50, 81, 42, 28.



**Задача 339. Догадка Боба.** Прочитав книгу по асимметричной криптографии — в частности главу о крипtosистеме Шамира, — Боб воскликнул: «Эврика! Ведь и у меня была подобная идея о том, как обмениваться секретной информацией без передачи ключа!» Боб вспомнил, как ещё в школьные годы он передавал Алисе записки оригинальным способом: он прятал записку в маленькую шкатулку, затем навешивал на неё замок и закрывал на ключ, который хранил у себя в кармане. Закрытую шкатулку Боб передавал через ребят Алисе — при этом шкатулка всегда проходила через руки любопытной Евы. Алиса, получив шкатулку, навешивала рядом с замком Боба свой замок, ключ от которого тоже держала в потайном кармане. После этого шкатулка отправлялась в обратное путешествие к Бобу. Как вы уже, наверное, догадались, Боб снимал свой замок и вновь отправлял шкатулку Алисе. Алиса, получив шкатулку, снимала свой замок и читала записку. И как ни крутила Ева трижды проходившую через её руки шкатулку, заглянуть внутрь ей не удавалось.

А новая идея Боба заключалась вот в чём. Что если вместо «навешивания замка» просто зашифровать сообщение с помощью какого-либо симметричного шифра, а ключ при этом не сообщать никому? Результат передать через Интернет Алисе, которая «добавит» своё шифрование, после чего Боб «снимет» свой шифр, и Алиса сможет расшифровать сообщение. Проблема только в том, чтобы шифрования «коммутировали».

И тут Боб вспомнил об одноразовом блокноте.

Пусть  $x$  — секретное сообщение (двоичный вектор длины  $n$ ), которое нужно передать Алисе от Боба. Пусть  $k_A$  и  $k_B$  — секретные ключи Алисы и Боба соответственно (двоичные векторы длины  $n$ ). Шифрование состоит в сложении сообщения с ключом по модулю 2. Опишите протокол взаимодействия Алисы и Боба, основанный на приведённых выше идеях.

Удастся ли теперь Алисе и Бобу сохранить секрет? Подумайте также о применении в данном методе других симметричных шифров.

### 5.3 Криптосистема RSA

Каждый абонент системы (например, Боб) выбирает два секретных больших простых числа  $p_B$  и  $q_B$  и публикует в качестве своего открытого ключа их произведение  $n_B = p_B q_B$ . Затем Боб выбирает два числа  $e_B$  и  $d_B$  такие, что  $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ , где  $\varphi$  — функция Эйлера.

Напомним, что *функция Эйлера*  $\varphi(n)$  числа  $n$  равна количеству натуральных чисел, не превышающих  $n$  и взаимно простых с ним. В случае  $n = pq$ , где  $p, q$  — простые, справедливо  $\varphi(n) = (p-1)(q-1)$ .

|       | Секретный ключ  | Открытый ключ |
|-------|-----------------|---------------|
| Алиса | $p_A, q_A, d_A$ | $n_A$ и $e_A$ |
| Боб   | $p_B, q_B, d_B$ | $n_B$ и $e_B$ |

Пусть Алиса хочет передать Бобу секретное сообщение  $m$ . При этом должно быть выполнено условие  $m < n_B$ .

Алгоритм передачи сообщения  $m$  от Алисы к Бобу:

Шаг 1. Алиса, используя открытый ключ Боба, вычисляет число  $c = m^{e_B} \pmod{n_B}$  и отправляет его Бобу.

Шаг 2. Боб, получив  $c$ , вычисляет число  $m' = c^{d_B} \pmod{n_B}$ .

В результате работы алгоритма Боб вычисляет сообщение  $m'$ , которое и является исходным сообщением, т. е.  $m' = m$ .

**Задача 340. Криптосистема RSA.** Докажите, что в результате работы алгоритма Боб действительно получает от Алисы секретное сообщение  $m$ , т. е. в обозначениях алгоритма  $m' = m$ .

**Задача 341.** Алиса и Боб используют криптосистему RSA. Пусть Боб выбрал числа  $p = 11$ ,  $q = 13$ ,  $e = 7$ . Определите его секретный и открытый ключи и расшифруйте поступившее ему от Алисы сообщение  $c = 103$ .

**Задача 342.** При шифровании каждая буква сообщения заменяется на двухразрядное число от 01 до 33 соответственно позициям в алфавите. Пусть пробелу соответствует 00. Шифрование происходит блоками, в каждом из которых по 4 цифры. Если зашифрованный блок меньше 1000 дописываем в начало нули до тех пор, пока его длина не станет равна 4. Вам пришло секретное сообщение:

2303 1071 0080 1032 1103 1883 2750

Расшифруйте сообщение, если ваши параметры  $p = 47$ ,  $q = 59$ ,  $d = 157$ ,  $e = 17$ .

**Задача 343. Спецагенты.** Спецагенты Джеймс и Рассел ведут переписку на русском языке, используя криптосистему RSA. Буквам алфавита перед шифрованием ставится в соответствие их порядковый номер от 1 до 33. Рассел должен в ближайшие дни передать Джеймсу украденный конверт с ценностями историческими письмами. Агенты договорились о встрече, но произошел сбой системы, и часть сообщения осталась незашифрованной. Разведчик Стив знает открытый ключ Рассела  $(33, 3)$  и перехватил следующее послание от Джеймса: «Цицеронъ-парк, скамейка у пруда, в йгсзгое». Во сколько и куда должен прийти Стив, чтобы помешать передаче?

**Задача 344. Двоичный канал связи.** В двоичном канале связи Евой были перехвачены два сообщения  $C_1 = (10000)$  и  $C_2 = (100100111)$ , отправленные от Алисы к Бобу. Известно, что было зашифровано сообщение, состоящее из трёх букв русского алфавита, в котором буквы «е» и «ё» отождествлены. Для представления сообщения в бинарном виде используются двоичные векторы длины 5, соответствующие порядковому номеру буквы (от 0 до 31). Итоговая двоичная строка была разбита на две части и каждая часть зашифрована с помощью криптосистемы RSA. Определите секретное сообщение, если открытый ключ Боба:  $e = 7$ ,  $n = 299$ .

**Задача 345. Секретный дом.** Вы решили воспользоваться криптосистемой RSA. Для этого выбрали простые числа  $p = 11$ ,  $q = 17$  и экспоненту  $e = 13$ .

- а) Определите свой секретный и открытый ключи.
- б) После публикации своего открытого ключа в сети, Вы получили сообщение от некого пользователя, который договаривается с Вами о встрече на улице N\* в доме номер 53. Расшифруйте настоящий номер дома.
- в) В каких реальных системах защиты информации используется система RSA? Опишите (кратко) её основные преимущества и недостатки.

## 5.4 Криптосистема Гольдвассер — Микали

В 1983 г. американские криптографы Ш. Гольдвассер и С. Микали выявили несколько недостатков криптосистем с открытым ключом и постарались их исправить.

Напомним основные идеи асимметричной криптографии.

Пусть  $f$  — односторонняя функция с «лазейкой»  $s$ . А именно,  $f$  — это эффективно вычислимая функция, для обращения которой не существует эффективного алгоритма. Однако если известно значение «лазейки»  $s$ , обращение функции  $f$  можно произвести эффективно. Алгоритм вычисления функции  $f$  объявляется абонентом А *открытым ключом* и делается общедоступным. «Лазейку»  $s$  абонент А называет своим *секретным ключом* и хранит в тайне. Любой другой абонент, скажем В, используя открытый ключ, может зашифровать секретное сообщение  $m$  для абонента А. Для этого он вычисляет значение  $f(m)$ , которое и передает абоненту А по открытому каналу связи. Злоумышленник, перехватив значение  $f(m)$ , не может восстановить сообщение  $m$ , так как задача обращения функции  $f$  «очень трудна». Только абонент А может справиться с задачей обращения, так как ему известна «лазейка»  $s$ . Вычисляя  $f^{-1}(m, s)$ , он «легко» восстанавливает сообщение  $m$ .

Ш. Гольдвассер и С. Микали отметили следующие недостатки такого подхода:

- 1) не исключена возможность того, что  $m$  может быть вычислена по  $f(m)$  при *некоторых* специальных  $m$ ;
- 2) не исключена возможность простого вычисления некоторой *частичной* информации об  $m$  по  $f(m)$ .

Криптографы предложили заменить одностороннюю функцию на неприближаемый односторонний предикат.

Функция  $B$ , определённая на некотором множестве  $M$  и принимающая значения из множества  $\{0, 1\}$  называется *предикатом*. Предикат  $B$  называется *неприближаемым односторонним*, если

- 1) «легко» можно выбрать  $x \in M$  так, что  $B(x) = 0$ ;
- 2) «легко» можно выбрать  $y \in M$  так, что  $B(y) = 1$ ;
- 3) для данного  $z \in M$  вычислить значение  $B(z)$  можно только при знании «лазейки»  $s$ .

Без знания «лазейки» полиномиально ограниченный злоумышленник не может вычислить значение  $B(z)$  способом лучшим, чем угадывание.

Следующей идеей Ш. Гольдвассер и С. Микали была идея о том, что процедуру зашифрования следует сделать неоднозначной.

Будем рассматривать побитовое шифрование. Пусть бит 0 имеет много различных зашифрований. Другими словами, существует много шифртекстов, отвечающих открытому тексту 0. Аналогично, пусть бит 1 можно зашифровать многими различными способами. Конкретно эту идею можно реализовать с помощью предиката  $B$ : пусть 0 зашифровывается произвольным  $x$  таким, что  $B(x) = 0$ ; значение 1 будет зашифровано произвольным  $y$  таким, что  $B(y) = 1$ .

### **Модель Ш. Гольдвассер, С. Микали (1983 г.)**

Выберем следующий предикат, определённый на множестве  $\mathbb{Z}_n$ , в качестве одностороннего:

$$Q_n(a) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } n; \\ 0, & \text{если } a \text{ — квадратичный невычет по модулю } n. \end{cases}$$

Напомним, что  $a$  — *квадратичный вычет* по модулю  $n$ , если сравнение  $x^2 = a \pmod{n}$  имеет решение. Иначе  $a$  называется *квадратичным невычетом*.

Пусть Алиса

- 1) выбирает случайные  $k$ -битные простые числа  $p, q$ ;
- 2) вычисляет  $n = pq$ ;
- 3) выбирает квадратичный невычет  $y$  по модулю  $n$   
(т. е. сравнение  $x^2 = y \pmod{n}$  не должно иметь решений);

Таблица секретных и открытых ключей имеет вид

|       | Секретный ключ | Открытый ключ |
|-------|----------------|---------------|
| Алиса | $p, q$         | $n, y$        |
| Боб   | $p_B, q_B$     | $n_B, y_B$    |

### Шифрование.

Пусть Боб передает Алисе двоичную строку  $b = (b_1, \dots, b_\ell)$ .

Для каждого  $b_i$  Боб выбирает случайно  $x \in \mathbb{Z}_n$ ,  $\text{НОД}(x, n) = 1$ .

Пусть  $e_i = \begin{cases} yx^2 \pmod{n}, & \text{если } b_i = 0; \\ x^2 \pmod{n}, & \text{если } b_i = 1. \end{cases}$

Боб посыпает Алисе набор  $e = (e_1, \dots, e_\ell)$ .

### Расшифрование.

Алиса получает набор  $e = (e_1, \dots, e_\ell)$ .

Для каждого  $e_i$  Алиса полагает  $b'_i = Q_n(e_i)$ .

Заметим, что это можно сделать, только зная разложение  $n = pq$ .

В результате Алиса получает  $b' = (b'_1, \dots, b'_\ell) = b$ .

Идеи Шафи Гольдвассер и Сильвио Микали получили большое развитие в криптографии, а сами авторы были награждены престижной премией Алана Тьюринга в 2012 г.

**Задача 346. Крипtosистема Гольдвассер — Микали.** Докажите, что в результате расшифрования Алиса восстановит именно то сообщение, которое зашифровал Боб.

**Задача 347.** Определите, является ли число  $a$  квадратичным вычетом по модулю  $n$ , если

- |                        |                           |
|------------------------|---------------------------|
| а) $a = 25, n = 35$ ;  | б) $a = 15, n = 91$ ;     |
| в) $a = 47, n = 319$ ; | г) $a = 131, n = 75151$ . |

**Задача 348.** Пусть Алиса выбрала  $p = 5, q = 7$  и квадратичный невычет  $y = 3$ . Определите открытый и секретный ключ Алисы и расшифруйте поступившее ей сообщение от Боба  $e = (13, 9, 11, 13, 29)$ .

**Задача 349.** Пусть Алиса выбрала  $p = 7$ ,  $q = 11$  и квадратичный невычет  $y = 5$ . Определите открытый и секретный ключ Алисы и расшифруйте поступившее ей сообщение от Боба  $e = (4, 48, 58, 20, 45)$ .

**Задача 350.** Для получения сообщений с помощью криптосистемы Гольдвассер — Микали Алиса выбрала простые числа  $p = 3$ ,  $q = 5$  и некоторый невычет  $y$ . Определите, сколькими способами Боб может зашифровать для Алисы бит 1, а сколькими — бит 0. Зависят ли эти количества от выбранного Алисой невычета  $y$ ?

**Задача 351.** Пусть выбраны числа  $p$ ,  $q$  и невычет  $y$ . Пусть Боб передает Алисе некоторый бит  $b_i$ . Сколькими способами он может выбрать случайное число  $x$ , необходимое ему для зашифрования?

**Задача 352.** Верно ли, что количества квадратичных вычетов и невычетов по модулю  $n = pq$  одинаковы?

## 5.5 Криптосистема Эль-Гамаля

Наиболее известной и удачной криптосистемой, отражающей принципы вероятностного шифрования, стала система Эль-Гамаля, предложенная в 1985 г.

Пусть есть группа абонентов, которые собираются передавать сообщения друг другу. Для всей группы выбраны два числа  $p$  и  $g$  такие, что  $p$  — большое простое число, а  $g$  — целое число такое, что  $2 \leq g \leq p - 2$  и числа  $g^0 \bmod p, \dots, g^{p-2} \bmod p$  попарно различны, т. е. пробегают все элементы множества  $\{1, 2, \dots, p-1\}$ . Каждый абонент группы выбирает себе своё число  $c$ , которое является секретным ключом.

|              | Секретный ключ                  | Открытый ключ   |
|--------------|---------------------------------|---|
| <b>Алиса</b> | число $c_A$ , $1 < c_A < p - 1$ | числа $p$ и $g$ , а также число $d_A = g^{c_A} \bmod p$ |
| <b>Боб</b>   | число $c_B$ , $1 < c_B < p - 1$ | числа $p$ и $g$ , а также число $d_B = g^{c_B} \bmod p$ |

Алгоритм передачи сообщения  $m$  от Алисы к Бобу:

Шаг 1. Алиса выбирает случайное число  $s$ ,  $1 \leq s \leq p - 2$ , и вычисляет два числа  $r$  и  $e$ , которые передает Бобу, где

$$r = g^s \pmod{p}, \quad e = m \cdot d_B^s \pmod{p}.$$

Шаг 2. Боб, получив числа  $r$  и  $e$ , вычисляет число

$$m' = e \cdot r^{p-1-c_B} \pmod{p}.$$

В результате работы алгоритма Боб на втором шаге вычисляет сообщение  $m'$ , которое и является исходным сообщением, т. е.  $m' = m$ .

**Задача 353. Крипtosистема Эль-Гамаля.** Докажите, что в результате алгоритма Боб действительно получает от Алисы секретное сообщение  $m$ , т. е. в обозначениях алгоритма  $m' = m$ .

**Задача 354.** Используя крипtosистему Эль-Гамаля с параметрами  $p = 23$ ,  $g = 5$ , Вы хотите передать сообщение  $m = 15$  абоненту, секретный ключ которого  $c = 13$ . Определите его открытый ключ. Какие сообщения Вы передадите Бобу по открытому каналу связи, если выбрали  $s = 7$ ? Проверьте, что абонент получил верное сообщение.

**Задача 355.** Алиса и Боб используют крипtosистему Эль-Гамаля. Пусть Алиса выбрала числа  $p = 73$ ,  $g = 5$ ,  $c_A = 4$ . Определите её секретный и открытый ключи и расшифруйте поступившее ей от Боба сообщение  $C = (9, 28)$ . Можно ли определить, какое секретное число  $s$  использовал Боб при зашифровании?

**Задача 356. Точки радиосвязи.** Перед Вами стоит задача определить число действующих точек радиосвязи в некоторой области  $K^*$ . Эту информацию должен сообщить неизвестный Вам секретный агент. Для связи с ним Вы решили воспользоваться крипtosистемой Эль-Гамаля. Для этого выбрали простое число  $p = 101$ , целое число  $g = 3$  и секретный ключ 6.

- а) Определите свой секретный и открытый ключи.
- б) После публикации своего открытого ключа в Интернете Вы получили от некого пользователя сообщение  $(66, 82)$ . Затем пришло еще два сообщения от других пользователей  $(66, 63)$  и  $(97, 73)$ , которые

Вас несколько озадачили. Чем? Что во всех этих трёх сообщениях Вам показалось странным? Как они связаны? Какой ответ Вы направите в Центр?

в) Какие преимущества и недостатки имеет криптосистема Эль-Гамаля?

**Задача 357. Маршрут.** Вам должны передать по каналу связи зашифрованную схему маршрута от точки  $X$  до точки  $Y$ , состоящую из указаний о поворотах. Маршрут кодируется так: повернуть налево — «0», направо — «1». Полная двоичная строка маршрута разбивается на части по шесть бит, каждая часть преобразуется в соответствующее десятичное число и шифруется с помощью криптосистемы Эль-Гамаля с параметрами  $p = 107$ ,  $g = 7$ . Шифрованные сообщения передаются в бинарном виде. Восстановите маршрут, если Вам поступили три сообщения: (10100, 1010), (11000, 1000000), (110010, 111101); Ваш секретный ключ  $c = 21$ .

# ГЛАВА 6. ЦИФРОВАЯ ПОДПИСЬ

Для осуществления аутентификации источника данных, установления целостности сообщения или электронного документа, обеспечения невозможности отказа от факта подписи конкретного сообщения или документа применяется *цифровая подпись*. Цифровая подпись сообщения является числом, зависящим от самого сообщения и от секретного ключа, известного только тому, кто подписывает.



При изложении задач этой главы мы опирались в основном на книги Б. Я. Рябко, А. Н. Фионова [26] и А. П. Алфёрова, А. Ю. Зубова, А. С. Кузьмина, А. В. Черёмушкина [3].

## 6.1 Цифровая подпись RSA

Рассмотрим цифровую подпись, основанную на криптосистеме RSA. Абонент формирует ключи RSA, как это описано в разделе 5.3.

|       | Секретный ключ  | Открытый ключ |
|-------|-----------------|---------------|
| Алиса | $p_A, q_A, d_A$ | $n_A$ и $e_A$ |

Алгоритм подписания Алисой сообщения  $M = m_1, \dots, m_n$ :

Шаг 1. Вычисляет хэш-функцию  $y = h(m_1, \dots, m_n)$ , которая ставит в соответствие сообщению  $M$  число  $y$ .

Если сообщение  $M$  состоит из одного числа, например,  $M = m$ , то можно считать, что  $y = m$ .

Шаг 2. Вычисляет число  $s = y^{d_A} \bmod n_A$ .

Шаг 3. Формирует подписанное сообщение  $\langle M, s \rangle$ .

Цифровой подписью сообщения  $M$  будет число  $s$ , которое Алиса добавляет к сообщению.

Для проверки подписи Боб сначала расшифровывает исходное сообщение  $M$ , а затем проверяет равенство между значением хэш-функции  $h(M)$  и числом  $y' = s^{e_A} \bmod n_A$ . В случае, если значения совпали, Боб признаёт авторство Алисы.

**Задача 358. Корректность подписи RSA.** Докажите, что если сообщение подписывала Алиса с использованием секретного ключа  $d_A$ , то проверка Боба даст положительный результат.

**Задача 359. Атака на подпись RSA.** Пусть Ева хочет подделать подпись Алисы, зная только её открытый ключ. Что должна вычислить Ева (какие уравнения решить), чтобы достичь успеха?

**Задача 360. Авторство.** Алиса и Боб претендуют на авторство подписанного сообщения  $\langle M, 7 \rangle$ . Известно, что открытые ключи Алисы и Боба имеют следующие значения:  $n_A = 55$ ,  $e_A = 3$ ,  $n_B = 44$ ,  $e_B = 9$ , а значение хэш-функции от  $M$  равно 13. Определите настоящего автора.

**Задача 361. Топливо.** Космический корабль совершает промежуточную посадку на станции, где автоматический заправщик подаёт топливо после получения подписанного (с помощью цифровой подписи RSA) документа от капитана корабля с указанием вида горючего. Корабль «Титан» для полёта на спутник Сатурна нуждается в топливе MD и генерирует открытый ключ  $(35, 5)$ . Злоумышленники из соседней галактики хотят помешать операции и посыпают указание от имени «Титана» залить топливо FW. Оператор заправщика получил два документа —  $(9, 4)$ ,  $(11, 15)$ . Определите, какое топливо соответствует коду 9, а какое — коду 11?

## 6.2 Цифровая подпись Эль-Гамаля

Рассмотрим цифровую подпись, основанную на криптосистеме Эль-Гамаля. Подписывающий формирует ключи, как в разделе 5.5.

|       | Секретный ключ                  | Открытый ключ                              |
|-------|---------------------------------|--|
| Алиса | число $c_A$ , $1 < c_A < p - 1$ | числа $p$ и $g$ , $d_A = g^{c_A} \pmod{p}$ |

Алгоритм подписания Алисой сообщения  $M = m_1, \dots, m_n$ :

- Шаг 1. Вычисляет значение хэш-функции  $y = h(M)$ , которое должно удовлетворять неравенству  $1 < y < p$ .
- Шаг 2. Выбирает случайное число  $k$  взаимно простое с  $p - 1$  и такое, что  $1 < k < p - 1$ .
- Шаг 3. Вычисляет  $r = g^k \pmod{p}$  и  $u = (y - c_A r) \pmod{p - 1}$ .
- Шаг 4. Вычисляет  $s = k^{-1} u \pmod{p - 1}$ , где  $k^{-1}$  это число, удовлетворяющее сравнению  $k^{-1}k \equiv 1 \pmod{p - 1}$ .
- Шаг 5. Формирует подписанное сообщение  $\langle M, r, s \rangle$ .

Для проверки подписи Боб восстанавливает секретное сообщение  $M$ , вычисляет значение хэш-функции  $y = h(M)$  и проверяет равенство  $d_A^r r^s \equiv g^y \pmod{p}$ . Если равенство выполняется, Боб признаёт авторство Алисы.

**Задача 362. Корректность подписи Эль-Гамаля.** Докажите, что если сообщение подписывала Алиса с использованием секретного ключа  $c_A$ , то проверка Боба даст положительный результат.

**Задача 363. Атака на подпись Эль-Гамаля.** Пусть Ева хочет подделать подпись Алисы, зная только её открытый ключ. Что должна вычислить Ева (какие уравнения решить), чтобы достичь успеха?

**Задача 364. Авторство.** Пусть  $p = 23$ ,  $g = 5$  — общие параметры для Алисы и Боба. Алиса и Боб претендуют на авторство подписанного сообщения  $\langle M, 20, 21 \rangle$ . Определите настоящего автора, если известно, что открытые ключи Алисы и Боба имеют следующие значения:  $p_A = 13$ ,  $p_B = 17$ , а значение хэш-функции от  $M$  равно 3.

**Задача 365. Археологическое открытие.** К комиссару полиции Луи Помпиду обратился за помощью юный секретарь научного журнала «La Revue Archeologique» мсье Жерар. Он рассказал, что в редакцию одновременно пришли три подписанных письма ( $M, 11, 18$ ), ( $M, 10, 8$ ), ( $M, 6, 11$ ), сообщающих о важном археологическом открытии в южной провинции Китая. Первый автор — итальянский палеонтолог Луиджи Копатти. Помпиду выяснил, что его открытый ключом является набор:  $p = 23$ ,  $g = 5$ ,  $d_L = 15$ . Вторым отправителем был шведский историк Юхан Копатлунд с таким же набором открытых ключей, за исключением  $d_{\text{Ю}} = 17$ . Третьим человеком была археолог Ани Копатян из Армении, и вновь, её открытый ключ отличался только на  $d_A = 10$ . Также Помпиду узнал, что значение хэш-функции от сообщения  $M$  равно 10, т. е.  $h(M) = 10$ . Луи позвонил своей старой приятельнице, математику Рене Дюбуа, и через 10 минут она назвала имя настоящего автора открытия. Кто им был?

## 6.3 Цифровая подпись Фиата — Шамира

Рассмотрим алгоритм быстрой цифровой подписи. Сложность вычислений в данном случае значительно ниже, чем, например, при использовании алгоритма RSA.

Пусть  $h$  — некоторая хэш-функция, преобразующая исходное сообщение в битовую строку длины  $t$ . Подписывающий выбирает различные простые числа, например, Боб выбирает числа  $p_B$  и  $q_B$  и вычисляет  $n_B = p_B q_B$ . В качестве своего секретного ключа Боб генерирует  $t$  различных случайных взаимно простых с  $n_B$  чисел  $c_{B_1}, \dots, c_{B_m}$ . Открытым ключом объявляется набор чисел  $d_{B_1}, \dots, d_{B_m}$ , где  $d_{B_i} = (c_{B_i}^{-1})^2 \pmod{n}$ ,  $i = 1, \dots, t$ .

|       | Секретный ключ                                      | Открытый ключ                  |
|-------|---|--------------------------------|
| Алиса | $c_{A_1}, \dots, c_{A_m}$ — взаимно простые с $n_A$ | $d_{A_1}, \dots, d_{A_m}, n_A$ |
| Боб   | $c_{B_1}, \dots, c_{B_m}$ — взаимно простые с $n_A$ | $d_{B_1}, \dots, d_{B_m}, n_B$ |

Для подписи сообщения  $M$  Алиса выполняет следующие действия:

Шаг 1. Выбирает случайное число  $r$ ,  $1 \leq r \leq n - 1$ .

Шаг 2. Вычисляет  $u = r^2 \pmod{n_A}$ .

Шаг 3. Вычисляет  $h(M, u) = s = (s_1, s_2, \dots, s_m)$ .

Шаг 4. Вычисляет  $t = r \prod_{i=1}^m c_{A_i}^{s_i} \pmod{n}$ .

Шаг 5. Формирует подписанное сообщение  $\langle M, s, t \rangle$ .

Для проверки подписи Боб вычисляет  $w = t^2 \prod_{i=1}^m d_{A_i}^{s_i} \pmod{n}$  и проверяет равенство  $h(M, w) = s$ . Если равенство выполняется, авторство Алисы установлено.

**Задача 366. Корректность подписи Фиата — Шамира.** Докажите, что если сообщение подписывала Алиса с использованием своего секретного ключа, то проверка Боба даст положительный результат.

**Задача 367. Атака на подпись Фиата — Шамира.** Пусть Ева хочет подделать подпись Алисы, зная только её открытый ключ. Что должна вычислить Ева (какие уравнения решить), чтобы успешно подделать подпись Алисы?

**Задача 368. Аукцион I.** На недавнем аукционе Кристис господин Ротшильд приобрёл полотно Мондриана, поставив на экземпляре договора свою электронную подпись. Повесив картину над камином, он было сел в кресло напротив и начал любоваться, но тут же в дверь постучали. Вошедший представился инспектором Баррингтоном из Скотланд-Ярда и сообщил, что некий сэр Кингстон утверждает, что это он выкупил картину и подпись на договоре стоит именно его. Ротшильд возмутился и предоставил инспектору данные своего открытого ключа:  $d_{r_1} = 10$ ,  $d_{r_2} = 15$ ,  $d_{r_3} = 23$ ,  $d_{r_4} = 45$ ,  $d_{r_5} = 32$ ,  $d_{r_6} = 68$ ,  $n_r = 377$ . Баррингтон смог раздобыть ключ сэра Кингстона ( $d_{k_1} = 15$ ,  $d_{k_2} = 100$ ,  $d_{k_3} = 64$ ,  $d_{k_4} = 86$ ,  $d_{k_5} = 36$ ,  $d_{k_6} = 67$ ,  $n_k = 187$ ), образец договора (204, 35, 185) и хэш-функцию  $h(M, u) = M \pmod{u}$ . Сможет ли господин Ротшильд доказать свое право на собственность и продолжать любоваться картиной?

**Задача 369. Аукцион II.** Через год после вышеупомянутых событий сэр Кингстон оказался на аукционе Сотбис, где ему приглянулся карандашный рисунок Дега. Через час после торгов он узнал, что работу выкупил небезызвестный господин Ротшильд. Обуреваемый

жаждой отмщения, сэр Кингстон сфальсифицировал договор и цифровую подпись к нему, после чего аукционный дом заморозил сделку до выяснения обстоятельств. По возвращении Ротшильд обратился к инспектору Баррингтону с просьбой разобраться в деле. Инспектор, теперь уже имеющий некоторый опыт в таких делах, получив набор ключей Ротшильда ( $d_{r_1} = 238$ ,  $d_{r_2} = 16$ ,  $d_{r_3} = 142$ ,  $d_{r_4} = 192$ ,  $d_{r_5} = 179$ ,  $d_{r_6} = 1$ ,  $d_{r_7} = 77$ ) и Кингстона ( $d_{k_1} = 10$ ,  $d_{k_2} = 14$ ,  $d_{k_3} = 237$ ,  $d_{k_4} = 45$ ,  $d_{k_5} = 39$ ,  $d_{k_6} = 27$ ,  $d_{k_7} = 108$ ), сразу позвонил в Сотбис и попросил вернуть рисунок господину Ротшильду. Как он догадался, что Кингстон подделал договор?



Пит Мондриан. Ферма в Дювендрехте

# ГЛАВА 7. КРИПТОГРАФИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В 1985 г. независимо двумя исследователями Нилом Коблищем и Виктором Миллером было предложено использовать в криптографии алгебраические свойства эллиптических кривых. Роль основной операции в криптографии на эллиптических кривых (Elliptic curve cryptography — ECC) выполняет скалярное умножение точки на некоторое целое число. Такой подход позволяет переложить на эллиптические кривые многие схемы криптографии с открытым ключом (см. главу 5). Высокий интерес к ECC обусловлен тем, что можно использовать ключи существенно меньшей длины по сравнению с классическими схемами, например, 160-битный ключ RSA на эллиптических кривых эквивалентен 1024-битному ключу классической схемы RSA.

В данной главе описаны основные идеи криптографии на эллиптических кривых. Для более детального и основательного знакомства с ECC можно рекомендовать книги А. А. Болотова и др. [9], [10], а также книгу D. Hankerson et al. [45].

## 7.1 Эллиптическая кривая

Пусть  $F$  — некоторое поле характеристики  $\text{char}(F)$ . Эллиптической кривой  $E$  над полем  $F$  называется гладкая кривая третьего порядка. Известно, что такую кривую над любым полем всегда можно привести к форме Вейерштрасса

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (7.1)$$

где  $a_1, a_2, a_3, a_4, a_6 \in F$ . Пара  $(x, y)$ ,  $x, y \in F$ , удовлетворяющая уравнению кривой называется точкой эллиптической кривой.

Из теории алгебраических кривых известно, что кривая является гладкой, если её дискриминант  $\Delta$  отличен от нуля:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

где  $b_2 = a_1^2 + 4a_2$ ,  $b_4 = 2a_4 + a_1a_3$ ,  $b_6 = a_3^2 + 4a_6$ ,  $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ .

Две кривые  $E_1$  и  $E_2$  над полем  $F$  называются *изоморфными*, если они переходят друг в друга при допустимой замене координат:

$$x' = u^2x + r, \quad y' = u^3y + u^2sx + t,$$

где  $u, r, s, t \in F$ .

В зависимости от характеристики поля  $F$  уравнение (7.1) можно упростить при помощи допустимой замены координат ( $a, b, a_i \in F$ ):

- если  $\text{char}(F) \neq 2, 3$ , то  $y^2 = x^3 + ax + b$ ;
- если  $\text{char}(F) = 3$ , то  $y^2 = x^3 + a_2x^2 + a_4x + a_6$ ;
- если  $\text{char}(F) = 2$ , то возможны два случая:
  - *суперсингулярная* эллипт. кривая:  $y^2 + a_3y = x^3 + a_4x + a_6$ ;
  - *несуперсингулярная* эллипт. кривая:  $y^2 + xy = x^3 + a_2x^2 + a_6$ .

**Задача 370. Допустимая замена координат.** В каждом из случаев найдите допустимую замену координат, с помощью которой можно привести уравнение кривой  $E$  над полем  $F$ , заданное в форме Вейерштрасса, к следующему упрощённому виду:

- a)  $y^2 = x^3 + a_2x^2 + a_4x + a_6$  при  $\text{char}(F) = 3$ ;
- б)  $y^2 = x^3 + ax + b$  при  $\text{char}(F) \neq 2, 3$ ;
- в)  $y^2 + a_3y = x^3 + a_4x + a_6$  или  $y^2 + xy = x^3 + a_2x^2 + a_6$  при  $\text{char}(F) = 2$ ;

**Задача 371. Дискриминант.** Покажите, что для каждого из случаев а), б), в) задачи 370 дискриминант кривой вычисляется соответственно по формулам:

- а)  $\Delta = -a_2^3a_6 + a_2^2a_4^2 - a_4^3$ ;
- б)  $\Delta = -16(4a^3 + 27b^2)$ ;
- в)  $\Delta = a_3^4$  или  $\Delta = a_6$ .

**Задача 372.** Определите, являются ли следующие кривые  $E$  над полем  $\mathbb{R}$  эллиптическими, т. е. гладкими кривыми третьего порядка:

- а)  $E : y^2 = x^3 - 3x + 2$ ;
- б)  $E : y^2 = x^3 - \sqrt{2}x + \sqrt{3}$ ;
- в)  $E : y^4 = x^3 - 2x + 3$ ?

**Задача 373.** Найдите множество пар  $(x, y)$ ,  $x, y \in F$ , удовлетворяющих уравнению кривой  $E$  над полем  $GF(p)$ , где  $p$  — простое, если:

- а)  $p = 5, E : y^2 = x^3 + 4x + 3;$     б)  $p = 5, E : y^2 = x^3 + x + 1;$   
 в)  $p = 11, E : y^2 = x^3 + 7x + 2;$     г)  $p = 11, E : y^2 = x^3 + 10x + 9;$   
 д)  $p = 19, E : y^2 = x^3 + x + 2;$     е)  $p = 19, E : y^2 = x^3 + 2x + 4.$

**Задача 374.** Поле  $GF(2^3)$  построено с помощью неприводимого многочлена  $x^3+x+1$  и примитивного элемента  $\alpha = x$ . Найдите множество всех точек следующих кривых, заданных над полем  $GF(2^3)$ :

- а)  $y^2 + xy = x^3 + x^2 + \alpha^3;$   
 б)  $y^2 + xy = x^3 + x^2 + \alpha^4;$   
 в)  $y^2 + xy = x^3 + \alpha^3 x^2 + 1.$

**Задача 375.** Задана эллиптическая кривая  $E : y^2 + xy = x^3 + \alpha^{20}x^2 + \alpha^{14}$  над полем  $GF(2^5)$ . Для построения поля  $GF(2^5)$  выбрали неприводимый многочлен  $x^5 + x^2 + 1$  и примитивный элемент  $\alpha = x$ . Определите, принадлежат ли следующие точки кривой:

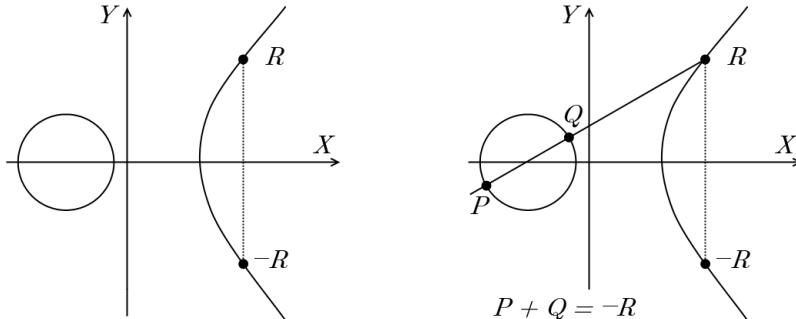
- а)  $P_1 = (0, 0);$     б)  $P_2 = (0, \alpha^7);$   
 в)  $P_3 = (\alpha, \alpha);$     г)  $P_4 = (\alpha^2, \alpha^2);$   
 д)  $P_5 = (\alpha^5, \alpha^{15});$     е)  $P_6 = (\alpha^{29}, \alpha^{30}).$

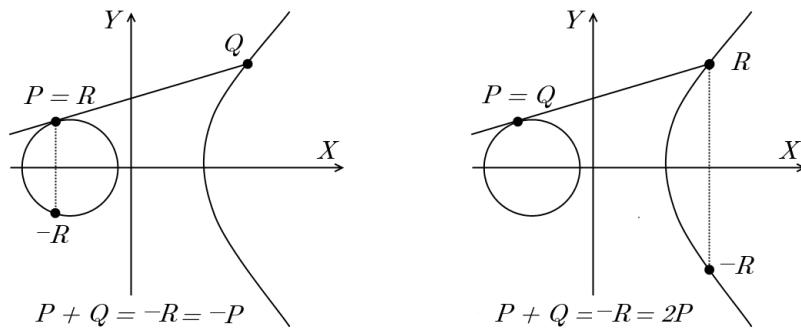
## 7.2 Группа точек эллиптической кривой

Через  $E(F)$  будем обозначать множество точек эллиптической кривой над полем  $F$  вместе с формально введённой бесконечно удалённой точкой  $\mathcal{O}$ , т. е.

$$E(F) = \{(x, y) \mid x, y \in F \text{ и } y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

Идея того, как происходит обращение и сложение точек на эллиптической кривой показана на графиках ниже на примере кривой над полем действительных чисел  $\mathbb{R}$ :





Далее мы будем рассматривать только эллиптические кривые над конечным полем характеристики не равной 2, 3, либо несуперсингулярные кривые над конечным полем характеристики 2. Отметим, что оба этих случая обобщаются на случай произвольной кривой, но для простоты рассмотрим только их, поскольку именно такие кривые используются в криптографических приложениях. Определим для поля  $F$  операции взятия обратного элемента и сложение на  $E(F)$ .

### I. Эллиптическая кривая $E: y^2 = x^3 + ax + b; \text{char}(F) \neq 2, 3$ .

- для любой точки  $P \in E(F)$  полагаем  $P + \mathcal{O} = \mathcal{O} + P = P$ ;
- для точки  $P = (x, y)$  полагаем  $-P = (x, -y)$  и  $P + (-P) = \mathcal{O}$ ;
- для точек  $P = (x_1, y_1)$  и  $Q = (x_2, y_2)$  при  $P \neq \pm Q$  полагаем  $P + Q = (x_3, y_3)$ , где

$$x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \quad \text{и} \quad y_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)(x_1 - x_3) - y_1.$$

- для точки  $P = (x_1, y_1)$  при  $P \neq -P$  полагаем  $2P = (x_3, y_3)$ , где

$$x_3 = \left( \frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 \quad \text{и} \quad y_3 = \left( \frac{3x_1^2 + a}{2y_1} \right)(x_1 - x_3) - y_1.$$

### II. Эллиптическая кривая $E: y^2 + xy = x^3 + ax^2 + b; F = GF(2^n)$ .

- для любой точки  $P \in E(F)$  полагаем  $P + \mathcal{O} = \mathcal{O} + P = P$ ;
- для точки  $P = (x, y)$  полагаем  $-P = (x, x + y)$  и  $P + (-P) = \mathcal{O}$ ;
- для точек  $P = (x_1, y_1)$  и  $Q = (x_2, y_2)$  при  $P \neq \pm Q$  полагаем  $P + Q = (x_3, y_3)$ , где

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad \text{и} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \quad \lambda = \frac{y_1 + y_2}{x_1 + x_2};$$

- для точки  $P = (x_1, y_1)$  при  $P \neq -P$  полагаем  $2P = (x_3, y_3)$ , где

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2} \quad \text{и} \quad y_3 = x_1^2 + \lambda x_3 + x_3, \quad \lambda = x_1 + \frac{y_1}{x_1}.$$

**Задача 376. Противоположный элемент.** Покажите, что в каждом из случаев I и II противоположный элемент  $-P$  для точки  $P$  определен корректно, т. е. точка  $-P$  также принадлежит рассматриваемой эллиптической кривой.

**Задача 377. Сложение.** Покажите, что в каждом из случаев I и II операция сложения определена корректно, т. е. сумма двух точек также принадлежит рассматриваемой эллиптической кривой.

**Задача 378. Теорема Пуанкаре.** Покажите, что множество точек эллиптической кривой вместе с бесконечно удалённой точкой образует абелеву группу относительно определённой выше операции сложения.

**Задача 379. (\*\* Теорема Хассе.** Пусть задана эллиптическая кривая над полем  $GF(q)$  и  $N$  — число точек этой кривой. Тогда  $N$  удовлетворяет неравенствам

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

**Задача 380.** Пусть заданы эллиптическая кривая  $E$  над полем  $GF(p)$  и точка  $P$ . Найдите точку  $2P$ , если

- $p = 5$ ,  $E : y^2 = x^3 + x + 1$ ;  $P = (0, 1)$ ;  $P = (2, 1)$ ;  $P = (3, 4)$ ;
- $p = 11$ ,  $E : y^2 = x^3 + 10x + 9$ ;  $P = (1, 3)$ ;  $P = (7, 2)$ ;  $P = (10, 8)$ ;
- $p = 19$ ,  $E : y^2 = x^3 + 2x + 4$ ;  $P = (1, 11)$ ;  $P = (5, 5)$ ;  $P = (18, 18)$ .

**Задача 381.** Пусть заданы эллиптическая кривая  $E$  над полем  $GF(p)$  и две точки  $P$  и  $Q$ . Найдите точку  $P + Q$ , если

- $p = 5$ ,  $E : y^2 = x^3 + x + 1$ ;  $P = (0, 1)$  и  $Q = (4, 3)$ ,  $P = (2, 4)$  и  $Q = (4, 2)$ ,  $P = (0, 4)$  и  $Q = (4, 2)$ ,  $P = (3, 1)$  и  $Q = (2, 1)$ ;
- $p = 11$ ,  $E : y^2 = x^3 + 10x + 9$ ;  $P = (0, 2)$  и  $Q = (1, 8)$ ,  $P = (2, 2)$  и  $Q = (9, 6)$ ,  $P = (10, 8)$  и  $Q = (4, 6)$ ,  $P = (7, 2)$  и  $Q = (7, 9)$ ;
- $p = 19$ ,  $E : y^2 = x^3 + 2x + 4$ ;  $P = (0, 17)$  и  $Q = (8, 0)$ ,  $P = (6, 2)$  и  $Q = (10, 13)$ ,  $P = (5, 5)$  и  $Q = (5, 14)$ ,  $P = (18, 18)$  и  $Q = (1, 11)$ .

**Задача 382.** Пусть заданы эллиптическая кривая  $E$  над полем  $GF(2^n)$  и точка  $P$ . Поле  $GF(2^n)$  при  $n = 2, 3, 4$  построено с помощью неприводимого многочлена  $x^n + x + 1$  и примитивного элемента  $\alpha = x$ . Найдите точку  $2P$ , если

а)  $n = 2, E : y^2 + xy = x^3 + x^2 + 1;$

$P = (0, 1); P = (\alpha, 1); P = (\alpha^2, 1);$

б)  $n = 3, E : y^2 + xy = x^3 + \alpha^6x^2 + 1;$

$P = (\alpha, 0), P = (\alpha^2, \alpha^4), P = (\alpha^6, \alpha^3);$

в)  $n = 4, E : y^2 + xy = x^3 + \alpha^7x^2 + \alpha^7;$

$P = (1, \alpha^5), P = (\alpha^3, \alpha^{13}), P = (\alpha^9, \alpha^1).$

**Задача 383.** Пусть заданы эллиптическая кривая  $E$  над полем  $GF(2^n)$  и две точки  $P$  и  $Q$ . Поле  $GF(2^n)$  построено с помощью неприводимого многочлена  $x^n + x + 1$  и примитивного элемента  $\alpha = x$ . Найдите точку  $P + Q$ , если

а)  $n = 2, E : y^2 + xy = x^3 + x^2 + 1;$

$P = (0, 1)$  и  $Q = (\alpha^2, \alpha^1), P = (1, \alpha)$  и  $Q = (1, \alpha^2); P = (0, 1)$  и  $Q = (\alpha, \alpha^2); P = (\alpha, 1)$  и  $Q = (\alpha^2, \alpha^1);$

б)  $n = 3, E : y^2 + xy = x^3 + \alpha^6x^2 + 1;$

$P = (0, 1)$  и  $Q = (\alpha^4, \alpha^5), P = (\alpha, 0)$  и  $Q = (\alpha^6, \alpha^3); P = (\alpha^3, 1)$  и  $Q = (\alpha^5, \alpha^2); P = (\alpha, \alpha)$  и  $Q = (\alpha^6, \alpha^4);$

в)  $n = 4, E : y^2 + xy = x^3 + \alpha^7x^2 + \alpha^7;$

$P = (0, \alpha^{11})$  и  $Q = (\alpha^4, \alpha^9), P = (\alpha^2, \alpha^{10})$  и  $Q = (\alpha^5, \alpha^{12}); P = (\alpha^{11}, \alpha^{10})$  и  $Q = (\alpha^{11}, \alpha^{14}); P = (\alpha^8, 1)$  и  $Q = (\alpha^6, 0).$

### 7.3 Протокол Диффи — Хеллмана на эллиптических кривых

В разделе 5.1 главы о криптосистемах с открытым ключом был описан классический вариант протокола Диффи — Хеллмана, позволяющий установить общий секретный ключ, обмениваясь сообщениями по открытому каналу связи. Стойкость такого алгоритма основана на *проблеме дискретного логарифма* (DLP), аналог которой можно сформулировать и для группы точек эллиптической кривой над конечным полем.

**Проблема DLP для группы точек эллиптической кривой.** Пусть задана эллиптическая кривая над конечным полем. Как найти целое число  $k$  по двум известным точкам кривой  $P$  и  $Q = kP$ ?

Для данной проблемы неизвестны на настоящий момент полиномиальные алгоритмы решения.

Опишем протокол Диффи — Хеллмана для эллиптических кривых. Пусть задана эллиптическая кривая  $E$  над конечным полем  $F$  и на ней выбрана точка  $P$  высокого порядка  $n$ . Напомним, что *порядком* точки  $P$  называется такое минимальное целое неотрицательное число  $n$ , что  $nP = \mathcal{O}$ . В таблице ниже приведено, как формируются открытые и секретные ключи Алисы и Боба для протокола Диффи — Хеллмана.

|              | Открытый ключ  | Секретный ключ                                |
|--------------|--|---|
| <b>Алиса</b> | Эллиптическая кривая $E$ , точка $P$ порядка $n$ , $Q_A = k_A P$ | случайное число $k_A$ , взаимно простое с $n$ |
| <b>Боб</b>   | Эллиптическая кривая $E$ , точка $P$ порядка $n$ , $Q_B = k_B P$ | случайное число $k_B$ , взаимно простое с $n$ |

Протокол формирования общего ключа:

Шаг 1. Алиса, используя открытый ключ Боба, вычисляет  $K_{AB} = k_A Q_B$ .

Шаг 2. Боб, используя открытый ключ Алисы, вычисляет  $K_{BA} = k_B Q_A$ .

В результате работы протокола Диффи — Хеллмана Алиса и Боб получают общий секретный ключ — точку  $K = K_{AB} = K_{BA}$ .

**Задача 384. Протокол Диффи — Хеллмана.** Докажите, что в результате работы протокола Алиса и Боб действительно устанавливают общий ключ, т. е. в обозначениях алгоритма  $K_{AB} = K_{BA}$ .

**Задача 385. Номер дома.** Алиса хочет сообщить Бобу номер дома  $N$ ,  $0 < N < 13$ , в котором планируется проведение встречи. Для этого она устанавливает общий секретный ключ  $K = (x_K, y_K)$  с Бобом с помощью протокола Диффи — Хеллмана на эллиптической кривой  $y^2 = x^3 + 10x + 1$  над полем  $GF(13)$  и затем зашифрованный номер дома  $C = (N + x_K) \bmod p = 4$  открыто передаёт Бобу. Помогите

Бобу, секретный ключ которого равен  $k_B = 6$ , узнать номер дома, если для работы протокола была выбрана точка  $P = (10, 10)$  порядка 19 и открытый ключ Алисы  $Q_A = (12, 4)$ .



**Задача 386. На Луну.** Профессор Селезнёв не хочет отпускать свою маленькую дочь Алису в путешествие на Луну, пока она не научится сама пользоваться системами шифрования, для начала — протоколом Диффи — Хеллмана. Для обучения Алиса с профессором Селезнёвым и капитаном Зелёным выбрали эллиптическую кривую  $y^2 + xy = x^3 + \alpha^3x^2 + \alpha^7$  над полем  $GF(2^4)$ , построенном с помощью неприводимого многочлена  $x^4 + x + 1$  и примитивного элемента  $\alpha = x$ , и договорились об общей точке  $P = (\alpha^3, \alpha^{10})$ . Помогите Алисе отправиться на Луну, выполнив следующее:

- определите порядок точки  $P$ ;
- сформируйте открытый ключ Алисы, если её секретный  $k_A = 5$ ;
- по протоколу Диффи — Хеллмана установите общие секретные ключи  $K_{AC}$  и  $K_{AZ}$  с профессором Селезнёвым и капитаном Зелёным соответственно, если их открытые ключи —  $Q_C = (\alpha^{11}, \alpha^{13})$  и  $Q_Z = (\alpha^7, \alpha^{11})$ .

**Задача 387. Прослушивание.** Два начинающих шифровальщика Гоша и Стас выбрали эллиптическую кривую  $y^2 + xy = x^3 + \alpha^5x^2 + \alpha^7$

над полем  $GF(2^5)$  и общую точку  $P = (\alpha, \alpha^4)$ . У каждого есть свой открытый ключ  $Q_G = (\alpha^7, \alpha^4)$  и  $Q_C = (\alpha^8, \alpha^{12})$ . С помощью протокола Диффи — Хеллмана они устанавливают секретный ключ  $K = (x_K, y_K)$  и координатой  $x_K$  шифруют букву сообщения по принципу «одноразового блокнота» (напомним, что каждому элементу поля  $GF(2^5)$  соответствует бинарный вектор длины 5). Каждая буква сообщения («е» и «ё» отождествлены) кодируется двоичной строкой длины 5, соответствующей порядковому номеру буквы в алфавите (от 0 до 31). Каждая буква сообщения складывается по модулю 2 с ключом  $x_K$ .

а) Может ли начинающий криptoаналитик Коля восстановить секретное сообщение Гоши и Стаса и секретный ключ  $x_K$  без вычисления множества точек кривой, если в открытом канале связи он подряд наблюдал следующее: (11101), (11111), (01111), (10011), (11001), (01101), (10011), (10001). При этом Коля знает, что передавалось осмысленное слово.

б) Если Коля успешно справится с первой задачей и восстановит ключ  $x_K$ , как ему определить секретные ключи  $k_G$  и  $k_C$ ?

## 7.4 Криптосистема Эль-Гамаля на эллиптических кривых

Классическую криптосистему Эль-Гамала (см. раздел 5.5) можно также переложить на эллиптические кривые. Пусть задана эллиптическая кривая  $E$  над полем  $F$ , и определён способ «вкладывания» сообщения  $m$  в соответствующую точку  $M$  кривой  $E$ . Группа абонентов (среди которых Алиса и Боб) договаривается о выборе общей точке  $P$  высокого порядка  $n$ . Далее каждый абонент формирует свой секретный и открытый ключ согласно таблице ниже.

|              | Открытый ключ  | Секретный ключ                                |
|--------------|--|---|
| <b>Алиса</b> | Эллиптическая кривая $E$ , точка $P$ порядка $n$ , $Q_A = k_A P$ | случайное число $k_A$ , взаимно простое с $n$ |
| <b>Боб</b>   | Эллиптическая кривая $E$ , точка $P$ порядка $n$ , $Q_B = k_B P$ | случайное число $k_B$ , взаимно простое с $n$ |

Алгоритм передачи сообщения  $M \in E(F)$  от Алисы Бобу:

Шаг 1. Алиса выбирает случайное число  $s$ , взаимно простое с  $n$ , и находит две точки кривой  $C_1$  и  $C_2$ , которые передает Бобу, где

$$C_1 = sP, \quad C_2 = M + sQ_B.$$

Шаг 2. Боб, получив пару точек  $C_1$  и  $C_2$ , определяет точку

$$M' = -k_B C_1 + C_2.$$

В результате работы алгоритма Боб на втором шаге вычисляет сообщение  $M'$ , которое и является исходным сообщением, т. е.  $M' = M$ .

**Задача 388. Криптосистема Эль-Гамаля.** Докажите, что в результате работы алгоритма Боб действительно получает от Алисы секретное сообщение  $M$ , т. е. в обозначениях алгоритма  $M' = M$ .

**Задача 389. Новички.** Алиса и Боб впервые используют для общения криптосистему Эль-Гамаля на эллиптической кривой  $y^2 + xy = x^3 + \alpha^6 x^2 + 1$  над полем  $GF(2^3)$ . Они договорились об общей открытой точке  $P = (\alpha^2, \alpha)$ . В качестве своего секретного ключа Алиса выбрала  $k_A = 5$ , а Боб сообщил свой личный открытый ключ  $Q_B = (\alpha, \alpha)$ .

а) Помогите Алисе передать Бобу сообщение  $M = (\alpha^2, \alpha^4)$ .

б) Сформируйте открытый ключ Алисы.

в) Алиса получила от Боба две точки  $C_1 = (\alpha^6, \alpha^3)$  и  $C_2 = (\alpha^6, \alpha^3)$ .

Какое сообщение отправлял Боб?

**Задача 390. Космические пираты.** Крыс планирует проникнуть на планету с кодовым номером  $N$ . Этот номер он собирается сообщить своему напарнику Весельчаку У в зашифрованном виде. Для этого он использует криптосистему Эль-Гамаля на эллиптической кривой  $y^2 = x^3 + 14x + 16$  над полем  $GF(23)$ . Точку  $M$  на кривой, содержащую в себе номер планеты, Крыс выбрал так, что  $x_M = N$ .

а) Сформируйте открытый и секретный ключи Весельчака У, если  $k_{By} = 14$  и выбрана общая точка  $P = (11, 11)$  порядка 31.

б) Расшифруйте номер планеты, если Весельчак У получил от Крыса две точки  $C_1 = (21, 16)$  и  $C_2 = (14, 9)$ .

**Задача 391. Монеты.** Лиса Алиса намеревается сообщить коту Базилио координаты точек на Поле Чудес, где зарыты четыре монеты.

Для этого она выбрала эллиптическую кривую  $y^2 = x^3 + 4x + 4$  над полем  $GF(41)$  так, что эта кривая содержит точки, являющиеся секретными координатами. Лиса Алиса использует крипtosистему Эль-Гамаля с открытой точкой  $P = (1, 3)$  порядка 53.

а) Помогите коту Базилио сформировать его открытый ключ  $Q_{KB}$ , для того, чтобы лиса могла передать ему сообщения; в качестве своего секретного ключа кот выбрал  $k_{KB} = 8$ .

б) Расшифруйте поступившие коту координаты четырёх точек:  $C_1^1 = (18, 2)$  и  $C_2^1 = (15, 35)$ ,  $C_1^2 = (29, 27)$  и  $C_2^2 = (9, 20)$ ,  $C_1^3 = (22, 30)$  и  $C_2^3 = (36, 8)$ ,  $C_1^4 = (19, 25)$  и  $C_2^4 = (23, 39)$ .



# ГЛАВА 8. КРИПТОАНАЛИЗ АСИММЕТРИЧНЫХ СИСТЕМ

В данной главе будут рассмотрены теоретико-числовые подходы к анализу таких асимметричных систем, как RSA и Эль-Гамаля. А именно, приводятся подходы к решению задач факторизации и дискретного логарифмирования, лежащих в основе многих криптосистем с открытым ключом. Для детального знакомства с методами асимметричного криptoанализа рекомендуем книги [13], [21], [38].

## 8.1 Атаки на основе алгоритмов факторизации

Напомним, что задача *факторизации* числа состоит в разложении составного числа  $n$  на множители. Будем рассматривать случай  $n = pq$ , где  $p, q$  — простые. И хотя в общем случае для решения задачи факторизации нет эффективно алгоритма, при определённых ограничениях на числа  $p$  и  $q$  эта задача может быть успешно решена. Приведём несколько методов факторизации.

### Метод пробных делений

Будем говорить, что мы решили задачу факторизации для числа  $n$ , если нашли один из его делителей  $p$ , поскольку далее можно запустить тот же алгоритм уже для меньшего числа  $n/p$ . Метод пробных делений — самый простой метод факторизации. Пусть дано число  $n$ , которое надо разложить на множители. Тогда, если число  $n$  является составным, то у него обязательно найдётся простой делитель  $p$  такой, что  $p \leq \sqrt{n}$ . Таким образом, формулируем алгоритм:

- шаг 1. Выписать все простые числа от 2 до  $\sqrt{n}$ ;  $p = 2$ .
- шаг 2. Если  $p$  является делителем числа  $n$ , то говорим, что задача решена, и выходим из алгоритма.
- шаг 3. Положить  $p$  равным следующему простому числу меньшему  $\sqrt{n}$  и перейти на шаг 2.

Если в результате работы алгоритма задача не была решена, т. е. не найдено ни одного простого делителя  $p$ ,  $p \leq \sqrt{n}$ , то число  $n$  является простым.

## Алгоритм факторизации Ферма

Пусть дано нечётное число  $n = ab$ , где  $a \geq b > 0$ . Данный метод основан на том, что такое число  $n$  представимо в виде  $n = x^2 - y^2$ ,  $x > y \geq 0$ , где  $a = x + y$ ,  $b = x - y$ . Алгоритм нахождения  $a$  и  $b$ :

- шаг 1. Для каждого целого числа  $x$ ,  $\sqrt{n} \leq x \leq (n+1)/2$ , вычислить величину  $t = x^2 - n$  и перейти на шаг 2.
- шаг 2. Вычислить число  $y$ , равное целой части числа  $\sqrt{x^2 - n}$ . Если  $t \neq y^2$ , то перейти к следующему  $x$  на шаге 1. Если  $t = y^2$ , то разложение  $n = ab$  найдено, где  $a = x + y$ ,  $b = x - y$ .

**Теорема 7.** Пусть  $n = pq$ ,  $p > q$ ,  $p, q$  — простые числа. Тогда если  $p - q < n^{1/4}$ , то алгоритм факторизации Ферма эффективно раскладывает  $n$  на множители.

## $(p - 1)$ -метод Полларда

Простые числа  $p$  и  $q$  в системе RSA необходимо также выбирать, исходя из тех соображений, чтобы каждое число  $p \pm 1$ ,  $q \pm 1$  имело по крайней мере один простой делитель, больший чем  $10^{20}$ . В противном случае  $p$  можно найти, используя  $(p - 1)$ -алгоритм Полларда. Данный метод применяется для частного случая факторизации, когда заранее известно, что число  $n$  равно произведению двух простых чисел  $p$  и  $q$ .

Число  $m$  называется *показательно  $b$ -гладким*, если любая степень простого числа, которая делит  $m$ , строго меньше числа  $b$ . Число  $b$  называется *порогом показательной гладкости* числа  $m$ . Например, число  $m = 2^5 \cdot 3$  является показательно 33-гладким. Заметим, что каждое показательно  $b$ -гладкое число  $m$  является делителем числа  $b!$ . Однако, число  $m$  может быть делителем факториала и меньшего числа, чем  $b$ . Например,  $m = 2^5 \cdot 3$  делит  $8!$ .

Предположим, что нам известно, что число  $p - 1$  является показательно  $b$ -гладким, а число  $q - 1$  таковым не является. Тогда число  $p - 1$  делит  $b!$ , и есть надежда, что  $q - 1$  не делит  $b!$ .

Алгоритм:

- шаг 1. Выбрать два числа:  $a$  — основание (можно положить  $a = 2$ ),  $b$  — предполагаемый порог показательной гладкости числа  $p - 1$ .
- шаг 2. Вычислить число  $A = a^{b!} \bmod n$ .
- шаг 3. Вычислить  $p' = \text{НОД}(A - 1, n)$ . Если  $1 < p' < n$ , то  $p'$  — делитель числа  $n$ , т. е.  $p' = p$ . Иначе результат не получен, переходим на шаг 1.

Для того чтобы применять данный алгоритм, необходимо подобрать такое число  $b$ , что  $(p - 1)$  делит  $b!$ , а  $(q - 1)$  не делит  $b!$ . Только в этом случае возможно получить требуемый результат.

**Задача 392. Метод пробных делений.** Методом пробных делений разложите на множители следующие числа:

- |            |             |               |
|------------|-------------|---------------|
| а) 1 496;  | б) 9 791;   | в) 10 374;    |
| г) 41 860; | д) 413 559; | е) 2 323 444. |

**Задача 393.** Покажите, что в алгоритме факторизации Ферма достаточно рассматривать только такие  $x$ , для которых  $\sqrt{n} \leq x \leq (n + 1)/2$ .

**Задача 394. Корректность метода Ферма.** Докажите корректность алгоритма факторизации Ферма числа  $n = ab$ , где  $a \geq b > 0$ .

**Задача 395. Алгоритм факторизации Ферма I.** Методом факторизации Ферма разложите на множители числа:

- |            |             |               |
|------------|-------------|---------------|
| а) 247;    | б) 1 769;   | в) 10 199;    |
| г) 24 843; | д) 252 178; | е) 1 022 177. |

**Задача 396. Алгоритм факторизации Ферма II.** Используя алгоритм факторизации Ферма, разложите  $n$  на простые множители:

- |                        |                         |
|------------------------|-------------------------|
| а) $n = 323$ ;         | б) $n = 62\ 879$ ;      |
| в) $n = 1\ 308\ 007$ ; | г) $n = 11\ 193\ 691$ . |

**Задача 397.** Определите минимальное значение  $b$ , для которого число  $n$  является показательно  $b$ -гладким, если:

- |                     |                        |
|---------------------|------------------------|
| а) $n = 4\ 752$ ;   | б) $n = 14\ 365$ ;     |
| в) $n = 225\ 792$ ; | г) $n = 4\ 899\ 069$ . |

**Задача 398.** Пусть  $m$  — показательно  $b$ -гладкое число. Докажите, что  $m$  делит  $b!$ .

**Задача 399. Корректность  $(p - 1)$ -метода Полларда.** Докажите корректность работы  $(p - 1)$ -метода Полларда факторизации числа  $n = pq$ , где  $p, q$  — простые числа.

**Задача 400.  $(p - 1)$ -метод Полларда I.** Используя алгоритм Полларда, факторизуйте  $n$ :

- |                        |                        |
|------------------------|------------------------|
| а) $n = 4\ 043$ ;      | б) $n = 8\ 227$ ;      |
| в) $n = 29\ 261$ ;     | г) $n = 540\ 143$ ;    |
| д) $n = 1\ 119\ 631$ ; | е) $n = 2\ 767\ 169$ . |

**Задача 401.  $(p - 1)$ -метод Полларда II.** Применяя метод Полларда, найдите разложение на простые множители следующих чисел:

- |                              |  |
|------------------------------|--|
| а) $n = 719\ 088\ 091$ ;     |  |
| б) $n = 15\ 770\ 708\ 441$ . |  |

При каких значениях порога показательной гладкости это возможно сделать?

## 8.2 Атаки на основе вычисления дискретного логарифма

Напомним формулировку задачи дискретного логарифмирования. Пусть  $y = a^x \bmod n$ . Требуется найти  $x$ . Это вычислительно трудная задача, на которой основана безопасность некоторых криптосистем с открытым ключом, таких как схема Эль-Гамаля (см. раздел 5.5), алгоритм обмена ключами Диффи — Хеллмана — Меркля, американский стандарт цифровой подписи (DSS).

## Метод малых и больших шагов

Метод малых и больших шагов впервые был описан Дэниэлем Шенкском в 1973 г. Алгоритм вычисляет дискретный логарифм  $x$  в простом поле характеристики  $p$ , т. е. по известным  $y, a, p$  находит  $x$  такой, что  $y = a^x \pmod{p}$ .

**Шаг 1. Инициализация.** Выбрать два целых числа  $m$  и  $k$ , что

$$mk > p.$$

**Шаг 2. Малый шаг.** Вычислить ряд чисел  $S$ :

$$S = \{y \pmod{p}, ay \pmod{p}, a^2y \pmod{p}, \dots, a^{m-1}y \pmod{p}\}.$$

**Шаг 2. Большой шаг.** Вычислить ряд чисел  $T$ :

$$T = \{a^m \pmod{p}, a^{2m} \pmod{p}, a^{3m} \pmod{p}, \dots, a^{km} \pmod{p}\}.$$

**Шаг 4. Поиск, сравнение, вычисление.** Найти совпадающие элементы в последовательностях  $S$  и  $T$ , а именно  $a^i y = a^{jm} \pmod{p}$ . Затем вычислить  $x = jm - i$ , что и будет требуемым значением логарифма  $\log_a y \pmod{n}$ .

## Алгоритм Сильвера — Полига — Хеллмана

Данный алгоритм был независимо предложен Роландом Сильвером и двумя американскими математиками Стивеном Полигом и Мартином Хеллманом в 1978 г. Алгоритм вычисляет дискретный логарифм  $x = \log_a b \pmod{q}$ , где  $q$  — простое число.

**Шаг 1.** Разложить  $q - 1$  на множители ( $p_i$  — простые числа):

$$q - 1 = \prod_{i=1}^k p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

**Шаг 2.** Вычислить значения  $r_{p_i,j}$ :

$$r_{p_i,j} = a^{j(q-1)/p_i} \pmod{q}, \quad 0 \leq j \leq p_i.$$

**Шаг 3.** Вычислить дискретный логарифм  $x = \log_a b \pmod{q}$ :

**I.** Аналогично алгоритму малых и больших шагов найти отдельные дискретные логарифмы  $\log_a b \bmod p_i^{\alpha_i}$ . Для вычисления  $\log_a b$  по модулю  $p_i^{\alpha_i}$  рассмотрим его представление по базе  $p_i$ :

$$\log_a b \bmod p_i^{\alpha_i} = x_0 + x_1 p_i + \dots + x_{\alpha_i-1} p_i^{\alpha_i-1},$$

где  $0 \leq x_i < p_i - 1$ .

а) Для нахождения  $x_0$  вычислить  $b^{(q-1)/p_i}$ , что эквивалентно  $r_{p_i,j}$  для некоторого  $j$ , и положить  $x_0 = j$ :

$$b^{(q-1)/p_i} \bmod q = r_{p_i,j}.$$

Это возможно, поскольку

$$b^{(q-1)/p_i} = a^{x(q-1)/p} = a^{x_0(q-1)/p} \pmod{q} = r_{p_i,x_0}.$$

б) Для нахождения  $x_1$  вычислить  $b_1 = ba^{-x_0}$ . Если

$$b_1^{(q-1)/p_i^2} \bmod q = r_{p_i,j},$$

то положить  $x_1 = j$ .

с) Для получения  $x_2$  найти  $b_2 = ba^{-x_0-x_1 p_i}$  и вычислить

$$b_2^{(q-1)/p_i^3} \bmod q.$$

Таким же образом итеративно находятся  $x_0, x_1, \dots, x_{\alpha_i-1}$ .

**II.** Используя китайскую теорему об остатках (см. теорему 3), найти значение  $x$ .

**Задача 402. Корректность метода малых и больших шагов.** Покажите, что метод малых и больших шагов всегда вычисляет значение логарифма  $\log_a y \bmod p$ , а именно, что на шаге 4 всегда найдутся подходящие  $i$  и  $j$ , для которых совпадут соответствующие элементы в последовательностях  $S$  и  $T$ .

**Задача 403. Трудоёмкость метода малых и больших шагов.** Оцените трудоёмкость метода малых и больших шагов в сравнении с методом полного перебора.

**Задача 404. Атака малых и больших шагов.** Используя метод малых и больших шагов, вычислите дискретные логарифмы:

- |                                  |                                   |
|----------------------------------|-----------------------------------|
| а) $x = \log_2 9 \bmod 17$ ;     | б) $x = \log_2 6 \bmod 19$ ;      |
| в) $x = \log_2 50 \bmod 53$ ;    | г) $x = \log_3 14 \bmod 41$ ;     |
| д) $x = \log_{11} 50 \bmod 61$ ; | е) $x = \log_{59} 67 \bmod 113$ . |

**Задача 405. Алгоритм Сильвера — Полига — Хеллмана.** Вычислите дискретные логарифмы:

- |                               |                                |
|-------------------------------|--------------------------------|
| а) $x = \log_3 8 \bmod 23$ ;  | б) $x = \log_2 18 \bmod 59$ ;  |
| в) $x = \log_2 55 \bmod 73$ ; | г) $x = \log_2 62 \bmod 181$ ; |
| д) $x = \log_3 25 \bmod 37$ ; | е) $x = \log_5 8 \bmod 13$ .   |

## 8.3 Частные алгоритмические атаки

### Атака с угадыванием значения функции Эйлера

Если возможно угадать значение функции Эйлера  $\varphi(n)$ , то можно восстановить открытый текст  $t$  по соответствующему шифртексту  $s$  за полиномиальное относительно логарифма  $n$  время. Покажем, что задача вычисления  $\varphi(n)$  сводится к задаче разложения  $n$  на простые множители за полиномиальное время на детерминированной машине Тьюринга (что означает эквивалентность задач).

**Теорема 8.** Задача вычисления  $\varphi(n)$  эквивалентна задаче разложения числа  $n$  на множители.

**Доказательство.** Сначала отметим, что если  $\varphi(n)$  и  $n$  известны, и  $n$  предположительно является произведением простых чисел  $p$  и  $q$ , тогда  $n$  можно быстро разложить на множители. Пусть  $n = pq$ , тогда  $\varphi(n) = (p-1)(q-1)$ , следовательно,  $pq - p - q + 1 - \varphi(n) = 0$ . Заменяя  $q = n/p$  в этом уравнении, получаем

$$p^2 - (n - \varphi(n) + 1)p + n = 0.$$

Обозначим  $a = n - \varphi(n) + 1$ , тогда числа

$$\frac{a \pm \sqrt{a^2 - 4n}}{2}$$

являются корнями данного уравнения и, следовательно, простыми множителями  $n$ , т. е. числами  $p, q$ . С другой стороны, если множители  $p$  и  $q$  известны, то сразу получаем  $\varphi(n) = (p - 1)(q - 1)$ .

В случае  $n \neq pq$  проведите доказательство самостоятельно.  $\square$

Данная теорема говорит о том, что если нарушитель может вычислить  $\varphi(n)$ , тогда он может осуществить успешную атаку на крипtosистему RSA, вычислив  $d$  как обратный элемент в мультиплексивной группе остатков по модулю  $\varphi(n)$ . Т. е.  $d = e^{-1} \pmod{\varphi(n)}$ .

С другой стороны, значение  $\varphi(n)$  позволит простым способом разложить на множители  $n$ , поскольку

$$p + q = n - \varphi(n) + 1,$$

$$(p - q)^2 = (p + q)^2 - 4n,$$

$$p = \frac{(p + q) + (p - q)}{2},$$

$$q = \frac{(p + q) - (p - q)}{2}.$$

Другими словами, вычислить  $\varphi(n)$  не сложнее, чем разложить на множители  $n$ .

## Атака методом неподвижной точки

Этот метод был открыт Г. Симмонсом и М. Норрисом в 1977 г. Атака с неподвижной точкой также называется циклической атакой или атакой методом повторного шифрования. Она не использует ни один из секретных параметров RSA.

Дадим определение неподвижной точки. Пусть  $0 \leq x < n$ . Если выполняется сравнение  $x^{e^k} = x \pmod{n}$ , где  $k$  — ненулевое целое число, то  $x$  называют *неподвижной точкой порядка  $k$*  крипtosистемы RSA с открытым ключом  $n$  и  $e$ .

**Теорема 9.** *Пусть  $c$  — неподвижная точка порядка  $k$  крипtosистемы RSA для сообщения  $m$  с параметрами  $e$  и  $n$ , т. е. выполняется  $c^{e^k} = c \pmod{n}$ . Тогда  $c^{e^{k-1}} = m \pmod{n}$ .*

**Доказательство.** Поскольку шифрование RSA  $c = m^e \pmod{n}$  есть перестановка сообщений  $0, 1, 2, \dots, n - 1$ , то существует неподвижная точка  $c$ , т. е. выполняется  $c^{e^k} = c \pmod{n}$ . По этой же причине должно выполняться  $c^{e^{k-1}} = m \pmod{n}$ , поскольку  $c^{e^k} = c \pmod{n} = m^e \pmod{n}$ , следовательно,  $c^{e^{k-1}e} = m^e \pmod{n}$ , а значит, имеем  $c^{e^{k-1}} = m \pmod{n}$ .  $\square$

Теорема описывает способ атаки крипtosистемы RSA путём вычисления последовательности степеней  $c$  по модулю  $n$ :  $c^e, c^{e^2}, \dots, c^{e^{k-1}}, c^{e^k}$ . Когда получено  $c^{e^k} \pmod{n} = c$ , мы прекращаем выполнение алгоритма и берём предыдущий элемент  $c^{e^{k-1}} \pmod{n}$ , который и будет решением.

**Задача 406. Угадывание значения функции Эйлера I.** Дано  $n$ . Предположим, критоаналитик каким-либо образом узнал значение функции Эйлера  $\varphi(n)$ . Разложите на множители число  $n$ .

- а)  $n = 713, \varphi(n) = 660$ ;
- б)  $n = 11663, \varphi(n) = 11448$ ;
- в)  $n = 8439703, \varphi(n) = 8433808$ ;
- г)  $n = 74153950911911911911, \varphi(n) = 741539500339832712$ .

**Задача 407. Угадывание значения функции Эйлера II.** Зная значение функции Эйлера  $\varphi(n)$ , разложите на множители число  $n$ .

- а)  $n = 3841, \varphi(n) = 3652$ ;
- б)  $n = 4009, \varphi(n) = 3780$ ;
- в)  $n = 21079, \varphi(n) = 20776$ ;
- г)  $n = 527077, \varphi(n) = 525600$ .

**Задача 408. Атака методом неподвижной точки.** Некоторое сообщение  $m$  зашифровано алгоритмом RSA с параметрами  $n, e$  и получен шифртекст  $c$ . Методом неподвижной точки найдите  $m$ .

- а)  $n = 91, e = 5, c = 88$ ;
- б)  $n = 323, e = 7, c = 36$ ;
- в)  $n = 1081, e = 3, c = 589$ ;
- г)  $n = 2773, e = 17, c = 2342$ .

## 8.4 Атаки с использованием свойств ключа

### Атака для одинаковых сообщений при малых значениях открытого ключа

Пусть, например, три корреспондента имеют следующие открытые ключи:  $n_1, n_2, n_3$  и общую экспоненту  $e = 3$ . Если ещё один пользователь посыпает им одинаковое сообщение  $m$ , то криптоаналитик может получить в своё распоряжение три зашифрованных текста  $c_i = m^3 \pmod{n_i}$ . Далее он может найти решение системы сравнений

$$\begin{cases} x = c_1 \pmod{n_1}, \\ x = c_2 \pmod{n_2}, \\ x = c_3 \pmod{n_3}, \end{cases}$$

лежащее в интервале  $0 < x < n_1 \cdot n_2 \cdot n_3$ .

По китайской теореме об остатках (см. теорему 3 из раздела 4.6) такое решение единствено, и  $x = m^3$ . Значение можно найти, вычислив кубический корень из  $x$ .

### Атака методом Винера

Если секретный ключ  $d$  крипtosистемы RSA принимает слишком малые значения, т. е.  $d < n^{1/4}$ , то с помощью атаки Винера  $d$  может быть вычислено за полиномиальное время по заданному значению открытого ключа  $e$ .

**Лемма 1.** Пусть  $\text{НОД}(e, n) = \text{НОД}(k, d) = 1$  и

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

Тогда  $k/d$  — одна из подходящих дробей разложения  $e/n$  в цепную дробь.

Напомним, что цепные дроби определялись в разделе 4.7.

**Теорема 10.** Пусть  $n = pq$ , где  $p$  и  $q$  — простые числа и

$$\begin{cases} q < p < 2q, \\ d < \frac{1}{3}\sqrt[4]{n}. \end{cases}$$

Тогда, если дано  $e$ , такое, что  $ed = 1 \pmod{\varphi(n)}$ , значение  $d$  может быть «легко» вычислено.

**Доказательство.** Так как  $ed = 1 \pmod{\varphi(n)}$ , то существует некоторое целое  $k$ , такое что  $ed - k\varphi(n) = 1$ . Следовательно,

$$\left| \frac{e}{\varphi(n)} - \frac{k}{d} \right| = \frac{1}{d\varphi(n)}.$$

Поскольку  $n = pq > q^2$ , получаем  $q < \sqrt{n}$ . Также в силу равенства  $\varphi(n) = n - p - q + 1$  верна цепочка неравенств

$$0 < n - \varphi(n) = p + q - 1 < 2q + q - 1 < 3q < 3\sqrt{n}.$$

Тогда

$$\begin{aligned} \left| \frac{e}{n} - \frac{k}{d} \right| &= \left| \frac{ed - kn + k\varphi(n) - k\varphi(n)}{dn} \right| = \left| \frac{1 - k(n - \varphi(n))}{dn} \right| < \\ &< \frac{3k\sqrt{n}}{dn} = \frac{3k}{d\sqrt{n}} < \frac{1}{2d^2}. \end{aligned}$$

Таким образом, по лемме 1,  $k/d$  должна быть одной из подходящих дробей простой цепной дроби  $e/n$ . Кроме того, если  $d < \frac{1}{3}\sqrt[4]{n}$ , она может быть найдена с помощью задачи вычисления нескольких подходящих дробей за полиномиальное время.  $\square$

**Задача 409. Атака с использованием китайской теоремы об остатках.** Три абонента используют следующие параметры криптосистемы RSA:  $e = 3$ ,  $n_1$ ,  $n_2$ ,  $n_3$ . Всем абонентам было послано некое сообщение  $m$ , причем абоненты получили сообщения  $c_1$ ,  $c_2$ ,  $c_3$  соответственно. Найдите исходное сообщение.

- a)  $n_1 = 85$ ,  $n_2 = 77$ ,  $n_3 = 247$  и  $c_1 = 4$ ,  $c_2 = 36$ ,  $c_3 = 77$ ;

- б)  $n_1 = 221$ ,  $n_2 = 209$ ,  $n_3 = 203$  и  $c_1 = 142$ ,  $c_2 = 103$ ,  $c_3 = 90$ ;  
 в)  $n_1 = 1961$ ,  $n_2 = 1457$ ,  $n_3 = 1957$  и  $c_1 = 1679$ ,  $c_2 = 1117$ ,  $c_3 = 816$ ;  
 г)  $n_1 = 26549$ ,  $n_2 = 45901$ ,  $n_3 = 25351$  и  $c_1 = 5366$ ,  $c_2 = 814$ ,  
 $c_3 = 4454$ .

**Задача 410. Криптоанализ RSA.** Используя метод Винера, восстановите секретную экспоненту  $d$ , если известно, что  $d < \sqrt[4]{n}/3$ .

- а)  $n = 82\ 063$ ,  $e = 48\ 797$ ;  
 б)  $n = 9\ 449\ 868\ 410\ 449$ ,  $e = 6\ 792\ 605\ 526\ 025$ .

**Задача 411. Атака методом Винера.** Пусть даны следующие значения  $n$  и  $e$  для крипtosистемы RSA. Найдите  $d$  методом Винера.

- а)  $n = 9173503$  и  $e = 6111579$ ;  
 б)  $n = 160523347$  и  $e = 60728973$ ;  
 в)  $n = 28562942440499$  и  $e = 7502876735617$ .

# ГЛАВА 9. ТЕОРИЯ СЕКРЕТНОСТИ ШЕННОНА

В этой главе приводятся три фундаментальные теоремы Шеннона в симметричной криптографии: о совершенной секретности, об избыточности языка открытых текстов, о числе ложных ключей. Серия задач поможет освоить эти классические результаты на практике.

В изложении теории и задач этой главы мы следуем в основном замечательной книге Г. П. Агибалова [1].

## 9.1 Совершенно секретные системы

Введём понятие шифрсистемы и опишем её вероятностную модель. Набор  $C = (X, Y, Z, p(x), p(z), E, D)$  называется *шифрсистемой*, где  $X$  — множество открытых текстов,  $Y$  — множество шифртекстов,  $Z$  — множество ключей,  $p(x) > 0$ ,  $p(z) > 0$  — функции вероятности открытых текстов и ключей соответственно,  $E : X \times Z \rightarrow Y$  — функция зашифрования,  $D : Y \times Z \rightarrow X$  — функция расшифрования. Последние связаны естественным соотношением: если  $E(x, z) = y$ , то  $D(y, z) = x$ . Будем считать, что в множестве  $Y$  нет лишних элементов, т. е. каждый шифртекст  $y \in Y$  можно получить для подходящих открытого текста  $x$  и ключа  $z$ . Здесь и везде далее будем обозначать элементы из  $X$  через  $x$ , из  $Y$  — через  $y$ , из  $Z$  — через  $z$ . Эта договорённость позволит нам упростить выражения.

Таблицей *шифрования* системы называется прямоугольная таблица, строки которой занумерованы всевозможными открытыми текстами, столбцы — ключами шифрования, а на пересечении строки  $x$  и столбца  $z$  находится шифртекст  $y$  такой, что  $y = E(x, z)$ .

Можно определить условные вероятности:

$p(y|x) = \sum_{z:E(x,z)=y} p(z)$  — вероятность получить шифртекст  $y$  при условии, что был зашифрован открытый текст  $x$ ;

$p(y|z) = \sum_{x:E(x,z)=y} p(x)$  — вероятность получить шифртекст  $y$  при условии, что использовался ключ  $z$ .

Определим  $p(y) = \sum_x p(x)p(y|x) = \sum_{x,z:E(x,z)=y} p(x)p(z) > 0$  — вероятность получить шифртекст  $y$ ;

$p(x|y)$  — апостериорная вероятность открытого текста  $x$  при известном шифртексте  $y$ ;

$p(z|y)$  — апостериорная вероятность ключа  $z$  при известном шифртексте  $y$ .

Справедливы формулы  $p(x|y) = \frac{p(x)p(y|x)}{p(y)}$ ,  $p(z|y) = \frac{p(z)p(y|z)}{p(y)}$ .

**Задача 412. Отношение обратимости.** Докажите, что для любых  $x \neq x'$  и любого  $z$  верно  $E(x, z) \neq E(x', z)$ .

**Задача 413. Свойство таблицы шифрования.** Докажите, что в любом столбце таблицы шифрования все элементы различны.

**Задача 414. Формула Байеса.** Докажите, что для любых  $x, y$  справедливо равенство  $p(x)p(y|x) = p(y)p(x|y)$ .

**Задача 415. Пример шифрсистемы.** Постройте таблицу шифрования для следующего шифрсистемы:  $X = \{0, 1, 2\}$ ,  $Z = \{0, 1, 2, 3, 4\}$ ,  $Y = \{0, 1, 2\}$ , все открытые тексты и ключи равновероятны, т. е.  $p(x) = 1/3$ ,  $p(z) = 1/5$  для любых  $x, y$ . Шифрование определяется так:  $y = E(x, z) = x + z \bmod 3$ ,  $x = D(y, z) = y - z \bmod 3$ . Найдите вероятности  $p(y|x)$  и  $p(x|y)$ .

Шифрсистема  $C$  называется *совершенно секретной*, если для любых  $x$  и  $y$  выполняется  $p(x) = p(x|y)$ . Эквивалентно,  $C$  — совершенно секретная, если для любых  $x$  и  $y$  выполняется  $p(y) = p(y|x)$ .

**Лемма 2. (О трёх кванторах.)** Пусть  $|X| = |Y| = |Z|$ ,  $C$  — совершенно секретная шифрсистема. Тогда

- (i)  $\forall x, \forall y$  существует единственный  $z$  такой, что  $E(x, z) = y$ ;
- (ii)  $\forall x, \forall z$  существует единственный  $y$  такой, что  $E(x, z) = y$ ;
- (iii)  $\forall y, \forall z$  существует единственный  $x$  такой, что  $E(x, z) = y$ .

**Теорема 11. (Шеннона о совершенной секретности.)** Пусть  $|X| = |Y| = |Z| = N$ . Шифрсистема  $C$  — совершенно секретная тогда и только тогда, когда выполняются условия

- (i)  $\forall x, \forall y$  существует единственный  $z$  такой, что  $E(x, z) = y$ ;
- (ii) для любого ключа  $z$  верно  $p(z) = 1/N$ .

**Задача 416.** Докажите эквивалентность двух определений совершенной секретности.

**Задача 417.** Докажите лемму о трёх кванторах.

**Задача 418.** Докажите теорему Шеннона о совершенной секретности.

**Задача 419. Совершенная система?** Определите, при каких параметрах  $n$  и  $m$  следующая шифрсистема (обобщение системы из задачи 415) является совершенно секретной. Пусть  $X = \{0, 1, \dots, n-1\}$ ,  $Z = \{0, 1, \dots, m-1\}$ ,  $Y = \{0, 1, \dots, n-1\}$ , все открытые тексты и ключи равновероятны, т. е.  $p(x) = 1/n$ ,  $p(z) = 1/m$  для любых  $x, y$ . Шифрование определяется так:  $y = E(x, z) = x + z \bmod n$ ,  $x = D(y, z) = y - z \bmod n$ .

**Задача 420.** Докажите, что шифр Вернама (одноразовый блокнот) является совершенно секретной системой. Шифр определяется так:  $X = Y = Z = \mathbb{Z}_2^n$ ,  $p(x) = p(z) = 1/2^n$ ,  $E(x, z) = x \oplus z$ ,  $D(y, z) = y \oplus z$ .

**Задача 421. Совершенная при каких  $a, b$ ?** Определите, при каких целых параметрах  $a$  и  $b$  следующая шифрсистема совершенно секретная. Пусть  $n$  — натуральное,  $X = Y = Z = \{0, 1, \dots, n-1\}$ , все открытые тексты и ключи равновероятны, т. е.  $p(x) = p(z) = 1/n$  для любых  $x, y$ . Функция зашифрования  $y = E(x, z) = ax + bz \bmod n$ .

**Задача 422. Совершенные шифрсистемы.** Согласно задаче 413 в любом столбце таблицы шифрования все элементы различны. Пусть  $X = Y = Z = \{0, 1, \dots, n-1\}$ , все открытые тексты и ключи равновероятны. Тогда шифрсистему можно задать с помощью набора из  $n$  перестановок, определяющих расположения элементов из  $Y$  в каждом столбце таблицы шифрования. Например, одноразовый блокнот

при  $n = 3$  с таблицей шифрования  $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$  можно определить с помощью перестановок:  $id$ ,  $(012)$ ,  $(021)$ , заданных в циклическом представлении. Действительно, первый столбец получается из  $(0, 1, 2)$  с помощью тождественной перестановки, второй столбец — путём перехода  $0 \rightarrow 1$ ,  $1 \rightarrow 2$ ,  $2 \rightarrow 0$ , третий столбец —  $0 \rightarrow 2$ ,  $1 \rightarrow 0$ ,  $2 \rightarrow 1$ .

Для каждой шифрсистемы, приведённой ниже, определите, является ли она совершенно секретной:

- $n = 3$ ; перестановки:  $id$ ,  $(012)$ ,  $(021)$ ;
- $n = 3$ ; перестановки:  $id$ ,  $(012)$ ,  $(02)$ ;
- $n = 4$ ; перестановки:  $id$ ,  $(01)(23)$ ,  $(02)(13)$ ,  $(03)(12)$ ;
- $n = 4$ ; перестановки:  $id$ ,  $(01)(23)$ ,  $(0213)$ ,  $(0312)$ ;
- $n = 4$ ; перестановки:  $id$ ,  $(01)(23)$ ,  $(0213)$ ,  $(032)$ .

**Задача 423.** Совершенные системы и латинские квадраты.  
Докажите, что таблица шифрования любой совершенно секретной шифрсистемы является латинским квадратом (см. раздел 3.4).

## 9.2 Избыточность языка открытых текстов

Пусть  $V = \{\xi_1, \dots, \xi_n\}$  — конечное множество с заданным на нём распределением вероятностей. Пусть  $p(\xi_i) = p_i$  для всех  $i = 1, \dots, n$ ,  $p_1 + \dots + p_n = 1$ . Пусть событие заключается в выборе элемента из множества  $V$  с вероятностью  $p$ . Меру неопределённости исхода этого события измеряет величина, которая называется *энтропией*

$$H(V) = - \sum_{i=1}^n p_i \log_2 p_i.$$

**Задача 424.** Покажите, что энтропия удовлетворяет условиям:

- $H(V) \leq \log_2 n$ ;
- $H(V) = 0 \iff$  существует номер  $i$  такой, что  $p_i = 1$ ;
- $H(V) = \log_2 n \iff$  для всех номеров  $i$  выполнено  $p_i = 1/n$ .

**Задача 425.** Вычислите энтропию множества  $V = \{\xi_1, \xi_2, \xi_3\}$ , если вероятности распределены следующим образом:

- $p_1 = 1/3$ ,  $p_2 = 1/3$ ,  $p_3 = 1/3$ ;
- $p_1 = 1/2$ ,  $p_2 = 1/4$ ,  $p_3 = 1/4$ ;
- $p_1 = 1/8$ ,  $p_2 = 1/8$ ,  $p_3 = 3/4$ .

**Задача 426.** Вычислите энтропию множества  $V = \{\xi_1, \xi_2, \xi_3, \xi_4\}$ , если вероятности распределены следующим образом:

- a)  $p_1 = 1/2, p_2 = 1/4, p_3 = 1/8, p_4 = 1/8;$
- б)  $p_1 = 1/8, p_2 = 1/8, p_3 = 3/4, p_4 = 0;$
- в)  $p_1 = 3/4, p_2 = 1/8, p_3 = 1/16, p_4 = 1/16.$

Применимельно к вероятностной модели шифрсистемы можно определить энтропии  $H(X), H(Y), H(Z)$ , а также рассмотреть энтропии  $H(X, Y), H(Y, Z), H(X, Z)$  для распределений  $p(x, y), p(y, z), p(x, z)$ . Введём условные энтропии:

$H(X|y) = -\sum_x p(x|y) \log_2(p(x|y))$  — средняя неопределенность открытого текста, если известен конкретный шифртекст  $y$ ;

$H(X|Y) = \sum_y p(y)H(X|y)$  — средняя неопределенность открытого текста при известном шифртексте;

$H(Z|y) = -\sum_z p(z|y) \log_2(p(z|y))$  — средняя неопределенность ключа, если известен конкретный шифртекст  $y$ ;

$H(Z|Y) = \sum_y p(y)H(Z|y)$  — средняя неопределенность ключа при известном шифртексте.

*Полной избыточностью* языка называется величина

$$D_X = \log_2 |X| - H(X).$$

**Теорема 12. (Шеннона об избыточности языка.)** Пусть выполняется  $|X| = |Y|$ . Тогда  $H(Z) - H(Z|Y) \leq D_X$ .

Эта теорема говорит о том, что среднее количество информации о ключе, которое содержится в шифртексте не превосходит избыточности языка открытых текстов.

Шифрсистема называется *строгого идеальной*, если  $H(Z) = H(Z|Y)$ . В частности, любая система с нулевой избыточностью языка открытых текстов,  $D_X = 0$ , является строгого идеальной.

**Задача 427.** Покажите, что

- 1)  $H(X|Y) \leq H(X);$
- 2)  $H(Z|Y) \leq H(Z);$
- 3)  $H(Y, Z) = H(Y) + H(Z|Y);$
- 4)  $H(X, Z) = H(X) + H(Z).$

**Задача 428.** Докажите, что  $H(Z|Y) = H(X) + H(Z) - H(Y)$ .

**Задача 429.** Докажите теорему Шеннона об избыточности языка.

**Задача 430.** Верно ли, что любая совершенно секретная шифрсистема является строго идеальной?

**Задача 431.** Верно ли, что если шифрсистема строго идеальна, то она и совершенно секретная?

**Задача 432.** Пусть шифрсистема определена так:  $X = Y = Z = \{0, 1\}$ ,  $y = E(x, z) = x \oplus z$ . При каких значениях  $p(x)$ ,  $p(z)$  шифрсистема может быть строго идеальной, но не совершенно секретной? А совершенно секретной, но не строго идеальной?

**Задача 433. (\*)** Приведите пример строго идеальной шифрсистемы с ненулевой полной избыточностью  $D_X$ .

Есть другой подход к измерению избыточности языка — на букву сообщения. Пусть  $A$  — некоторый алфавит,  $|A| = k$ . Пусть  $L \subset A^*$  — язык в этом алфавите.

*Энтропия языка на букву сообщения* определяется как

$$H_L = - \sum_{x \in L} \frac{1}{|x|} p(x) \log p(x),$$

где  $|x|$  — длина слова  $x$  (т. е. число букв в нём). Энтропия  $H_L$  приближается с помощью величин  $H(L_n)/n$ , где  $L_n$  — множество всех  $n$ -грамм (слов длины  $n$ ), встречающихся в словах языка  $L$ . А именно  $H_L = \lim_{n \rightarrow \infty} H(L_n)/n$ . При этом удобно полагать  $H_0 = \log_2 k$ . Величины  $H(L_n)$  находятся по формуле

$$H(L_n) = - \sum_{x \in L_n} p(x) \log_2 p(x),$$

где  $p(x)$  приближается частотой  $n$ -грамм  $x$  в языке  $L$ .

*Полная избыточность языка на букву сообщения* — это

$$B_L = \log_2 k - H_L.$$

*Относительная избыточность языка* определяется как

$$R_L = B_L / \log_2 k.$$

Например, относительная избыточность русского языка равна 0,73, английского — 0,75. Помните задачи 2, 3 на эту тему?

**Задача 434. (\*\*) Избыточность.** Проведите исследование избыточности естественных языков, таких как испанский, итальянский, немецкий и др. Какой из рассмотренных вами языков наименее избыточный?

**Задача 435. Искусственный язык I.** Оцените относительную избыточность искусственного языка  $L$  в алфавите  $A = \{0, 1\}$ , который строится так:

$$L = \{1, 10, 1000, 10000000, \dots, \underbrace{10\dots0}_{2^{n-1} \text{ битов}}\},$$

и все слова его равновероятны.

**Задача 436. Искусственный язык II.** Определите относительную избыточность языка, о котором Вам известно лишь то, что на нём был составлен следующий типичный текст: Кита ита кта та та ки.

**Задача 437. Искусственный язык III.** Определите относительную избыточность языка, на котором был составлен следующий типичный текст:

Арты аты оты рты ты. Ар арты атты отатрты рты ты!

### 9.3 Расстояние единственности шифра

При дешифровании некоторого шифртекста криptoаналитик может прийти к разным вариантам открытого текста. При этом ключи, которые приводят к этим вариантам, в основном ложные (за исключением, может быть, одного). Обозначим через  $s(\ell)$  среднее число ложных ключей для шифртекста длины  $\ell$ .

Какой минимальный объём шифртекста криptoаналитику необходимо получить, чтобы однозначно восстановить по нему исходный открытый текст? Этот объём в среднем, т. е. средняя длина шифртекста, называется *расстоянием единственности* шифра. Расстояние единственности шифра — минимальное  $\ell^*$  такое, что  $s(\ell^*) = 0$ .

Клод Шеннон показал, что расстояние единственности прямо пропорционально длине ключа и обратно пропорционально избыточности исходного открытого текста.

**Теорема 13. (Шеннона о числе ложных ключей).** Пусть все ключи равновероятны, т. е.  $H(Z) = \log_2 |Z|$ . Пусть  $X, Y \subset A^*$  и  $|A| = k$ . Предположим, что шифр сохраняет длину  $|x| = |E(x, z)|$ . Тогда

$$s(\ell) \geq \frac{|Z|}{k^{\ell R_X}} - 1.$$

**Следствие 1.** Справедливо

$$\ell^* = \lceil \frac{\log_2 |Z|}{R_X \cdot \log_2 k} \rceil.$$

**Задача 438. (\*)** Докажите теорему Шеннона о ложных ключах.

**Задача 439.** Докажите формулу для расстояния единственности  $\ell^*$ .

**Задача 440. Расстояние единственности I.** Посчитайте расстояние единственности

- а) шифра простой замены для английского языка;
- б) шифра Цезаря для английского языка. А для русского?
- в) лозунгового шифра с лозунгом длины  $n$  для английского языка;
- г) шифра «одноразовый блокнот».

**Задача 441. (\*\*\*) Расстояние единственности II.** Оцените (или определите точно) расстояния единственности шифров DES, ГОСТ 28147-89, AES и других из известных вам.

# ГЛАВА 10. АНАЛИЗ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

При изложении теории и задач этой главы мы опирались в основном на книги О. А. Логачёва, А. А. Сальникова, В. В. Ященко [17] и М. М. Глухова, В. П. Елизарова, А. А. Нечаева [12].

## 10.1 Линейные рекуррентные последовательности

Изучение свойств линейных рекуррентных последовательностей (ЛРП) — один из необходимых шагов для анализа псевдослучайных генераторов и стойкости поточных шифров. ЛРП вырабатываются так называемыми *регистрами сдвига с линейной обратной связью* (РСЛОС), которые наряду с обобщениями широко используются как компоненты поточных шифров (например, A5/1, Grain) и псевдослучайных генераторов. Они могут порождать последовательности с хорошим минимальным периодом из небольшого числа битов начального состояния, а их обобщения позволяют существенно увеличивать линейную сложность выходной последовательности.

Пусть  $\{u_i\}$ ,  $i = 0, 1, 2, \dots$ ,  $u_i \in \mathbb{Z}_2$  — бесконечная *двоичная* последовательность. Обозначим через  $\{u_i\} \oplus \{v_i\}$  последовательность  $\{u_i \oplus v_i\}$ , через  $\{0\}$  — нулевую последовательность  $0, 0, 0, \dots$ . Будем рассматривать только двоичные последовательности, хотя многие теоремы могут быть несложно перенесены на случай последовательностей над произвольным конечным полем.

Бесконечная последовательность  $\{u_i\}$  называется *линейной рекуррентной*, если для некоторых  $a_0, \dots, a_{n-1} \in \mathbb{Z}_2$  верно

$$u_{i+n} = a_0 u_i \oplus \dots \oplus a_{n-1} u_{i+n-1} \text{ для всех } i \geq 0.$$

Это выражение называют *линейным рекуррентным соотношением порядка  $n$* .

**Задача 442.** Докажите, что одна и та же ЛРП может быть задана линейными рекуррентными соотношениями различных порядков.

Многочлен  $g(x) = x^n \oplus a_{n-1}x^{n-1} \oplus \dots \oplus a_1x \oplus a_0$  называется *характеристическим многочленом* последовательности  $\{u_i\}$ . Минимальный многочлен — это характеристический многочлен минимальной степени. Он обозначается через  $M(x)$  или  $M_u(x)$ . *Линейной сложностью* ЛРП называется степень её минимального многочлена, которую обозначим через  $\ell_u$ .

**Задача 443.** Докажите, что минимальный многочлен ЛРП определен однозначно.

Пусть  $x^k$  — операторы сдвига последовательности  $\{u_i\}$ , где  $k$  — целое:

$$x^k\{u_i\} = \{u_{i+k}\} = u_k, u_{k+1}, u_{k+2}, \dots$$

Определим умножение последовательности  $\{u_i\}$  на многочлен  $p(x) = a_nx^n \oplus \dots \oplus a_1x \oplus a_0$  как линейное отображение пространства последовательностей:

$$p(x)\{u_i\} = a_n(x^n\{u_i\}) \oplus \dots \oplus a_1(x\{u_i\}) \oplus a_0\{u_i\},$$

где  $c\{u_i\} = \{cu_i\}$  для  $c \in \mathbb{Z}_2$ .

**Задача 444.** Докажите, что

$$((a_nx^n \oplus \dots \oplus a_1x \oplus a_0)\{u_i\})_i = a_0u_i \oplus \dots \oplus a_nu_{i+n}.$$

**Задача 445.** Докажите, что ненулевой многочлен  $g(x)$  характеристический для ЛРП  $\{u_i\}$  тогда и только тогда, когда  $g(x)\{u_i\} = \{0\}$ .

**Задача 446.** Докажите, что минимальный многочлен ЛРП делит любой её характеристический многочлен.

## 10.2 Минимальный период ЛРП

Последовательность  $\{u_i\}$  называется *периодической*, если для некоторых натуральных  $T$  и  $s$  верно  $u_{i+T} = u_i$ ,  $i$  — целое,  $i \geq s$ , и *строго периода*, если  $s = 0$ . Число  $T$  называется *периодом* последовательности. Минимальный возможный период называется *минимальным периодом* и обозначается через  $per_u$ .

**Задача 447.** Докажите, что минимальный период периодической последовательности делит любой её период.

**Задача 448.** Найдите минимальный период последовательности, состоящей из знаков после запятой двоичного представления дроби  $7/13$ .

**Задача 449.** Пусть  $p/q$  — несократимая дробь, где  $p, q > 1$ ,  $p < q$ . Докажите, что период последовательности, состоящей из знаков после запятой двоичной записи этой дроби, не превосходит значения функции Мёбиуса  $\varphi(q)$ . Верно ли, что первые  $\varphi(q)$  элементов однозначно определяют всю последовательность?

**Задача 450.** Докажите, что любая ЛРП  $\{u_i\}$  является периодической и  $\text{per}_u \leq 2^{\ell_u} - 1$ .

**Задача 451.** Докажите, что последовательность является периодической тогда и только тогда, когда она является ЛРП.

**Задача 452.** Докажите, что если для ЛРП  $\{u_i\}$  верно  $\text{per}_u = 2^{\ell_u} - 1$ , то  $\{u_i\}$  является строго периодической.

**Задача 453.** Докажите, что если если  $M(x)$  — минимальный многочлен ЛРП  $\{u_i\}$ , то

$$\text{per}_u = \min_{t \in \mathbb{N}} \{t : M(x) \mid x^s(x^t \oplus 1), s \in \mathbb{N}\}.$$

Неприводимый полином  $g(x)$  с коэффициентами из  $GF(2)$  называется *примитивным*, если

$$\min_{t \in \mathbb{N}} \{t : g \mid x^t \oplus 1\} = 2^{\deg g} - 1$$

Согласно задачам 452 и 453 ЛРП  $\{u_i\}$  имеет  $\text{per}_u = 2^{\ell_u} - 1$  тогда и только тогда, когда её минимальный многочлен является примитивным.

Заметим, что существуют примитивные полиномы любой степени, большей чем 1. Из задачи 453 видно, что период ЛРП однозначно определяется её минимальным многочленом. Также заметим, что понятие линейной сложности имеет смысл для любой периодической последовательности (см. задачу 451).

### 10.3 Алгоритм Берлекэмпа — Мэсси

Назовём  $\{u_i\}^N = u_0, u_1, \dots, u_{N-1}$  конечной двоичной последовательностью длины  $N$ . Если  $\{u_i\}^N$  и  $\{u_i\}$  используются вместе, то полагаем, что  $\{u_i\}^N$  является началом бесконечной последовательности  $\{u_i\}$ . Многочлен порождает  $\{u_i\}^N$ , если он — характеристический многочлен некоторой ЛРП, начало которой совпадает с  $\{u_i\}^N$ .

**Лемма 3.** Пусть  $\{u_i\}^N$  — ЛРП. Многочлен  $g(x)$  степени меньшей, чем  $N$ , порождает  $\{u_i\}^N$  тогда и только тогда, когда

$$g(x)\{u_i\} = \underbrace{0, \dots, 0}_k, 1, *, \dots, \quad N \leq k + \deg g(x).$$

Другими словами, первые  $N - \deg g(x)$  элементов последовательности  $g(x)\{u_i\}$  должны быть нулями.

Минимальным многочленом конечной последовательности называется любой многочлен минимальной степени, который её порождает. Степень такого многочлена называется её линейной сложностью. Минимальный многочлен конечной последовательности  $\{u_i\}^N$  обозначается через  $M_u^N$ , её линейная сложность — через  $\ell_u^N$ . Очевидно, что минимальный многочлен конечной последовательности всегда существует.

**Задача 454.** Докажите лемму 3.

**Задача 455.** Приведите пример конечных последовательностей, которые имеют несколько минимальных многочленов.

Найти минимальный многочлен конечной (или, при некоторых условиях, бесконечной) последовательности можно с помощью алгоритма Берлекэмпа — Мэсси. Существует много вариантов этого алгоритма.

**Вход:**  $\{u_i\}^N = u_0, u_1, \dots, u_{N-1}$  — конечная ненулевая последовательность.

**Выход:** семейство многочленов  $G_n(x), n = 0, \dots, N - 1$ , таких что  $G_n(x)$  — минимальный многочлен последовательности  $\{u_i\}^{n+1}$ . Для удобства изложения включим в семейство многочлен  $G_{-1}(x)$ .

**Алгоритм:**

1. Пусть  $n_0$  — номер первого ненулевого бита  $\{u_i\}^N$ . Тогда

- $G_{-1}(x) = G_0(x) = \dots = G_{n_0-1}(x) = 1;$
- $G_{n_0}(x) = x^{n_0+1} \oplus 1.$

2. Пусть  $G_{-1}(x), G_0(x), \dots, G_{n-1}(x)$  уже построены;

- если  $G_{n-1}$  порождает  $\{u_i\}^{n+1}$  то  $G_n(x) = G_{n-1}(x);$   
 $G_{n-1}(x) = c_0 \oplus \dots \oplus c_k x^k, c_k \neq 0,$  порождает  $\{u_i\}^{n+1} \iff$

$$c_0 u_{n-k} \oplus c_1 u_{n-k+1} \oplus \dots \oplus c_k u_n = 0.$$

- иначе пусть  $m$  — последний номер, когда  $\deg G_m$  менялась:

$$\deg G_{m-1} < \deg G_m = \deg G_{m+1} = \dots = \deg G_{n-1} \implies$$

$$a = m - \deg G_{m-1} \quad b = n - \deg G_{n-1};$$

- a) если  $a \geq b$  то  $G_n(x) = G_{n-1}(x) \oplus x^{a-b} G_{m-1}(x);$
- б) если  $a < b$  то  $G_n(x) = x^{b-a} G_{n-1}(x) \oplus G_{m-1}(x).$

3.  $G_n$  построен; если  $n < N - 1$ , перейти на шаг 2.

**Теорема 14.** Для  $n = 0, \dots, N - 1$  многочлен  $G_n$  является минимальным многочленом  $\{u_i\}^{n+1}.$

**Следствие 2.** Пусть  $n = 1, \dots, N - 1$ . Тогда если  $G_{n-1} \neq G_n$ , то

$$\deg G_n = \max\{\deg G_{n-1}, n + 1 - \deg G_{n-1}\}.$$

**Следствие 3.** Пусть  $\{u_i\}$  — ЛРП линейной сложности  $\ell$ . Тогда алгоритм Берлекэмпа — Мэсси восстановит минимальный многочлен  $\{u_i\}$  по  $\{u_i\}^{2\ell}.$

Таким образом, если  $\{u_i\}^N$  имеет линейную сложность  $\ell$ , то алгоритм Берлекэмпа — Мэсси имеет сложность  $O(N\ell)$ . Если  $\ell$  заранее известно, то —  $O(\ell^2)$ .

**Задача 456.** Докажите теорему 14.

**Задача 457.** (\*) Докажите следствия 2, 3.

**Задача 458.** Докажите, что существует бесконечное семейство конечных последовательностей, таких что сложность алгоритма Берлекэмпа — Мэсси для последовательности длины  $N$  будет  $O(N^2)$ .

**Задача 459. Линейная сложность и период.** Докажите, что для строго периодической ЛРП  $\{u_i\}$  верно  $\ell_u \leqslant \text{per}_u$ . Приведите пример строго периодических последовательностей, для которых  $\ell_u = \text{per}_u$ , в случае произвольной линейной сложности  $\ell_u$ .

**Задача 460.** Определите минимальные многочлены последовательностей, начала которых имеют вид:

- а) 00000...01 ( $n$  первых подряд идущих нулей);
- б) 1010;
- в) 101011110;
- г) 1010111100010011010.

**Задача 461. «Красивые» последовательности.** С помощью алгоритма Берлекэмпа — Мэсси найдите минимальные многочлены следующих конечных последовательностей:

- а) 110111011011001 (первые знаки двоичного представления  $\sqrt{3}$ );
- б) 101101010000010 (первые знаки двоичного представления  $\sqrt{2}$ );
- в) 110011110001101 (первые знаки двоичного представления  $\frac{1+\sqrt{5}}{2}$ );
- г) 110010010000111 (первые знаки двоичного представления  $\pi$ );
- д) 10110111110000 (первые знаки двоичного представления  $e$ ).

**Задача 462.** С помощью алгоритма Берлекэмпа — Мэсси восстановите минимальный многочлен бесконечной последовательности  $\{u_i\} = 0, 1, 1, 0, 1, 1, 0, 1, 1, \dots$  периода 3.

**Задача 463.** С помощью алгоритма Берлекэмпа — Мэсси восстановите минимальный многочлен бесконечной последовательности  $\{u_i\} = 1, 0, 1, 1, \dots$  периода 4.

**Задача 464.** Найдите минимальные многочлены следующих конечных последовательностей:

- а) 01011011011011;

- б) 011011101110111011;
- в) 1001001001011001001011001;
- г) 01011011101111011101111011101111.

**Задача 465.** Определите минимальные многочлены следующих конечных последовательностей длины 15:

- а) 011001011010001;
- б) 000111111100110;
- в) 111010110001001;
- г) 001001010000100.

**Задача 466. Линейная сложность: свойства.** Докажите следующие свойства линейной сложности конечных последовательностей.

1.  $0 \leq \ell_u^N \leq N$ .
2.  $\ell_u^N = 0 \iff \{u_i\}^N = \underbrace{0, \dots, 0}_N$ .
3.  $\ell_u^N = N \iff \{u_i\}^N = \underbrace{0, \dots, 0}_{N-1}, 1$ .
4.  $\ell_{u \oplus v}^N \leq \ell_u^N + \ell_v^N$ .
5. Если  $\ell_u^{N-1} \neq \ell_u^N$ , то  $\ell_u^N = N - \ell_u^{N-1}$ .

**Задача 467.** Приведите примеры конечных последовательностей длины  $N$ , имеющих линейную сложность  $N - 1$ ,  $N - 2$ ,  $N - 3$ .

**Задача 468.** Предложите алгоритм, генерирующий конечную последовательность длины  $N$  и линейной сложностью  $\ell$  для заданных  $N$  и  $\ell$ ,  $0 \leq \ell \leq N$ .

**Задача 469.** Предложите алгоритм, генерирующий последовательность  $\{u_i\}$  такую что  $\ell_u^N \geq \lceil \frac{N}{2} \rceil$  для всех натуральных  $N$ . Возможно ли, что  $\ell_u^N > \lceil \frac{N}{2} \rceil$  для любого  $N$ ?

# ГЛАВА 11. БУЛЕВЫ ФУНКЦИИ

Булевы функции являются неотъемлемой частью криптографических систем, поскольку реализуют преобразования битов открытого текста. В данной главе рассматриваются основные понятия теории булевых функций.

Некоторые задачи этой главы взяты из книг О. А. Логачёва, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [17], [18], В. М. Фомичёва [34], Г. П. Гаврилова и А. А. Сапоженко [11], Ф. Дж. Мак-Вильямса и Н. Дж. А. Слоэна [19], а также из пособия [33].

## 11.1 Булев куб. Метрика Хэмминга

Одними из важных объектов дискретной математики являются графы. *Графом*  $G$  называется пара множеств  $(V, E)$ , где  $V$  — множество вершин,  $E$  — множество рёбер, т. е. некоторое подмножество неупорядоченных пар вершин.

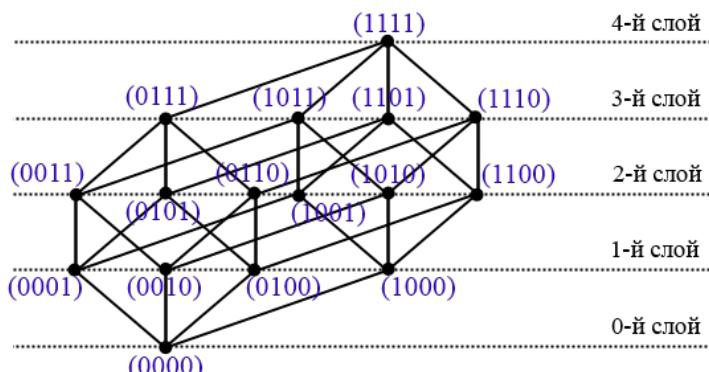
*Булевым кубом размерности*  $n$  называется граф, у которого множество вершин состоит из всех  $n$ -мерных двоичных векторов, т. е.

$$V = \{x = (x_1, \dots, x_n) \mid x_i \in \mathbb{Z}_2\},$$

а рёбрами соединяются такие вершины, которые различаются ровно в одной координате, т. е.

$$E = \{(x, y) \mid x, y \in V \text{ и существует единственный } j, \text{ что } x_j \neq y_j\}.$$

Обозначим такой граф через  $E^n$ . Наглядный пример графа  $E^4$ , отражающий его структуру, приведён на рисунке ниже:



Для любого вектора  $x \in E^n$  определяется его *вес Хэмминга*  $wt(x) = \sum_{i=1}^n x_i$  как число ненулевых координат. В булевом кубе  $E^n$  подмножество вершин  $\{x \mid wt(x) = k\}$  называется *k-м слоем*, где  $k$  — целое число от 0 до  $n$ .

Для любых векторов  $x$  и  $y$  определяется вектор их суммы  $x \oplus y = (x_1 \oplus y_1, \dots, x_n \oplus y_n)$ , где  $\oplus$  — сложение по модулю 2. *Расстоянием Хэмминга* между векторами  $x$  и  $y$  называется число координат, в которых они различаются,  $d(x, y) = wt(x \oplus y)$ .

На множестве вершин определяется *отношение предшествования*:  $x \preceq y$ , если для всех  $i$  выполнено  $x_i \leq y_i$ . Если к тому же  $x \neq y$ , то предшествование *строгое*, оно обозначается  $x \prec y$ .

*Скалярным произведением* векторов  $x$  и  $y$  из  $E^n$  называется число  $\langle x, y \rangle = x_1y_1 + x_2y_2 + \dots + x_ny_n$ . Два вектора  $x$  и  $y$  *ортогональны*, если  $\langle x, y \rangle = 0$ .

**Задача 470.** Проверьте, что расстояние Хэмминга определяет метрику, т. е. удовлетворяет следующим аксиомам:

- 1)  $d(x, y) = 0 \iff x = y$ ;
- 2)  $d(x, y) = d(y, x)$ ;
- 3)  $d(x, z) \leq d(x, y) + d(y, z)$ .

**Задача 471.** Определите количество вершин в булевом кубе  $E^n$ .

**Задача 472.** Определите число вершин в  $k$ -м слое булева куба  $E^n$ .

**Задача 473.** Найдите число ребер в  $E^n$ . Чему равно число пар векторов  $x, y \in E^n$  таких, что  $d(x, y) = k$ ?

**Задача 474.** Пусть  $n$  — чётное. Сколькими способами можно выбрать вектор булева куба  $E^n$  так, чтобы в первой половине его координат содержалось ровно  $k$  единиц, а во второй — ровно  $\ell$  единиц?

**Задача 475.** Определите, чему равно число векторов булева куба  $E^n$  таких, что в каждом из них никакие две единицы не стоят рядом. А если три единицы?

**Задача 476.** Найдите мощности сферы  $S_r(x) = \{y : d(x, y) = r\}$  и шара  $B_r(x) = \{y : d(x, y) \leq r\}$  радиуса  $r$  в  $n$ -мерном булевом кубе.

**Задача 477.** Пусть  $x, y$  — векторы булева куба  $E^n$  такие, что  $d(x, y) = m$ . Определите количество векторов  $z$ , для которых:

- а)  $d(x, z) + d(z, y) = d(x, y)$ ;
- б)  $d(x, z) = k, d(y, z) = r$ ;
- в)  $d(x, z) \leq k, d(y, z) = r$ ;
- г)  $d(x, z) \leq k, d(y, z) \geq r$ .

**Задача 478.** Для фиксированного вектора  $x$  длины  $n$  определите число ортогональных и неортогональных ему векторов.

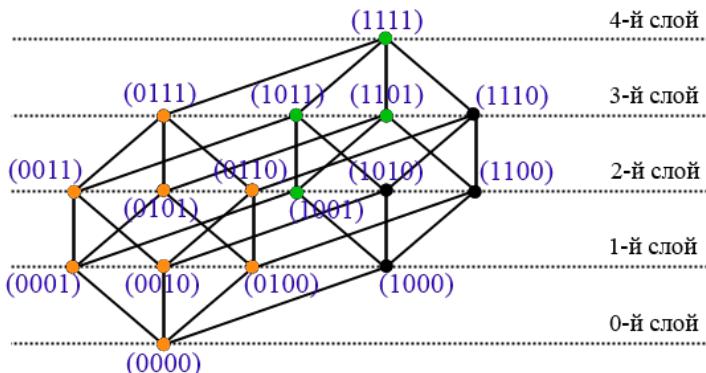
## 11.2 Границы и подпространства

Гранью размерности  $k$  в булевом кубе  $E^n$  называется множество

$$\Gamma_{i_1, \dots, i_{n-k}}^{a_1, \dots, a_{n-k}} = \{x \in E^n \mid x_{i_1} = a_1, \dots, x_{i_{n-k}} = a_{n-k}\}.$$

Множество индексов  $\{i_1, \dots, i_{n-k}\}$  называется *направлением* грани. Число  $n - k$  в данном случае называется *рангом* грани.

На рисунке булева куба  $E^4$  выделены грань  $\Gamma_1^0$  размерности 3 и грань  $\Gamma_{1,4}^{1,1}$  размерности 2:



Линейным подпространством булева куба  $E^n$  называется такое его подмножество  $L$ , что сумма любых двух его элементов  $x$  и  $y$  принадлежит  $L$ . Максимальная по включению система линейно независимых векторов из  $L$  образует базис подпространства; число векторов в базисе называется *размерностью* подпространства и обозначается через  $\dim(L)$ . Аффинным подпространством называется любой смежный класс линейного пространства, т. е. множество вида  $M = z \oplus L$ , где  $z$  — некоторый вектор из  $E^n$ .

**Задача 479.** Найдите мощность произвольной грани размерности  $k$  в булевом кубе  $E^n$ .

**Задача 480.** Чему равно число различных граней в  $E^n$  фиксированного направления  $i_1, \dots, i_{n-k}$ ? Докажите, что такие грани не пересекаются и в объединении дают весь куб  $E^n$ .

**Задача 481.** Определите число всех граней размерности  $k$  в  $E^n$ . Чему равно число всех граней в  $E^n$ ?

**Задача 482.** Чему равно число граней в  $E^n$  размерности  $k$ , содержащих заданную вершину  $x$ ? А заданную грань размерности  $\ell$ ?

**Задача 483.** Докажите, что любое линейное подпространство содержит нулевой вектор.

**Задача 484.** Проверьте, что грань является частным случаем аффинного подпространства булева куба.

**Задача 485.** Пусть  $H$  — некоторое подмножество вершин булева куба  $E^n$  мощности  $2^{n-1}$  такое, что если  $x, y \in H$ , то  $x \oplus y \notin H$ . Докажите, что множество  $E^n \setminus H$  образует линейное подпространство размерности  $n - 1$ .

**Задача 486.** Сколько существует различных базисов у линейного подпространства размерности 3 в булевом кубе  $E^n$ ? А у линейного подпространства размерности  $k$  в  $E^n$ ?

**Задача 487.** Определите количество различных линейных подпространств размерности  $k$  в  $E^n$ .

**Задача 488.** Пусть  $L$  — линейное подпространство размерности  $k$  в  $E^n$ . Пусть  $M$  — матрица, строки которой пробегают все векторы пространства  $L$ . Докажите, что любой столбец матрицы  $M$  состоит либо из всех 0, либо из 0 и 1 в нём одинаково.

**Задача 489.** Пусть  $L$  — линейное подпространство в  $E^n$  такое, что для любого вектора  $x \in L$  выполнено  $wt(x) \leq k$ . Докажите, что в этом случае  $\dim(L) \leq k$ .

### 11.3 Алгебраическая нормальная форма булевой функции

Введём следующие обозначения:

$n$  — некоторое натуральное число;

$\mathbb{Z}_2$  — множество, состоящее из 0 и 1;

$x = (x_1, \dots, x_n)$  — двоичный вектор с координатами из  $\mathbb{Z}_2$ ;

$\mathbb{Z}_2^n$  — множество всех двоичных векторов длины  $n$ ;

$f$  — булева функция от  $n$  переменных, т. е. отображение из множества  $\mathbb{Z}_2^n$  в множество  $\mathbb{Z}_2$ . Важнейшие элементарные булевые функции представлены с помощью таблиц истинности:

| $x$ | $y$ | 0 | 1 | $\bar{x}$ | $x \cdot y$ | $x \vee y$ | $x \oplus y$ | $x \rightarrow y$ | $x   y$ | $x \downarrow y$ |
|-----|-----|---|---|-----------|-------------|------------|--------------|-------------------|---------|------------------|
| 0   | 0   | 0 | 1 | 1         | 0           | 0          | 0            | 1                 | 1       | 1                |
| 0   | 1   | 0 | 1 | 1         | 0           | 1          | 1            | 1                 | 1       | 0                |
| 1   | 0   | 0 | 1 | 0         | 0           | 1          | 1            | 0                 | 1       | 0                |
| 1   | 1   | 0 | 1 | 0         | 1           | 1          | 0            | 1                 | 0       | 0                |

**Задача 490.** Чему равно число булевых функций от  $n$  переменных?

**Задача 491.** Докажите законы дистрибутивности:

- а)  $(x \vee y)z = xz \vee yz$ ;
- б)  $(x \cdot y) \vee z = (x \vee z) \cdot (y \vee z)$ ;
- в)  $(x \oplus y)z = xz \oplus yz$ .

**Задача 492.** Докажите равенства:

- а)  $x\bar{x} = 0$  (закон противоречия);
- б)  $x \vee \bar{x} = 1$  (закон исключённого третьего);
- в)  $\bar{\bar{x}} = x$  (закон снятия двойного отрицания);
- г)  $\overline{x \cdot y} = \bar{x} \vee \bar{y}$ ,  $\overline{x \vee y} = \bar{x} \cdot \bar{y}$  (законы де Моргана).

**Задача 493.** Докажите равенства:

- |                       |                      |
|-----------------------|----------------------|
| а) $x \cdot x = x$ ;  | б) $x \vee x = x$ ;  |
| в) $x \cdot 1 = x$ ;  | г) $x \cdot 0 = 0$ ; |
| д) $x \vee 1 = 1$ ;   | е) $x \vee 0 = x$ ;  |
| ж) $x \oplus x = 0$ ; |                      |

- |   |   |
|---|---|
| и) $\bar{x} = x \oplus 1;$                | к) $x \vee y = xy \oplus x \oplus y;$               |
| л) $x \rightarrow y = \bar{x} \vee y;$    | м) $x \sim y = \overline{x \oplus y};$              |
| н) $x \oplus y = \bar{x}y \vee x\bar{y};$ | о) $x \oplus y = (\bar{x} \vee \bar{y})(x \vee y);$ |
| п) $x y = \overline{xy};$                 | п) $x \downarrow y = \overline{x \vee y};$          |

Одно из возможных представлений булевой функции — это её представление с помощью операций умножения и сложения по модулю 2, а также констант 0 и 1, в следующем виде:

$$f(x_1, \dots, x_n) = \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \dots x_{i_k} \oplus a_0,$$

где  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$  и  $a_{i_1, \dots, i_k}, a_0 \in \mathbb{Z}_2$ . Такое представление единственно и называется *алгебраической нормальной формой* (АНФ) или *полиномом Жегалкина* булевой функции

Булева функция от  $n$  переменных

$$\ell_{a,a_0}(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$$

называется *аффинной*; в случае  $a_0 = 0$  функция *линейна*.

Определим операцию возведения в степень булевой переменной  $z$ :

$$z^\delta = \begin{cases} z, & \text{если } \delta = 1; \\ 1, & \text{если } \delta = 0. \end{cases}$$

Используя эту операцию, АНФ булевой функции можно представить в следующем виде:

$$f(x_1, \dots, x_n) = \sum_{a \in \mathbb{Z}_2^n} g(a_1, \dots, a_n) x_1^{a_1} \dots x_n^{a_n},$$

где  $g$  — некоторая булева функция от  $n$  переменных. При этом значения функции  $g$  вычисляются следующим образом:

$$g(a) = \sum_{x \leq a} f(x).$$

*Преобразованием Мёбиуса* называется отображение  $\mu$ , которое со-поставляет каждой булевой функции  $f$  соответствующую булеву функцию  $g$ , т. е.  $\mu : f \rightarrow g$ .

**Задача 494.** Докажите единственность представления любой булевой функции в виде АНФ.

**Задача 495.** Восстановите АНФ булевой функции по вектору её значений. Считаем, что значения  $f(x)$  выписаны в порядке лексикографического возрастания вектора  $x$ .

- а) (10011101);    б) (11001100);    в) (10000001).

**Задача 496.** Представьте следующие функции в АНФ:

- |  |   |
|--|---|
| а) $f(x_1, x_2) = x_1 \sim x_2;$               | б) $f(x_1, x_2) = x_1   x_2;$                               |
| в) $f(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3;$ | г) $f(x_1, x_2, x_3) = (x_1 \sim x_2) \sim x_3;$            |
| д) $f(x_1, x_2, x_3) = x_1 x_2 x_3;$           | е) $f(x_1, x_2, x_3) = (x_1 \vee x_2) x_3 \rightarrow x_2;$ |

**Задача 497.** Преобразование Мёбиуса. Докажите формулу для вычисления преобразования Мёбиуса булевой функции  $f$ , а именно:  $g(a) = \sum_{x \leq a} f(x)$ .

**Задача 498. Обратимость преобразования Мёбиуса.** Докажите, что преобразование Мёбиуса обратно самому себе,  $\mu(\mu(f)) = f$ .

## 11.4 Характеристики булевой функции

Булевой функции  $f$  от  $n$  переменных можно однозначно сопоставить подмножество векторов булева куба  $E^n$ , на которых функция  $f$  принимает значение 1. Это подмножество называется *носителем функции* и обозначается  $\text{supp}(f) = \{x \in \mathbb{Z}_2^n \mid f(x) = 1\}$ .

Аналогично расстоянию Хэмминга в булевом кубе определяется расстояние Хэмминга между любыми двумя булевыми функциями  $f$  и  $g$  от  $n$  переменных:

$$\text{dist}(f, g) = |\{x \in \mathbb{Z}_2^n \mid f(x) \neq g(x)\}|.$$

Расстояние Хэмминга от функции  $f$  от  $n$  переменных до произвольного множества  $\mathcal{M}_n$  булевых функций от  $n$  переменных определяется как  $\text{dist}(f, \mathcal{M}_n) = \min \{\text{dist}(f, g) \mid g \in \mathcal{M}_n\}$ .

Приведём некоторые числовые характеристики булевой функции.

1. *Вес*  $\text{wt}(f)$  булевой функции  $f$  — это число единиц в векторе её значений, т. е.  $\text{wt}(f) = |\text{supp}(f)|$ .

2. Алгебраическая степень  $\deg(f)$  булевой функции  $f$  — число переменных в самом длинном слагаемом АНФ функции  $f$ , коэффициент при котором равен единице. Для краткости  $\deg(f)$  называют *степенью* функции  $f$ .

3. Нелинейность  $N_f$  булевой функции  $f$  от  $n$  переменных — это расстояние Хэмминга от  $f$  до множества  $\mathcal{A}_n$  всех аффинных функций от  $n$  переменных, т. е.  $N_f = \text{dist}(f, \mathcal{A}_n)$ .

Для любой булевой функции  $f$  и любого вектора  $a \in \mathbb{Z}_2^n$  определяется булева функция  $D_a f(x) = f(x) \oplus f(x \oplus a)$ , которая называется *производной функции  $f$  по направлению  $a$* .

Переменная  $x_i$  называется *существенной* для булевой функции  $f$  от  $n$  переменных, если существует такой двоичный набор значений  $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$ , что

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n).$$

В противном случае переменная  $x_i$  называется *фиктивной* (несущественной) для функции  $f$ .

**Задача 499.** Определите вес булевой функции  $f$  от  $n$  переменных:

- |   |  |
|---|--|
| а) $f(x) = 0;$                              | б) $f(x) = 1;$                               |
| в) $f(x) = x_1;$                            | г) $f(x) = x_2;$                             |
| д) $f(x) = x_1 x_2;$                        | е) $f(x) = x_1 x_2 \oplus x_1;$              |
| ж) $f(x) = x_1 \dots x_k, 2 \leq k \leq n;$ | з) $f(x) = g(x) \oplus 1, \text{wt}(g) = w.$ |

**Задача 500.** Определите вес произвольной аффинной булевой функции  $\ell_{a,a_0}$  от  $n$  переменных.

**Задача 501.** Существуют ли булевые функции от  $n$  переменных веса  $2^{n-1}$ , отличные от аффинных?

**Задача 502.** Пусть  $f$  — булева функция от  $n$  переменных, а  $g$  — булева функция от  $n + 1$  переменных, причём  $g(x_1, \dots, x_{n-1}, y_1, y_2) = f(x_1, \dots, x_{n-1}, y_1 \oplus y_2)$ . Докажите, что  $\text{wt}(g) = 2\text{wt}(f)$ .

**Задача 503.** Упростите выражение и найдите степень функции:

- а)  $x_1 x_2 (x_1 x_2 x_3 \oplus x_1) \oplus x_3 (x_1 x_2 \oplus 1);$
- б)  $(x_1 x_2 \oplus x_3 x_4 \oplus x_1)(x_1 \oplus x_3)(x_2 \oplus x_4);$
- в)  $x_1 (x_1 x_2 x_3 \oplus x_2 x_3 \oplus x_1 \oplus 1);$
- г)  $x_1 (x_2 x_3 x_4 \oplus x_2 x_3 \oplus x_1 \oplus 1).$

**Задача 504.** Определите число линейных и аффинных булевых функций от  $n$  переменных. Сколько существует булевых функций от  $n$  переменных степени не выше  $k$ ?

**Задача 505.** Покажите, что булева функция  $f$  является линейной тогда и только тогда, когда  $f(x \oplus y) = f(x) \oplus f(y)$  для любых  $x, y$ . Аналогично проверьте, что функция является аффинной тогда и только тогда, когда  $f(x \oplus y) = f(x) \oplus f(y) \oplus f(0)$ .

**Задача 506.** Докажите, что если  $\deg(f) = k > 0$ , то  $\text{wt}(f) \geq 2^{n-k}$ .

**Задача 507.** Докажите, что вес булевой функции от  $n$  переменных нечётный тогда и только тогда, когда её степень равна  $n$ .

**Задача 508. (\*\*\*) Нерешённая [17].** Можно ли выделить множество мономов в АНФ булевой функции, которое будет «отвечать» за делимость веса булевой функции на  $2^k$ ,  $k = 2, 3, 4, \dots$ ?

**Задача 509.** Вычислите производную  $D_b f$  булевой функции  $f$  по направлению  $b$ , если

- а)  $f(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3$ ,  $b = (111)$ ;
- б)  $f(x_1, x_2) = x_1 \sim x_2$ ,  $b = (11)$ ;
- в)  $f(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4 \oplus x_1$ ,  $b = (1000)$ .

**Задача 510. Производные.** Верно ли, что набор производных  $D_b f$  по всем направлениям  $b \in \mathbb{Z}_2^n$  однозначно определяет булеву функцию  $f$  от  $n$  переменных?

**Задача 511. Существенная переменная.** Докажите, что любая переменная булевой функции  $f$  является существенной тогда и только тогда, когда она входит в АНФ функции  $f$ .

**Задача 512. (\*) Функции, существенно зависящие от всех переменных.** Найдите число  $T_n$  булевых функций от  $n$  переменных, существенно зависящих от всех своих переменных. Найдите предел отношения  $|T_n|/|P_n|$  при  $n \rightarrow \infty$ , где  $P_n$  — все булевые функции от  $n$  переменных.

**Задача 513. Свойства степеней.** Покажите, что для булевой функции  $f$  от  $n$  переменных и её преобразования Мёбиуса справедливо  $\deg(f) + \deg(\mu(f)) \geq n$ .

## 11.5 Спектр Уолша — Адамара

Помимо числовых параметров булевой функции, рассмотренных в предыдущем разделе, одной из важных её характеристик является спектр Уолша — Адамара. Он заслуживает отдельного изучения в силу своего широкого применения в исследовании различных свойств булевых функций.

Для каждого  $y \in \mathbb{Z}_2^n$  коэффициентом Уолша — Адамара  $W_f(y)$  булевой функции  $f$  от  $n$  переменных называется величина, определяемая равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}.$$

Набор коэффициентов  $W_f(y)$  по всем  $y \in \mathbb{Z}_2^n$  называется *спектром Уолша — Адамара* булевой функции  $f$ . При этом считаем, что векторы  $y$  перебираются в лексикографическом порядке.

**Задача 514.** Найдите спектр Уолша — Адамара функции:

- а)  $f(x_1, x_2) = x_1 x_2$ ;
- б)  $f(x_1, x_2, x_3) = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_3 \oplus 1$ ;
- в)  $f(x_1, \dots, x_n) = \langle a, x \rangle \oplus a_0$ , где  $a \in \mathbb{Z}_2^n$ ,  $a_0 \in \mathbb{Z}_2$ .

**Задача 515. Равенство Парсеваля.** Докажите, что для любой булевой функции  $f$  от  $n$  переменных справедливо равенство

$$\sum_{y \in \mathbb{Z}_2^n} (W_f(y))^2 = 2^{2n}.$$

**Задача 516.** Определите нижнюю достижимую оценку максимума модуля всех коэффициентов  $W_f(y)$ ,  $y \in \mathbb{Z}_2^n$ , для произвольной булевой функции  $f$  от  $n$  переменных.

**Задача 517.** Докажите, что коэффициенты Уолша — Адамара любой булевой функции всегда чётны.

**Задача 518.** (\*) Соотношения ортогональности. Пусть задана некоторая целочисленная функция  $W : \mathbb{Z}_2^n \rightarrow \mathbb{Z}$ . Докажите, что булева функция  $f$  от  $n$  переменных такая, что  $W_f(y) = W(y)$  для любого  $y \in \mathbb{Z}$ , существует тогда и только тогда, когда значения функции  $W$  удовлетворяют соотношениям ортогональности:

$$\sum_{y \in \mathbb{Z}_2^n} W(y)W(y \oplus z) = \begin{cases} 0, & \text{при } z \neq 0, \\ 2^{2n}, & \text{при } z = 0. \end{cases}$$

**Задача 519.** Является ли следующий набор чисел спектром Уолша — Адамара некоторой булевой функции:

- |                     |                    |                     |
|---------------------|--------------------|---------------------|
| а) $(0, 0, 0, 4);$  | б) $(0, 2, 2, 0);$ | в) $(0, 2, 0, -2);$ |
| г) $(2, -2, 2, 2);$ | д) $(2, 2, 2, 2);$ | е) $(0, 1, -2, 4)?$ |

**Задача 520.** Докажите, что справедливо равенство:

$$\sum_{y \in S} W_f(y) = 2^{\dim(S)} \sum_{y \in S^\perp} (-1)^{f(y)},$$

где  $S$  — произвольное линейное подпространство  $E^n$ , а  $S^\perp$  — ортогональное к нему, т. е.  $S^\perp = \{y \in E^n \mid \langle x, y \rangle = 0 \text{ для всех } x \in S\}$ .

**Задача 521.** (\*) Пусть функция  $g$  получена преобразованием Мёбиуса булевой функции  $f$  от  $n$  переменных. Докажите, что верно следующее равенство:

$$g(a) = \left( 2^{wt(a)-1} - 2^{wt(a)-n-1} \sum_{b \preceq a \oplus 1} W_f(b) \right) \bmod 2.$$

**Задача 522.** Пусть  $f$  — булева функция от  $n$  переменных. Докажите, что если  $W_f(y) = 0 \pmod{2^k}$  для любого  $y \in \mathbb{Z}_2^n$ , то  $\deg(f) \leq n - k + 1$ .

**Задача 523.** Определите АНФ булевой функции по её спектру Уолша — Адамара:

- |                     |                      |                     |
|---------------------|----------------------|---------------------|
| а) $(2, -2, 2, 2);$ | б) $(2, 2, -2, -2);$ | в) $(-2, 2, 2, 2).$ |
|---------------------|----------------------|---------------------|

**Задача 524. Формула обращения.** Покажите, что верна формула обращения:

$$(-1)^{f(x)} = 2^{-n} \sum_{y \in \mathbb{Z}_2^n} W_f(y) (-1)^{\langle x, y \rangle}.$$

**Задача 525.** Пусть  $h$  — булева функция от  $n + m$  переменных и  $h(x, y) = f(x) \oplus g(y)$ , где  $f$  и  $g$  — булевы функции от  $n$  и  $m$  непересекающихся переменных соответственно. Докажите, что  $W_h(u, v) = W_f(u)W_g(v)$  для всех  $u \in \mathbb{Z}_2^n$  и  $v \in \mathbb{Z}_2^m$ .

**Задача 526. (\*) Тождество Саркара.** Докажите следующее равенство для любого  $b \in \mathbb{Z}_2^n$  и любой булевой функции  $f$  от  $n$  переменных:

$$\sum_{a \in \mathbb{Z}_2^n, a \leq b} W_f(a) = 2^n - 2^{wt(b)+1} wt(f^b),$$

где  $f^b$  — подфункция  $f$ , полученная фиксацией значения 0 для тех переменных, которые в векторе  $b$  равны 1.

## 11.6 Классификация булевых функций

Важную часть исследований булевых функций составляет какая-либо их классификация. Благодаря ей можно разделить всё множество булевых функций на подмножества — классы эквивалентности, функции в которых обладают некоторыми общими свойствами. Изучать представителей классов эквивалентности, как правило, существенно легче, чем работать со всем множеством булевых функций.

Пусть  $G$  — некоторая группа преобразований  $\mathbb{Z}_2^n$ . Две булевые функции  $f$  и  $g$  называются *эквивалентными относительно группы*  $G$ , если в группе  $G$  найдется преобразование  $\pi$  такое, что выполнено равенство  $f(x) = g(\pi(x))$ .

Перечислим основные группы преобразований переменных булевой функции:

1.  $S_n$  — группа перестановок переменных, состоящая из элементов:

$$\pi = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{j_1} & x_{j_2} & \dots & x_{j_n} \end{pmatrix},$$

где  $j_1, \dots, j_n$  — перестановка элементов  $1, \dots, n$ . Булевы функции, совпадающие с точностью до перестановки переменных, называются *перестановочно эквивалентными*.

2.  $\Sigma_n$  — группа сдвигов переменных, состоящая из элементов:

$$\pi = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_1 \oplus a_1 & x_2 \oplus a_2 & \dots & x_n \oplus a_n \end{pmatrix},$$

где  $(a_1, \dots, a_n)$  — вектор из  $\mathbb{Z}_2^n$ .

3.  $Q_n$  — группа геометрической эквивалентности, являющаяся произведением групп  $S_n$  и  $\Sigma_n$ , т. е. состоит из элементов:

$$\pi = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{j_1} \oplus a_1 & x_{j_2} \oplus a_2 & \dots & x_{j_n} \oplus a_n \end{pmatrix},$$

где  $j_1, \dots, j_n$  — перестановка элементов  $1, \dots, n$ ;  $(a_1, \dots, a_n) \in \mathbb{Z}_2^n$ .

4.  $GL_n(2)$  — полная линейная группа, состоящая из преобразований, заданных невырожденной матрицей  $A$  размера  $n \times n$  с элементами из множества  $\mathbb{Z}_2$ :

$$\pi(x) = A \cdot x.$$

5.  $GA_n(2)$  — полная аффинная группа; её элементы определяются невырожденной матрицей  $A$  размера  $n \times n$  с элементами из множества  $\mathbb{Z}_2$  и вектором  $b \in \mathbb{Z}_2^n$ :

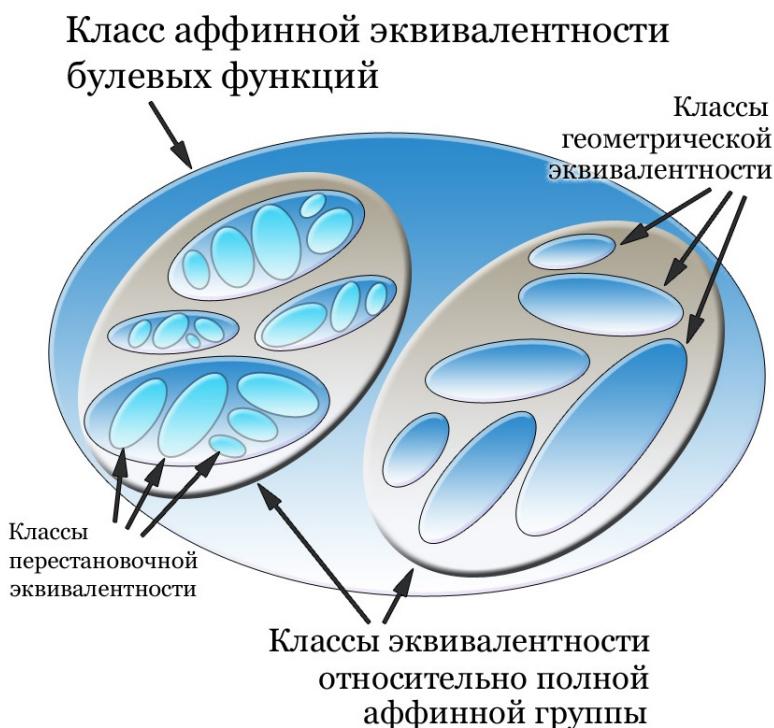
$$\pi(x) = A \cdot x \oplus b.$$

6. С помощью полной аффинной группы определяется основной тип эквивалентности булевых функций — аффинная эквивалентность. Булевы функции  $f$  и  $g$  от  $n$  переменных называются *аффинно эквивалентными*, если существует невырожденная матрица  $A$  размера  $n \times n$  с элементами из множества  $\mathbb{Z}_2$ , векторы  $b, c \in \mathbb{Z}_2^n$  и константа  $d \in \mathbb{Z}_2$  такие, что

$$f(x) = g(A \cdot x \oplus b) \oplus c \cdot x \oplus d.$$

Заметим, что некоторые введённые эквивалентности можно упорядочить. Будем говорить, что одно отношение эквивалентности  $R$  сильнее другого отношения эквивалентности  $r$ , если из того, что две функции эквивалентны относительно  $R$  следует, что они эквивалентны и относительно  $r$ . Если про отношения нельзя сказать, что одно сильнее другого, то будем говорить, что отношения *не сравнимы*.

Так, в приведённом ряду некоторые отношения эквивалентности сравнимы между собой. Например, перестановочная эквивалентность, геометрическая эквивалентность, эквивалентность относительно полной аффинной группы и аффинная эквивалентность. Эти отношения перечислены, начиная с самой сильной эквивалентности, что отражает и рисунок ниже.



**Задача 527.** Докажите, что если булевы функции  $f$  и  $g$  перестановочно эквивалентны, то они эквивалентны и геометрически. Покажите, что обратное неверно.

**Задача 528.** Докажите, что если булевы функции  $f$  и  $g$  эквивалентны относительно группы сдвигов переменных, то они и геометрически эквивалентны. Верно ли обратное?

**Задача 529.** Покажите, что перестановочная эквивалентность и эквивалентность относительно группы сдвигов не сравнимы.

**Задача 530.** Докажите, что если булевые функции  $f$  и  $g$  геометрически эквивалентны, то они эквивалентны и относительно полной аффинной группы. Верно ли обратное?

**Задача 531.** Докажите, что если булевые функции  $f$  и  $g$  эквивалентны относительно полной аффинной группы, то они и аффинно эквивалентны. Приведите пример, подтверждающий, что обратное неверно.

**Задача 532.** Покажите, что геометрическая эквивалентность и эквивалентность относительно полной линейной группы не сравнимы.

**Задача 533.** Докажите, что если булевые функции  $f$  и  $g$  эквивалентны относительно полной линейной группы, то они эквивалентны и относительно полной аффинной группы. Верно ли обратное?

**Задача 534.** Определите число элементов в группах  $S_n$ ,  $\Sigma_n$  и  $Q_n$ .

**Задача 535.** Докажите, что  $|GL_n| = \prod_{i=0}^{n-1} (2^n - 2^i)$ .

**Задача 536.** Докажите, что  $|GA_n| = 2^n \prod_{i=0}^{n-1} (2^n - 2^i)$ .

**Задача 537. (\*)** Докажите, что при достаточно больших  $n$  справедливо приближение  $\prod_{i=0}^{n-1} (2^n - 2^i) \approx 0.29 \cdot 2^{n^2}$ .

**Задача 538.** Определите, являются ли следующие функции перестановочно эквивалентными. Если — да, найдите соответствующие перестановки переменных:

- а)  $f(x) = x_1x_2 \oplus x_1x_4 \oplus x_2x_3$ ,  $g(x) = x_1x_3 \oplus x_2x_3 \oplus x_2x_4$ ;
- б)  $f(x) = x_1x_2 \oplus x_1x_4 \oplus x_2x_3$ ,  $g(x) = x_1x_2 \oplus x_1x_4 \oplus x_3x_4$ ;
- в)  $f(x) = x_1x_2 \oplus x_1x_4 \oplus x_2x_3$ ,  $g(x) = x_1x_2 \oplus x_1x_4 \oplus x_2x_4$ ;
- г)  $f(x) = x_1x_3x_4 \oplus x_2x_3x_5 \oplus x_1x_2x_5 \oplus x_1x_3 \oplus x_2x_4$ ,  
 $g(x) = x_1x_3x_5 \oplus x_2x_3x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_1x_4$ ;
- д)  $f(x) = x_1 \cdot \dots \cdot x_n$ ,  $g(x) = x_n \cdot \dots \cdot x_1 \oplus 1$ .

**Задача 539. Поясковые функции.** Булева функция  $f$  называется *поясковой*, если она совпадает с любой перестановочно эквивалентной ей булевой функцией. Другими словами, если для любой перестановки переменных  $\pi$  выполняется равенство  $f(x) = f(\pi(x))$  при

всех  $x \in \mathbb{Z}_2^n$ . Опишите все поисковые функции от  $n$  переменных. Чему равно их число?

**Задача 540.** Эквивалентны ли данные булевые функции относительно какой-либо из групп  $S_3$ ,  $\Sigma_3$ ,  $Q_3$ ,  $GL_3$ ,  $GA_3$ :

- а)  $x_1x_2 \oplus x_3$  и  $x_1x_2 \vee x_3$ ;
- б)  $x_1x_2 \vee x_1x_3$  и  $x_1x_2 \oplus x_1x_3 \oplus x_3$ ;
- в)  $x_1 \vee x_2$  и  $x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3$ ;
- г)  $x_1x_2 \vee x_1\overline{x_2}$  и  $x_1 \oplus x_2 \oplus x_3$ ?

**Задача 541.** Верно ли, что все аффинные функции от  $n$  переменных аффинно эквивалентны друг другу?

**Задача 542.** Постройте аффинную классификацию булевых функций от двух переменных. Сколько классов эквивалентности она содержит?

**Задача 543. (\*\* Квадратичные функции I.** Докажите, что множество всех булевых функций степени не выше 2 разбивается на классы эквивалентности относительно полной аффинной группы со следующими представителями: 0, 1,  $x_1$ , а также

$$\bigoplus_{i=1}^s x_{2i-1}x_{2i}, \quad \bigoplus_{i=1}^s x_{2i-1}x_{2i} \oplus 1, \quad \bigoplus_{i=1}^s x_{2i-1}x_{2i} \oplus x_{2s+1},$$

при  $s = 1, 2, \dots, \lfloor n/2 \rfloor$ . Найдите число классов эквивалентности.

**Задача 544. (\*\* Квадратичные функции II.** Докажите, что множество всех булевых функций степени не выше 2 разбивается на  $\lfloor n/2 \rfloor + 1$  классов аффинной эквивалентности, представителями которых являются следующие функции:

| №                         | представитель  |
|---------------------------|--|
| 1                         | 0  |
| 2                         | $x_1x_2$   |
| 3                         | $x_1x_2 \oplus x_3x_4$   |
| 4                         | $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$   |
| 5                         | $x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$   |
| ...                       | ...  |
| $\lfloor n/2 \rfloor + 1$ | $x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n$ (если $n$ чётно), либо<br>$x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-2}x_{n-1}$ (если $n$ нечётно) |

**Задача 545.** Пусть булевые функции  $f$  и  $g$  эквивалентны относительно одной из групп  $S_n$ ,  $\Sigma_n$ ,  $Q_n$ ,  $GL_n$ ,  $GA_n$  или аффинно эквивалентны. Верно ли, что

- а)  $wt(f) = wt(g)$ ;
- б)  $deg(f) = deg(g)$ ;
- в) множества, состоящие из различных значений коэффициентов Уолша — Адамара функций  $f$  и  $g$  совпадают;
- г)  $N_f = N_g$ ?

## 11.7 Трэйс-форма булевой функции

Напомним, что множество  $\mathbb{Z}_2^n$  двоичных векторов длины  $n$  можно рассматривать как конечное поле со специальным образом определёнными операциями сложения и умножения (см. раздел 4.9). При этом каждому вектору  $(c_1, \dots, c_n) \in \mathbb{Z}_2^n$  однозначно соответствует многочлен  $c_1x^{n-1} + c_2x^{n-2} + \dots + c_n$ . Множество  $\mathbb{Z}_2$  также является полем, а именно  $GF(2)$ , состоящим из двух элементов 0 и 1.

Любую булеву функцию от  $n$  переменных  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  можно отождествить с функцией, действующей из  $GF(2^n)$  в  $GF(2)$ . Функцию из  $GF(2^n)$  в  $GF(2)$  для удобства также будем называть булевой.

Напомним, что след  $tr : GF(2^n) \rightarrow GF(2)$  определяется как  $tr(c) = c + c^2 + c^{2^2} + \dots + c^{2^{n-1}}$ . Свойства следа подробно рассматривались в разделе 4.9. Известно, что любую булеву функцию  $f$  от  $n$  переменных можно представить с помощью следа в виде (см. [33]):

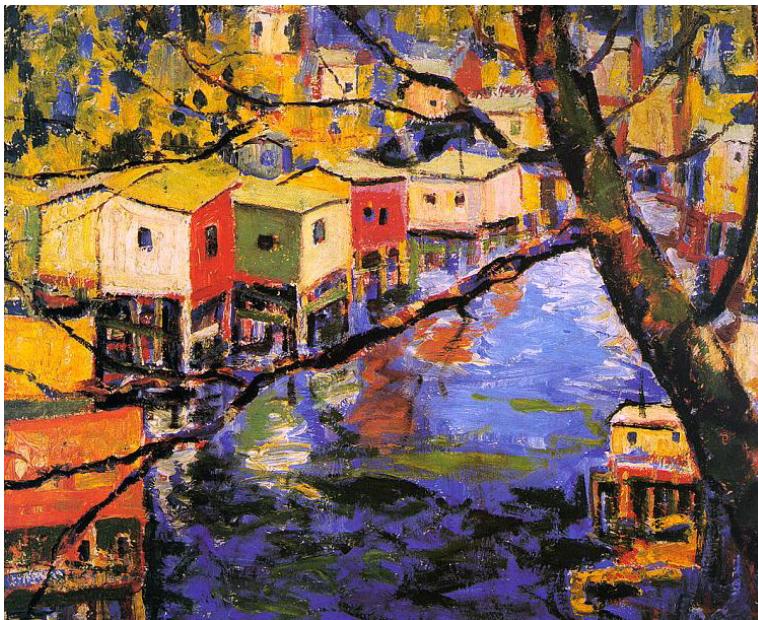
$$f(c) = tr\left(\sum_{j=0}^{2^n-1} a_j c^j\right), \text{ где } a_j \in GF(2^n).$$

При этом считаем, что  $c^0 = 1$  для всех  $c \in GF(2^n)$ . Кроме того,  $c^{2^n-1} = 1$  для любого  $c \in GF^*(2^n)$  и  $c^{2^n-1} = 0$  для  $c = 0$ .

Функция вида  $f(c) = tr(\lambda c^k)$  называется *мономиальной*.

*Циклотомическим классом* по модулю  $2^n - 1$  с представителем  $t$  называется множество  $C(t) = \{2^j t \bmod 2^n - 1 \mid 0 \leq j < n_t\}$ , где  $n_t$  — наименьшее натуральное число такое, что  $2^{n_t}t = t \pmod{2^n - 1}$ . Обозначим через  $CS$  множество наименьших представителей всех циклотомических классов по модулю  $2^n - 1$ .

**Задача 546.** Найдите все циклотомические классы по модулю  $2^n - 1$  при  $n = 3, 4, 5$ .



Селдон Коннор Гил. Arks Along the Lagoon

**Задача 547.** Докажите свойства циклотомического класса по модулю  $2^n - 1$ :

- для любого числа  $t$  мощность  $n_t$  циклотомического класса  $C(t)$  является делителем числа  $n$ , т. е.  $n_t|n$ ;
- для любого числа  $s$  из циклотомического класса с представителем  $t$  выполняется:  $tr(c^s) = tr(c^t)$ .

**Задача 548. Трейс-форма булевой функции.** Докажите, что любую булеву функцию от  $n$  переменных можно представить с помощью следа в виде:

$$f(c) = \operatorname{tr}\left(\sum_{j \in CS} a_j c^j\right) + \operatorname{tr}(a_{2^n-1} c^{2^n-1}), \text{ где } a_j \in GF(2^n).$$

Данное представление для функции  $f$  называется её *трейс-формой*.

**Задача 549.** Верно ли, что каждой булевой функции соответствует ровно одна трейс-форма? Если да, то почему? Если нет, то приведите пример.

**Задача 550. Линейные функции.** Докажите, что множество функций вида  $f(c) = \text{tr}(\lambda c)$ , когда  $\lambda$  пробегает всё поле  $GF(2^n)$ , совпадает с множеством всех линейных функций от  $n$  переменных.

**Задача 551. (\*) Степень мономиальной функции.** Докажите, что алгебраическая степень мономиальной функции  $f(c) = \text{tr}(\lambda c^k)$  равна двоичному весу числа  $k$ , где число  $k$  строго меньше, чем  $2^n - 1$ , и мощность циклотомического класса  $C(k)$  равна  $n$ . Что будет, если мощность  $C(k)$  меньше  $n$ ?

**Задача 552. (\*)** Докажите, что булева функция  $f$  от  $n$  переменных, представленная в виде  $f(c) = \text{tr}(\sum_{j \in CS} a_j c^j)$ , тождественно равна нулю тогда и только тогда, когда для всех  $j \in CS$  выполняется  $\text{tr}(a_j c^j) \equiv 0$ .

**Задача 553. (\*)** Докажите, что для любого  $j \in CS$  такого, что мощность циклотомического класса с представителем  $j$  равна  $n$ , т. е.  $|C(j)| = n$ , функция  $f(c) = \text{tr}(a_j c^j)$  от  $n$  переменных не может тождественно равняться константе, если  $a_j \neq 0$ .

**Задача 554. Трейс-форма I.** Пусть поле  $GF(2^3)$  построено с помощью порождающего многочлена  $g(x) = x^3 + x + 1$ . Пусть выбран примитивный элемент  $\alpha = x + 1$ . Найдите алгебраические нормальные формы следующих булевых функций:

- |   |   |
|---|---|
| а) $f(c) = \text{tr}(\alpha^3 c);$  | б) $f(c) = \text{tr}(\alpha^2 c);$                |
| в) $f(c) = \text{tr}(\alpha^5 c^2) + \text{tr}(\alpha);$                  | г) $f(c) = \text{tr}(\alpha c) + \text{tr}(c^3);$ |
| д) $f(c) = \text{tr}(c) + \text{tr}(\alpha^5 c^3) + \text{tr}(\alpha^2).$ |   |

**Задача 555. Трейс-форма II.** Пусть поле  $GF(2^3)$  построено с помощью порождающего многочлена  $g(x) = x^3 + x + 1$  и выбран примитивный элемент  $\alpha = x + 1$ . Найдите трейс-формы булевых функций:

- |  |  |
|--|--|
| а) $f(x_1, x_2, x_3) = 1;$   | б) $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3;$ |
| в) $f(x_1, x_2, x_3) = x_1 x_2 \oplus 1;$  | г) $f(x_1, x_2, x_3) = x_1 x_2 x_3;$               |
| д) $f(x_1, x_2, x_3) = x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_1 \oplus x_2 \oplus x_3.$ |  |

# ГЛАВА 12. КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ

Булевы функции, используемые в криптографических приложениях, должны обладать рядом специальных свойств, чтобы обеспечивать стойкость шифров к различным видам криптоанализа. В данной главе задачи посвящены криптографическим свойствам булевых функций, а также возможности их комбинирования.

При изложении теории и задач этой главы мы опирались в основном на книги О. А. Логачёва, А. А. Сальникова, С. В. Смыслилева, В. В. Ященко [17], [18], В. М. Фомичёва [34], книгу [32] по бент-функциям, пособие [33], книги Т. W. Cusick, P. Stănică [44], Ю. В. Таранникова [31], главы в монографиях С. Carlet [42], [43] и многочисленные научные статьи. В 2014 г. из печати выйдет пособие И. А. Панкратовой [24], целиком посвящённое теме данной главы, — очень рекомендуем его заинтересованному читателю.

## 12.1 Сбалансированность

Булева функция  $f$  от  $n$  переменных называется *сбалансированной* (или *уравновешенной*), если функция принимает значения 0 и 1 одинаково часто. Заметим, что её вес равен  $2^{n-1}$ . В противном случае функция называется *несбалансированной*.

**Задача 556.** Каких булевых функций от одной переменной больше: сбалансированных или несбалансированных? А от двух переменных?

**Задача 557.** Определите число сбалансированных булевых функций от  $n$  переменных.

**Задача 558.** Докажите, что любая аффинная функция, отличная от константы, является сбалансированной.

**Задача 559.** Докажите, что если булева функция линейна по некоторой переменной (т. е. без ограничения общности можно считать, что  $f(x_1, \dots, x_n) = g(x_1, \dots, x_{n-1}) \oplus x_n$ ), то она сбалансирована.

**Задача 560.** Докажите, что булева функция  $f$  от  $n$  переменных является сбалансированной тогда и только тогда, когда  $W_f(0) = 0$ .

**Задача 561.** Пусть  $f(x_1, \dots, x_n)$  и  $g(y_1, \dots, y_m)$  — булевы функции от непересекающихся множеств переменных. Докажите, что:

- а)  $f \cdot g$  несбалансирована, если обе функции  $f$  и  $g$  не константы;
- б)  $f \oplus g$  сбалансирована тогда и только тогда, когда сбалансирована одна из них.

**Задача 562.** Определите, являются ли следующие булевы функции сбалансированными:

- а)  $f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ ;
- б)  $f(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 x_3$ ;
- в)  $f(x_1, x_2, x_3) = x_1 x_2 \oplus x_3 \oplus 1$ ;
- г)  $f(x_1, \dots, x_n) = x_1 x_2 \oplus x_{n-1} x_n$ , где  $n$  — четное;
- д)  $f(c) = \text{tr}(c)$ , где  $c$  пробегает  $GF(2^n)$ ;
- е)  $f$  такая, что  $D_a f(x_1, x_2, x_3) = x_1 x_2 \oplus 1$ , где  $a = (001)$ .

## 12.2 Устойчивость и корреляционная иммунность

Подфункцией булевой функции  $f$  от переменных  $x_1, \dots, x_n$  называется булева функция, полученная из  $f$  подстановкой вместо переменных  $x_{i_1}, \dots, x_{i_k}$  конкретных констант  $a_{i_1}, \dots, a_{i_k}$ , принимающих значения 0 или 1. Такая подфункция обозначается  $f_{i_1, \dots, i_k}^{a_1, \dots, a_k}$ .

Булева функция  $f$  называется  $r$ -устойчивой, если любая её подфункция, полученная фиксацией не более  $r$  переменных, является сбалансированной. Наибольшее такое число  $r$  называется порядком устойчивости функции. Нетрудно заметить, что  $0 \leq r \leq n - 1$ .

Булева функция  $f$  называется корреляционно-иммунной порядка  $r$ , если вес её любой подфункции  $f_{i_1, \dots, i_r}^{a_1, \dots, a_r}$  удовлетворяет соотношению:

$$\text{wt}(f_{i_1, \dots, i_r}^{a_1, \dots, a_r}) = \frac{\text{wt}(f)}{2^r}$$

для любого набора индексов  $1 \leq i_1 < \dots < i_r \leq n$  и любых констант  $a_{i_1}, \dots, a_{i_r} \in \mathbb{Z}_2$ . Другими словами, булева функция  $f$  корреляционно-иммунна порядка  $k$ , если для всех подфункций  $f_{i_1, \dots, i_r}^{a_1, \dots, a_r}$  выполнено:

$Pr(f = 1) = Pr(f_{i_1, \dots, i_k}^{a_1, \dots, a_k} = 1)$ , где  $Pr$  — функция вероятности. Наибольшее такое  $k$  называется *порядком корреляционной иммунности* функции, обозначается  $CI(f)$ . Нетрудно заметить, что  $0 \leq CI(f) \leq n$ .

**Задача 563.** Постройте таблицы истинности всех булевых функций от одной переменной и покажите, что:

- а) все функции являются 0-устойчивыми;
- б) две функции имеют порядок корреляционной иммунности равный 0, а две — 1. Определите их вид.

**Задача 564.** По приведённому ниже набору таблиц истинности всех булевых функций  $f_1, \dots, f_{16}$  от двух переменных определите для каждой функции порядок её устойчивости и корреляционной иммунности. Найдите АНФ функций с ненулевыми порядками устойчивости и корреляционной иммунности.

| $x_1$ | $x_2$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ | $f_{11}$ | $f_{12}$ | $f_{13}$ | $f_{14}$ | $f_{15}$ | $f_{16}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|
| 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 1     | 1     | 1        | 1        | 1        | 1        | 1        | 1        |          |
| 0     | 1     | 0     | 0     | 0     | 0     | 1     | 1     | 1     | 0     | 0     | 0        | 0        | 1        | 1        | 1        | 1        |          |
| 1     | 0     | 0     | 0     | 1     | 1     | 0     | 0     | 1     | 1     | 0     | 0        | 1        | 0        | 0        | 1        | 1        |          |
| 1     | 1     | 0     | 1     | 0     | 1     | 0     | 1     | 0     | 1     | 0     | 1        | 0        | 1        | 0        | 1        | 1        |          |

**Задача 565.** Покажите, что порядки корреляционной иммунности функций  $f$  и  $f \oplus 1$  совпадают. Что можно сказать о порядках устойчивости этих функций?

**Задача 566.** Докажите, что корреляционно-иммунная порядка  $r$  булева функция является также и корреляционно-иммунной порядка  $k$  для всех  $k$  меньших  $r$ .

**Задача 567.** Докажите, что булева функция  $f$  является  $r$ -устойчивой тогда и только тогда, когда она сбалансирована и корреляционно-иммунна порядка  $r$ .

**Задача 568. (\*)** Докажите, что булева функция  $f$  является корреляционно-иммунной порядка  $r$  тогда и только тогда, когда  $W_f(y) = 0$  для всех векторов  $y$  таких, что  $1 \leq wt(y) \leq r$ .

**Задача 569.** Докажите, что любая булева функция от  $n$  переменных степени  $n$  имеет порядок корреляционной иммунности равный нулю.

**Задача 570. Теорема Зигенталера I.** Докажите, что если  $f$  — корреляционно-иммунная порядка  $r$ , то выполняется  $\deg(f) + r \leq n$ .

**Задача 571. Теорема Зигенталера II.** Докажите, что если  $f$  —  $r$ -устойчивая и  $r \leq n - 2$ , то выполняется  $\deg(f) + r \leq n - 1$ .

**Задача 572. (\*) Теорема Фон-дер-Флаасса.** Пусть  $f$  — несбалансированная корреляционно-иммунная функция порядка  $r$ , отличная от константы. Докажите, что  $r \leq (2n/3) - 1$ .

**Задача 573.** Докажите следующие свойства булевой функции  $f$  от  $n$  переменных:

- а) если  $f$  — корреляционно-иммунна порядка  $r$ ,  $r \leq n - 1$ , то  $2^{r+1}$  делит  $W_f(y)$  при всех  $y \in \mathbb{Z}_2^n$ ;
- б) если  $f$  —  $r$ -устойчивая,  $r \leq n - 2$ , то  $2^{r+2}$  делит  $W_f(y)$  при всех  $y \in \mathbb{Z}_2^n$ .

**Задача 574. (\*)** Пусть функция  $f$  от  $n$  переменных является корреляционно-иммунной порядка  $r = n - k$  для подходящего числа  $k$ . Пусть  $g$  — булева функция от  $n + 1$  переменных такая, что  $g(x_1, \dots, x_n, y) = f(x_1, \dots, x_n) \oplus y$ . Докажите, что порядок корреляционной иммунности функции  $g$  равен  $r + 1$ , т. е. разница между числом переменных и порядком корреляционной иммунности у функций  $f$  и  $g$  одинаковая, в данном случае равная  $k$ .

### 12.3 Алгебраическая иммунность

Пусть задана булева функция  $f$  от  $n$  переменных. Булева функция  $g$  от  $n$  переменных называется *аннулятором* функции  $f$ , если выполнено равенство  $f \cdot g = 0$ . Обозначим множество всех аннуляторов функции  $f$  через

$$An(f) = \{g \mid f(x) \cdot g(x) = 0 \text{ для всех } x \in \mathbb{Z}_2^n\}.$$

*Алгебраической иммунностью*  $AI(f)$  функции  $f$  называется такое наименьшее число  $d$ , что существует аннулятор  $g$  степени  $d$ , не тождественно равный нулю, либо для функции  $f$ , либо для  $f \oplus 1$ .

**Задача 575.** Найдите все аннуляторы следующих булевых функций:

- |                              |                              |
|------------------------------|------------------------------|
| а) $f(x_1, \dots, x_n) = 0;$ | б) $f(x_1, \dots, x_n) = 1;$ |
| в) $f(x_1, x_2) = x_1;$      | г) $f(x_1, x_2) = x_1 x_2.$  |

**Задача 576.** Определите число аннуляторов для каждой булевой функции от трёх переменных, заданной своим набором значений:

- |                        |                        |
|------------------------|------------------------|
| а) $f = (0000\ 0000);$ | б) $f = (0000\ 0001);$ |
| в) $f = (0000\ 1000);$ | г) $f = (1100\ 0000);$ |
| д) $f = (0011\ 1100);$ | е) $f = (1111\ 0011);$ |
| ж) $f = (1111\ 1110);$ | з) $f = (1111\ 1111);$ |

**Задача 577.** Пусть  $\pi$  — произвольная перестановка  $n$  координат. Докажите, что булевы функции  $f(x)$  и  $f(\pi(x))$  от  $n$  переменных имеют равные по мощности множества аннуляторов.

**Задача 578. Число аннуляторов булевой функции.** Для произвольной функции  $f$  от  $n$  переменных определите мощность множества  $An(f)$  всех аннуляторов функции  $f$ .

**Задача 579.** Найдите значение алгебраической иммунности и вид аннулятора для произвольной аффинной функции

$$\ell_{a,a_0}(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n.$$

**Задача 580.** Докажите, что для любых булевых функций  $f$  и  $g$  от  $n$  переменных верны следующие свойства:

- а) если  $f \cdot g = h$ , то  $h$  — аннулятор функции  $f \oplus 1$ ;
- б)  $AI(f) \leqslant \deg(f)$ ;
- в)  $AI(f \cdot g) \leqslant AI(f) + AI(g)$ ;
- г)  $AI(f \oplus g) \leqslant AI(f) + AI(g)$ ;
- д)  $AI(f) - 1 \leqslant AI(f \oplus \ell_{a,a_0}) \leqslant AI(f) + 1$  для любой аффинной функции  $\ell_{a,a_0}$  от  $n$  переменных;
- е)  $AI(f) = AI(g)$ , если  $g$  получена из  $f$  аффинным преобразованием переменных, а именно  $g(x) = f(Ax \oplus b)$ , где  $A$  — невырожденная матрица порядка  $n$  из нулей и единиц,  $b$  — произвольный двоичный вектор длины  $n$ .

**Задача 581.** Определите значение  $AI(f)$  для следующих функций  $f$ :

- а)  $f(x_1, x_2, x_3, x_4) = x_1x_2x_4 \oplus x_1x_2 \oplus 1$ ;
- б)  $f(x_1, \dots, x_6) = x_1x_2 \oplus x_3x_4x_5x_6$ ;
- в)  $f(x_1, \dots, x_n) = 0$ ;
- г)  $f(x_1, \dots, x_n) = 1$ ;
- д)  $f(x_1, \dots, x_n) = x_1 \dots x_k$ , где  $k = 1, 2, \dots, n$ ;
- е)  $f(x_1, \dots, x_n) = x_1x_2 \oplus \dots \oplus x_{n-1}x_n$  (все попарные произведения).

Найдите в каждом случае вид ненулевого аннулятора наименьшей степени для  $f$  или  $f \oplus 1$ .

**Задача 582. (\*) Оценка алгебраической иммунности.** Докажите, что для произвольной булевой функции  $f$  от  $n$  переменных верна следующая оценка на значение алгебраической иммунности:  $AI(f) \leq \lceil n/2 \rceil$ , где  $\lceil k \rceil$  — целая часть сверху от числа  $k$ .

**Задача 583.** Приведите пример булевой функции  $f$  с наименьшим числом переменных такой, что  $AI(f) = d$ , где  $d$  — некоторое целое число.

**Задача 584. (\*)** Докажите, что следующие функции от  $n$  переменных имеют максимальную алгебраическую иммунность  $\lceil n/2 \rceil$ :

- а) для нечётного  $n$ :  $f(x) = \begin{cases} 0, & \text{если } wt(x) < \lceil n/2 \rceil; \\ 1, & \text{если } wt(x) \geq \lceil n/2 \rceil. \end{cases}$
- б) для чётного  $n$ :  $f(x) = \begin{cases} 0, & \text{если } wt(x) < n/2; \\ b \in \{0, 1\}, & \text{если } wt(x) = n/2; \\ 1, & \text{если } wt(x) > n/2. \end{cases}$

## 12.4 Высокая нелинейность

*Нелинейностью* булевой функции  $f$  от  $n$  переменных называется величина  $N_f$ , равная расстоянию Хэмминга от  $f$  до множества  $\mathcal{A}_n$  всех аффинных функций от  $n$  переменных, т. е.  $N_f = dist(f, \mathcal{A}_n)$ . Например, определим нелинейность булевой функции от трёх переменных, заданной набором своих значений  $f = (0101\ 0000)$ . Считаем, что значения приводятся в лексикографическом порядке возрастания аргументов, т. е.  $f(000) = 0$ ,  $f(001) = 1$  и т. д. Для начала выпишем

наборы значений всех линейных булевых функций от трёх переменных:

| $x_1$ | $x_2$ | $x_3$ | 0 | $x_1$ | $x_2$ | $x_3$ | $x_1 \oplus x_2$ | $x_1 \oplus x_3$ | $x_2 \oplus x_3$ | $x_1 \oplus x_2 \oplus x_3$ |
|-------|-------|-------|---|-------|-------|-------|------------------|------------------|------------------|-----------------------------|
| 0     | 0     | 0     | 0 | 0     | 0     | 0     | 0                | 0                | 0                | 0                           |
| 0     | 0     | 1     | 0 | 0     | 1     | 0     | 1                | 1                | 1                | 1                           |
| 0     | 1     | 0     | 0 | 1     | 0     | 1     | 0                | 0                | 1                | 1                           |
| 0     | 1     | 1     | 0 | 1     | 1     | 1     | 1                | 1                | 0                | 0                           |
| 1     | 0     | 0     | 1 | 0     | 0     | 1     | 1                | 0                | 0                | 1                           |
| 1     | 0     | 1     | 1 | 0     | 1     | 1     | 0                | 1                | 1                | 0                           |
| 1     | 1     | 0     | 1 | 1     | 0     | 0     | 1                | 0                | 1                | 0                           |
| 1     | 1     | 1     | 1 | 1     | 1     | 0     | 0                | 1                | 0                | 1                           |

Множество  $\mathcal{A}_3$  состоит из всех линейных функций и их отрицаний,  $|\mathcal{A}_3| = 16$ . Далее определим минимальное расстояние от функции  $f$  до множества  $\mathcal{A}_3$ . Заметим, что оно равно двум и достигается, например, между функцией  $f$  и  $x_1 \oplus x_3$ . Таким образом,  $N_f = 2$ .

Булева функция называется *максимально нелинейной*, если её величина нелинейности достигает своей верхней оценки. В случае чётного  $n$  максимально нелинейная булева функция называется *бент-функцией*.

**Задача 585.** Докажите, что для любой булевой функции  $f$  нелинейности функций  $f$  и  $f \oplus 1$  совпадают, т. е.  $N_f = N_{f \oplus 1}$ .

**Задача 586.** Определите нелинейность следующих функций:

- |  |   |
|--|---|
| а) $f(x_1, x_2) = x_1 \oplus 1$ ;            | б) $f(x_1, x_2) = x_1 x_2 \oplus x_2 \oplus 1$ ;              |
| в) $f(x_1, x_2, x_3) = x_1 x_3 \oplus x_2$ ; | г) $f(x_1, x_2, x_3) = x_1 x_2 x_3 \oplus x_2 x_3 \oplus 1$ . |

**Задача 587.** Пусть  $f$  и  $g$  — булевые функции соответственно от  $n$  и  $m$  переменных. Докажите, что для нелинейности функции  $h(x, y) = f(x) \oplus g(y)$ , где  $x \in \mathbb{Z}_2^n$ ,  $y \in \mathbb{Z}_2^m$ , справедлива оценка

$$N_h \geq 2^m N_f + 2^n N_g - 2N_f N_g.$$

**Задача 588. Формула для нелинейности.** Докажите, что нелинейность произвольной булевой функции  $f$  от  $n$  переменных вычисляется по формуле:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{y \in \mathbb{Z}_2^n} |W_f(y)|.$$

**Задача 589. Максимальная нелинейность ( $n$  чётное).** В случае чётного  $n$  докажите, что максимально возможное значение  $N_f$  нелинейности булевой функции  $f$  от  $n$  переменных равно  $2^{n-1} - 2^{n/2-1}$ .

**Задача 590.** Определите, являются ли следующие булевые функции бент-функциями:

- а)  $f(x_1, x_2) = x_1x_2 \oplus 1$ ;
- б)  $f(x_1, x_2, x_3, x_4) = x_1x_4 \oplus x_2x_3 \oplus x_3 \oplus 1$ ;
- в)  $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3$ .

**Задача 591.** Докажите, что любая бент-функция существенно зависит от каждой своей переменной.

**Задача 592. (\*) Итеративная конструкция.** Докажите, что булева функция  $f(x', x'') = g(x') \oplus h(x'')$ , где векторы  $x'$ ,  $x''$  имеют чётные длины  $r$ ,  $k$  соответственно, является бент-функцией тогда и только тогда, когда функции  $g$ ,  $h$  — бент-функции.

**Задача 593. (\*) Конструкция Мэйорана — МакФарланда.** Пусть  $h$  — любая перестановка на множестве  $\mathbb{Z}_2^{n/2}$ , пусть  $g$  — произвольная булева функция от  $n/2$  переменных. Докажите, что функция  $f(x', x'') = \langle x', h(x'') \rangle \oplus g(x'')$  является бент-функцией от  $n$  переменных.

**Задача 594. Свойства бент-функций МакФарланда. (\*)** Докажите, что любая бент-функция от  $n$  переменных из класса Мэйорана — МакФарланда представима в виде суммы двух бент-функций от  $n$  переменных.

**Задача 595. (\*) Свойство производной.** Докажите, что булева функция  $f$  от  $n$  переменных является бент-функцией тогда и только тогда, когда каждая её производная  $D_y f$  по ненулевому направлению  $y$  сбалансирована.

**Задача 596. (\*) Степень бент-функции.** Докажите, что алгебраическая степень  $\deg(f)$  любой бент-функции  $f$  от  $n$  переменных,  $n \geq 4$ , не превосходит  $n/2$ .



Джорджо де Кирико. Меланхолия и тайна улицы

**Задача 597. Дуальная функция I.** Для любой бент-функции  $f$  от  $n$  переменных можно определить *дуальную функцию*  $\tilde{f}$ , которая отвечает за знак коэффициентов Уолша — Адамара функции  $f$ , т. е.  $(-1)^{\tilde{f}(y)} 2^{n/2} = W_f(y)$  для всех  $y \in \mathbb{Z}_2^n$ . Докажите, что  $\tilde{f}$  также является бент-функцией. Покажите, что  $\tilde{\tilde{f}} = f$ .

**Задача 598. Дуальная функция II.** Докажите, что степени бент-функции  $f$  от  $n$  переменных и дуальной к ней  $\tilde{f}$  удовлетворяют соотношению:

$$n/2 - \deg(f) \geq \frac{n/2 - \deg(\tilde{f})}{\deg(\tilde{f}) - 1}.$$

**Задача 599. (\*\*)** Докажите, что любая квадратичная бент-функция аффинно эквивалентна функции  $x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n$ .

**Задача 600.** (\*) Докажите, что класс  $\mathcal{B}_n$  бент-функций замкнут относительно любого невырожденного аффинного преобразования переменных, а также прибавления любой аффинной функции.

**Задача 601.** (\*) Найдите все симметрические бент-функции, т. е. такие бент-функции  $f$ , что  $f(x_1, \dots, x_n) = f(\pi(x_1, \dots, x_n))$ , где  $\pi$  — элемент группы  $S_n$  перестановок переменных.

**Задача 602.** Определите, может ли бент-функция быть сбалансированной? Корреляционно-иммунной? Устойчивой?

**Задача 603.** Алгебраическая иммунность бент-функции. Покажите, что алгебраическая иммунность произвольной бент-функции от  $n$  переменных,  $n \geq 4$ , не меньше двух.

**Задача 604.** (\*) Нелинейность и корреляционная иммунность. Докажите, что для нелинейности несбалансированной корреляционно-иммунной порядка  $r$  функции  $f$  от  $n$  переменных,  $r \leq n - 1$ , справедлива оценка  $N_f \leq 2^{n-1} - 2^r$ .

**Задача 605.** (\*) Нелинейность и устойчивость I. Докажите, что для нелинейности  $r$ -устойчивой булевой функции  $f$  от  $n$  переменных,  $r \leq n - 2$ , справедлива оценка  $N_f \leq 2^{n-1} - 2^{r+1}$ .

**Задача 606.** Нелинейность и устойчивость II. Пусть булева функция  $f$  от  $n$  переменных является  $r$ -устойчивой. Докажите, что  $N_f = 2^{n-1} - 2^{r+1}$  тогда и только тогда, когда  $W_f(u) \in \{0, 2^{m+2}, -2^{m+2}\}$  при всех  $u \in \mathbb{Z}_2^n$ .

**Задача 607.** (\*\* Нелинейность и алгебраическая иммунность. Докажите, что верна следующая связь между алгебраической иммунностью булевой функции и нелинейностью:

$$N_f \geq 2 \cdot \sum_{i=0}^{AI(f)-2} C_{n-1}^i.$$

# ГЛАВА 13. ВЕКТОРНЫЕ БУЛЕВЫ ФУНКЦИИ (S-БЛОКИ)

Векторные булевые функции являются неотъемлемой частью блочных шифров. Они реализуют основные преобразования в нелинейных компонентах шифра — S-блоках, от свойств которых существенно зависит стойкость шифра.

Подробнее о векторных булевых функциях, использующихся в криптографии, можно прочитать в главе С. Carlet [43], докторской диссертации Л. Будагян [41], книгах О. А. Логачёва, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [17], [18] и др.

## 13.1 Основные понятия

*Векторной булевой функцией*  $F$  от  $n$  переменных (или *S-блоком*) называется произвольное отображение  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , где  $n, m$  — натуральные числа. Для краткости удобно говорить, что *функция*  $F$  имеет тип  $n \rightarrow m$ . Векторную функцию можно рассматривать как набор из  $m$  координатных булевых функций от  $n$  переменных, т. е.  $F = (f_1, \dots, f_m)$ . Например, векторная функция  $F$  типа  $2 \rightarrow 3$ , заданная следующим образом  $F(00) = (001)$ ,  $F(01) = (111)$ ,  $F(10) = (011)$ ,  $F(11) = (000)$ , имеет три координатные функции:  $f_1 = (0100)$ ,  $f_2 = (0110)$ ,  $f_3 = (1110)$  (функции представлены с помощью векторов значений).

*Компонентной функцией* называется любая линейная комбинация координатных функций, т. е. булева функция  $\langle b, F \rangle$ , где  $b \in \mathbb{Z}_2^m$ . Для нашего примера имеется ровно 8 компонентных функций:  $0$ ,  $f_1$ ,  $f_2$ ,  $f_3$ ,  $f_1 \oplus f_2$ ,  $f_1 \oplus f_3$ ,  $f_2 \oplus f_3$ ,  $f_1 \oplus f_2 \oplus f_3$ .

Для векторной булевой функции (так же как в случае обычных булевых функций) справедливо однозначное представление в виде *алгебраической нормальной формы* (АНФ):

$$F(x_1, \dots, x_n) = \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \dots x_{i_k} \oplus a_0,$$

где  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$  и  $a_{i_1, \dots, i_k}$ ,  $a_0 \in \mathbb{Z}_2^m$ . Для приведённого выше примера такое представление имеет вид  $F(x_1, x_2) = (001) \oplus$

$(010)x_1 \oplus (110)x_2 \oplus (101)x_1x_2$ . Действительно, АНФ векторной булевой функции несложно получить из АНФ её координатных функций. Поскольку в нашем примере  $f_1(x_1, x_2) = x_2 \oplus x_1x_2$ ,  $f_2(x_1, x_2) = x_1 \oplus x_2$ ,  $f_3(x_1, x_2) = 1 \oplus x_1x_2$ , выбираем векторы  $a_0$ ,  $a_1$ ,  $a_2$ ,  $a_{12}$  так, чтобы отразить вхождение каждого монома  $(1, x_1, x_2$  или  $x_1x_2)$  в соответствующую координатную функцию. Имеем:  $a_0 = (001)$ ,  $a_1 = (010)$ ,  $a_2 = (110)$ ,  $a_{12} = (101)$ .

Любую векторную функцию типа  $n \rightarrow m$  удобно представлять с помощью упорядоченного набора длины  $2^n$  со значениями из множества  $\{0, 1, \dots, 2^m - 1\}$ . При этом каждому числу  $r \in \{0, 1, \dots, 2^m - 1\}$  сопоставляется двоичный вектор длины  $m$ , являющийся его двоичным представлением. Векторную функцию  $F$  из рассматриваемого примера можно представить как  $F = (1 \ 7 \ 3 \ 0)$ .

*Степень*  $\deg(F)$  векторной булевой функции определяется аналогично булевому случаю как количество переменных в максимальном по длине слагаемом, при котором коэффициент не равен нулевому вектору. *Спектр Уолша — Адамара* векторной  $n \rightarrow m$  функции состоит из всех коэффициентов Уолша — Адамара всех её компонентных булевых функций:

$$W_F(u, v) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle v, F \rangle \oplus \langle u, x \rangle}, \quad \text{где } u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m.$$

**Задача 608.** Определите, каких векторных булевых функций больше: типа  $2 \rightarrow 3$  или  $3 \rightarrow 2$ .

**Задача 609.** Найдите, чему равно число всех векторных булевых функций из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2^m$ .

**Задача 610.** Определите число взаимно однозначных векторных булевых функций типа  $n \rightarrow m$ .

**Задача 611.** Определите АНФ следующих векторных булевых функций, заданных наборами значений (рядом с набором указывается тип функции):

- а)  $F = (4 \ 7)$ , тип  $1 \rightarrow 3$ ;
- б)  $F = (0 \ 15 \ 3 \ 8)$ , тип  $2 \rightarrow 4$ ;
- в)  $F = (2 \ 3 \ 2 \ 3 \ 4 \ 5 \ 4 \ 5)$ , тип  $3 \rightarrow 3$ ;
- г)  $F = (7 \ 4 \ 0 \ 2 \ 3 \ 5 \ 6 \ 1)$ , тип  $3 \rightarrow 3$ .

**Задача 612.** Покажите, что справедливо эквивалентное определение степени векторной булевой функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ :

$$\deg(F) = \max_{b \in \mathbb{Z}_2^m} \deg(\langle b, F \rangle).$$

Пусть  $F$  — векторная булева функция типа  $n \rightarrow m$ . Для любого  $b \in \mathbb{Z}_2^m$  обозначим множество его прообразов относительно  $F$  через  $F^{-1}(b) = \{x \in \mathbb{Z}_2^n \mid F(x) = b\}$ . Функция  $F$  называется *сбалансированной*, если для любого  $b$  верно  $|F^{-1}(b)| = 2^{n-m}$ .

**Задача 613. Взаимно однозначные функции.** Покажите, что любая  $n \rightarrow n$  функция является взаимно однозначной тогда и только тогда, когда она сбалансирована.

**Задача 614.** Пусть  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . Для любого  $b \in \mathbb{Z}_2^m$  верно:

$$|F^{-1}(b)| = 2^{-m} \sum_{x \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m} (-1)^{\langle v, F(x) \oplus b \rangle}.$$

**Задача 615. Сбалансированная функция.** Докажите, что векторная функция  $F$  типа  $n \rightarrow m$  сбалансирована тогда и только тогда, когда все её компонентные функции  $\langle v, F \rangle$ ,  $v \in \mathbb{Z}_2^m$ ,  $v \neq 0$ , являются сбалансированными.

**Задача 616. (\*)** Пусть  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . Покажите, что верна оценка

$$\sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m} (W_F(u, v))^4 \geq 2^{n+m} (3 \cdot 2^{2n} - 2 \cdot 2^n).$$

## 13.2 Нелинейные функции

Пусть  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  — векторная булева функция. *Нелинейностью*  $N_F$  функции  $F$  называется величина, равная минимуму из нелинейностей компонентных булевых функций функции  $F$  (кроме  $\langle 0, F \rangle$ ):

$$N_F = \min_{v \in \mathbb{Z}_2^m, v \neq 0} N_{\langle v, F \rangle}.$$

Вычислим, например, нелинейность векторной булевой функции  $F = (1 \ 3 \ 2 \ 2)$  типа  $2 \rightarrow 2$ . Выпишем векторы значений всех компонентных функций (кроме  $\langle 0, F \rangle$ ):

| $x_1$ | $x_2$ | $f_1$ | $f_2$ | $f_1 \oplus f_2$ |
|-------|-------|-------|-------|------------------|
| 0     | 0     | 0     | 1     | 1                |
| 0     | 1     | 1     | 1     | 0                |
| 1     | 0     | 1     | 0     | 1                |
| 1     | 1     | 1     | 0     | 1                |

Нетрудно заметить, что функция  $f_2$  аффинная, а именно  $f_2(x_1, x_2) = x_1 \oplus 1$ . Таким образом,  $\text{dist}(f_2, x_1 \oplus 1) = 0$ , и как следствие,  $N_F = 0$ .

**Задача 617.** Докажите, что нелинейность любой векторной булевой функции типа  $2 \rightarrow 2$  равна нулю.

**Задача 618.** Определите нелинейности следующих векторных булевых функций, заданных своими наборами значений:

- а)  $F = (3\ 1\ 0\ 0\ 0\ 0\ 0\ 1)$ , тип  $3 \rightarrow 2$ ;
- б)  $F = (0\ 2\ 5\ 0\ 0\ 7\ 3\ 4)$ , тип  $3 \rightarrow 3$ .

**Задача 619. Формула для нелинейности.** Покажите, что по аналогии с булевым случаем нелинейность векторной функции вычисляется по формуле

$$N_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} |W_F(u, v)|.$$

**Задача 620.** Определите максимально возможное значение нелинейности векторной функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ . Какое условие в данном случае накладывается на компонентные функции?

Векторная функция  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , нелинейность которой равна  $2^{n-1} - 2^{n/2-1}$ , называется *векторной бент-функцией*.

**Задача 621.** Существуют ли векторные бент-функции типа  $2 \rightarrow 2$ ? Типа  $3 \rightarrow 2$ ? А типа  $4 \rightarrow 2$ ? Если да, то приведите примеры.

**Задача 622. (\*) Существование бент-функций.** Докажите, что бент-функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  существуют только при  $m \leq n/2$ .

**Задача 623. (\*) Оценка Сидельникова.** Пусть  $m \geq n-1$  и  $F$  – векторная булева функция типа  $n \rightarrow m$ . Докажите, что справедлива оценка

$$N_F \leqslant 2^{n-1} - \frac{1}{2} \sqrt{3 \cdot 2^n - 2 - 2 \frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}}.$$

Эту оценку также независимо получили F. Chabaud и S. Vaudenay.

**Задача 624. (\*\*\*) Нерешённая.** Предложите нетривиальные оценки нелинейности векторной функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$  в случае, если:

- а)  $n$  нечётное и  $m < n - 1$ ;
- б)  $n$  чётное и  $n/2 < m < n - 1$ .

Максимальное значение нелинейности из оценки Сидельникова (задача 623) в случае  $n = m$  равно  $2^{n-1} - 2^{\frac{n-1}{2}}$ . Векторные функции, нелинейность которых достигает такого значения, называются *AB-функциями* (Almost Bent).

**Задача 625.** Определите, являются ли следующие функции AB-функциями:

- а) каждая из функций типа  $1 \rightarrow 1$ ;
- б)  $F = (1\ 0\ 1\ 3)$ , тип  $2 \rightarrow 2$ ;
- в)  $F = (0\ 0\ 0\ 1\ 0\ 2\ 4\ 7)$ , тип  $3 \rightarrow 3$ ;
- г)  $F = (1\ 7\ 1\ 1\ 4\ 2\ 4\ 6)$ , тип  $3 \rightarrow 3$ ;
- д)  $F = (5\ 2\ 1\ 4\ 7\ 6\ 0\ 3)$ , тип  $3 \rightarrow 3$ .

**Задача 626. (\*) Степень АВ-функций.** Пусть  $F$  — векторная булева функция типа  $n \rightarrow n$  и  $n \geqslant 3$ . Докажите, что если  $F$  является АВ-функцией, то её степень не превосходит величины  $(n + 1)/2$ .

**Задача 627.** Установите, являются ли АВ-функциями следующие взаимно однозначные функции типа  $3 \rightarrow 3$ :

- а)  $F = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7)$ ;
- б)  $F = (0\ 1\ 2\ 4\ 3\ 7\ 5\ 6)$ ;
- в)  $F = (7\ 2\ 3\ 5\ 6\ 1\ 4\ 0)$ ;
- г)  $F = (4\ 5\ 7\ 1\ 2\ 0\ 6\ 3)$ .

### 13.3 Дифференциальны равномерные функции

Ещё одно свойство векторных функций, как установим позже, тесно связанное с нелинейностью, возникло с появлением дифференциального криптоанализа. Рассмотрим уравнение

$$F(x) \oplus F(x \oplus a) = b,$$

где  $F$  — векторная функция из  $\mathbb{Z}_2^n$  в  $\mathbb{Z}_2^n$ ,  $a, b$  — произвольные векторы из  $\mathbb{Z}_2^n$ ,  $a \neq 0$ . Можно считать, например, что функция  $F$  представляет собой преобразование шифра при некотором неизвестном ключе. Уравнение выше означает тогда, что, если мы возьмём пару открытых текстов, являющихся решениями уравнения и отличающихся на вектор  $a$ , то на выходе получим пару шифртекстов, отличающихся на вектор  $b$ . Если для некоторых  $a$  и  $b$  таких открытых текстов (решений) достаточно много, то это будет «зацепкой» для проведения дифференциального криптоанализа. Таким образом, формулируем требование на функцию.

Векторная функция  $F$  называется *дифференциално  $\delta$ -равномерной*, если для любых  $a \neq 0$ ,  $b$  уравнение  $F(x) \oplus F(x \oplus a) = b$  имеет не более  $\delta$  решений. Минимальное такое  $\delta$  назовём *порядком дифференциальной равномерности* функции.

Для векторной функции  $F$  и любого ненулевого вектора  $a$  определим множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{Z}_2^n\}.$$

Далее определим следующую булеву функцию от  $2n$  переменных:

$$\gamma_F(a, b) = \begin{cases} 1, & \text{если } a \neq 0 \text{ и } b \in B_a(F); \\ 0, & \text{иначе.} \end{cases}$$

**Задача 628.** Определите порядок дифференциальной равномерности следующих функций:

- а)  $F = (2 \ 1 \ 0 \ 3)$ , тип  $2 \rightarrow 2$ ;
- б)  $F = (3 \ 3 \ 3 \ 0)$ , тип  $2 \rightarrow 2$ ;
- в)  $F = (0 \ 1 \ 1 \ 3 \ 1 \ 5 \ 4 \ 3)$ , тип  $3 \rightarrow 3$ ;
- г)  $F = (0 \ 0 \ 2 \ 1 \ 2 \ 2 \ 3 \ 6)$ , тип  $3 \rightarrow 3$ ;
- д)  $F = (1 \ 1 \ 1 \ 7 \ 6 \ 3 \ 2 \ 7)$ , тип  $3 \rightarrow 3$ .

**Задача 629.** Докажите, что функция  $F : \mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2^8$ , задающая S-блок шифра AES, является дифференциально 4-равномерной.

**Задача 630.** Докажите, что минимальное  $\delta$ , для которого существуют дифференциально  $\delta$ -равномерные функции, равно 2.

*APN-функцией* (Almost Perfect Nonlinear) называется дифференциально 2-равномерная векторная функция.

**Задача 631.** Покажите, что справедливы эквивалентные определения APN-функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ :

- функция  $F$  является APN-функцией, если она не аффинна на любом аффинном подпространстве  $A$  размерности 2, т. е.  $F(x) \oplus F(y) \oplus F(z) \oplus F(x \oplus y \oplus z) \neq 0$ , где  $\{x, y, z, x \oplus y \oplus z\} = A$ ;
- функция  $F$  является APN-функцией, если  $|B_a(F)| = 2^{n-1}$  для любого ненулевого  $a$ .

**Задача 632.** Определите, являются ли следующие функции APN-функциями:

- каждая из функций типа  $1 \rightarrow 1$ ;
- $F = (1 \ 1 \ 1 \ 3)$ , тип  $2 \rightarrow 2$ ;
- $F = (2 \ 1 \ 0 \ 3)$ , тип  $2 \rightarrow 2$ ;
- $F = (3 \ 0 \ 2 \ 2)$ , тип  $2 \rightarrow 2$ ;
- $F = (6 \ 7 \ 2 \ 2 \ 4 \ 6 \ 7 \ 4)$ , тип  $3 \rightarrow 3$ .

**Задача 633.** (\*) Докажите, что в АНФ любой APN-функции встречаются все квадратичные слагаемые  $x_i x_j$ , где  $1 \leq i < j \leq n$ .

**Задача 634.** Существуют ли взаимно однозначные APN-функции от трёх переменных? Если да, то приведите примеры.

**Задача 635.** (\*) Докажите, что не существует взаимно однозначных APN-функций от двух и четырёх переменных.

**Задача 636. APN-функция Диллона.** Докажите, что следующая функция типа  $6 \rightarrow 6$  является взаимно однозначной APN-функцией:

$$F = \begin{pmatrix} 0 & 54 & 48 & 13 & 15 & 18 & 53 & 35 & 25 & 63 & 45 & 52 & 3 & 20 & 41 & 33 \\ 59 & 36 & 2 & 34 & 10 & 8 & 57 & 37 & 60 & 19 & 42 & 14 & 50 & 26 & 58 & 24 \\ 39 & 27 & 21 & 17 & 16 & 29 & 1 & 62 & 47 & 40 & 51 & 56 & 7 & 43 & 44 & 38 \\ 31 & 11 & 4 & 28 & 61 & 46 & 5 & 49 & 9 & 6 & 23 & 32 & 30 & 12 & 55 & 22 \end{pmatrix}.$$

## 13.4 Связь АВ- и APN-свойств

Эта группа задач посвящена характеристизации АВ- и APN-свойств через свойства дополнительных объектов. При этом оказывается, что данные свойства тесно связаны.

**Задача 637. (\*) Характеризация свойств АВ и APN через коэффициенты Уолша — Адамара.** Пусть  $F$  — векторная функция типа  $n \rightarrow n$ . Докажите, что справедливы следующие утверждения:

а) функция  $F$  является АВ-функцией  $\iff$  все её коэффициенты Уолша — Адамара принимают значения из множества  $\{0, \pm 2^{\frac{n+1}{2}}\}$ ;

б) функция  $F$  является APN-функцией  $\iff$  её коэффициенты Уолша — Адамара удовлетворяют тождеству:

$$\sum_{u,v \in \mathbb{Z}_2^n} (W_F(u,v))^4 = 3 \cdot 2^{4n} - 2 \cdot 2^{3n}.$$

**Задача 638. (\*) Характеризация свойств АВ и APN через количество решений специально построенных систем уравнений.** Пусть  $F$  — векторная функция типа  $n \rightarrow n$ . Докажите, что справедливы следующие утверждения:

а) функция  $F$  является APN-функцией  $\iff$  система уравнений

$$\begin{cases} x \oplus y = a, \\ F(x) \oplus F(y) = b \end{cases}$$

имеет не более двух решений для всех  $a \neq 0, b$ ;

б) функция  $F$  является АВ-функцией  $\iff$  система уравнений

$$\begin{cases} x \oplus y \oplus z = a, \\ F(x) \oplus F(y) \oplus F(z) = b \end{cases}$$

имеет  $3 \cdot 2^n - 2$  решения, если  $b = F(a)$ , и  $2^n - 2$  решения иначе.

**Задача 639. Характеризация свойств АВ и APN через  $\gamma_F$ .** Пусть  $F$  — векторная функция типа  $n \rightarrow n$ . Докажите, что справедливы следующие утверждения:

а) функция  $F$  — APN-функция  $\iff$  вес  $\gamma_F$  равен  $2^{2n-1} - 2^{n-1}$ ;

б) функция  $F$  — АВ-функция  $\iff$  функция  $\gamma_F$  — бент-функция.

Функция  $F$  называется *платовидной*, если все её компонентные функции  $\langle v, F \rangle$ ,  $v \neq 0$ , платовидны, т. е. существуют натуральные числа  $\lambda_v$  такие, что коэффициенты Уолша — Адамара  $W_F(u, v)$  принимают значения из множества  $\{0, \pm \lambda_v\}$  для всех  $u$ . Числа  $\lambda_v$  называются *амплитудами* соответствующих компонентных функций.

**Задача 640.** На основе предыдущих задач покажите, что

- любая АВ-функция является APN-функцией;
- любая квадратичная APN-функция является АВ-функцией;
- любая платовидная APN-функция, у которой все амплитуды компонентных функций равны, является АВ-функцией.

## 13.5 Эквивалентность векторных функций

Для векторных булевых функций, так же как и для булевых функций, важной задачей является их классификация с точностью до какой-либо эквивалентности. Напомним, что *аффинной* называется такая функция  $A$ , что  $A(x \oplus y) = A(x) \oplus A(y) \oplus A(0)$  для всех  $x$  и  $y$ ; при  $A(0) = 0$  функция называется *линейной*. Пусть  $F$  и  $G$  — две векторные функции типа  $n \rightarrow m$ . Тогда  $F$  и  $G$  называются:

- 1) *аффинно (линейно) эквивалентными*, если  $G = A_1 \circ F \circ A_2$ , где  $A_1$  и  $A_2$  — взаимно однозначные аффинные (линейные) функции типов  $m \rightarrow m$  и  $n \rightarrow n$  соответственно;
- 2) *расширенно аффинно эквивалентными* (сокращённо — ЕА-эквивалентными), если  $G = A_1 \circ F \circ A_2 \oplus A$ , где  $A$  — аффинная функция типа  $n \rightarrow m$  и  $A_1$  и  $A_2$  — взаимно однозначные аффинные функции типов  $m \rightarrow m$  и  $n \rightarrow n$  соответственно;
- 3) *CCZ-эквивалентными*, если существует взаимно однозначная аффинная функция  $A = (A_1, A_2)$ , где  $A_1$  типа  $(n+m) \rightarrow n$  и  $A_2$  типа  $(n+m) \rightarrow m$ , такая, что  $y = F(x)$  тогда и только тогда, когда  $A_2(x, y) = G(A_1(x, y))$  для любых  $x \in \mathbb{Z}_2^n$ ,  $y \in \mathbb{Z}_2^m$ ; при этом функция  $F_1(x) = A_1(x, F(x))$  должна быть взаимно однозначной.

**Задача 641.** Пусть функции  $F$  и  $G$  типа  $n \rightarrow m$  являются CCZ-эквивалентными. Пусть  $A = (A_1, A_2)$  — соответствующая аффинная

взаимно однозначная функция. Покажите, что  $G = F_2 \circ F_1^{-1}$ , где  $F_1(x) = A_1(x, F(x))$  и  $F_2 = A_2(x, F(x))$ .

**Задача 642.** Проверьте следующие утверждения.

- а) Пусть две функции  $F$  и  $G$  типа  $n \rightarrow m$  EA-эквивалентны. Верно ли, что  $F$  и  $G$  CCZ-эквивалентны?
- б) Пусть  $F$  — взаимно однозначная функция типа  $n \rightarrow n$ . Верно ли, что  $F$  и  $F^{-1}$  CCZ-эквивалентны?

**Задача 643.** Докажите, что алгебраическая степень векторной функции является инвариантом относительно EA-эквивалентности.

**Задача 644.** Что можно сказать про степени CCZ-эквивалентных векторных функций? Приведите примеры.

**Задача 645.** Докажите, что две CCZ-эквивалентные функции типа  $n \rightarrow n$  всегда одновременно являются или не являются APN-функциями; другими словами CCZ-преобразование сохраняет свойство функции быть APN-функцией.

**Задача 646.** Пусть функции  $F$  и  $G$  типа  $n \rightarrow m$  являются CCZ-эквивалентными. Пусть  $A = (A_1, A_2)$  — соответствующая аффинная взаимно однозначная функция. Докажите, что булевые функции  $\gamma_F$  и  $\gamma_G$  от  $2n$  переменных связаны следующим образом:  $\gamma_G = \gamma_F \circ L^{-1}$ , где  $L$  — линейная часть аффинного преобразования  $A$ .

**Задача 647.** Пусть  $F$  — АВ-функция типа  $n \rightarrow n$  и  $G$  — CCZ-эквивалентная  $F$  функция. Докажите, что  $G$  также является АВ-функцией.

**Задача 648. (\*)** Пусть функции  $F$  и  $G$  типа  $n \rightarrow m$  являются CCZ-эквивалентными. Докажите следующие утверждения:

- а) если  $F$  — дифференциальна  $\delta$ -равномерная, то и  $G$  — дифференциальна  $\delta$ -равномерная;
- б) нелинейность функций  $F$  и  $G$  совпадает.

## 13.6 Алгебраическое представление векторной функции

Напомним, что множество  $\mathbb{Z}_2^n$  двоичных векторов длины  $n$  можно рассматривать как конечное поле со специальным образом определёнными операциями сложения и умножения (см. раздел 4.9). При этом каждому вектору  $(c_1, \dots, c_n) \in \mathbb{Z}_2^n$  однозначно соответствует многочлен  $c_1x^{n-1} + c_2x^{n-2} + \dots + c_n$ . Множество  $\mathbb{Z}_2$  также является полем, а именно  $GF(2)$ , состоящим из двух элементов 0 и 1.

Любую векторную булеву функцию от  $n$  переменных  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  можно отождествить с функцией, действующей из  $GF(2^n)$  в  $GF(2^n)$ . Функцию из  $GF(2^n)$  в  $GF(2^n)$  для удобства также будем называть векторной булевой функцией.

Пусть  $k$  — целое число. Напомним, что весом целого числа  $wt(k)$  называется вес его двоичного представления.

**Задача 649. Алгебраическое представление векторной функции типа  $n \rightarrow n$ .** Докажите, что произвольная векторная булева функция  $F : GF(2^n) \rightarrow GF(2^n)$  однозначно представляется в виде

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \text{ где } \delta_i \in GF(2^n).$$

При этом справедливо, что  $\deg(F) = \max_{i: \delta_i \neq 0} \{wt(i)\}$ .

В частном случае такое алгебраическое представление справедливо и для обычных булевых функций: а именно, если выбрать коэффициенты  $\delta_i$  так, чтобы сумма элементов поля  $GF(2^n)$ , находящаяся в правой части, всегда принадлежала простому подполю  $GF(2)$ . Так, например, и была получена трейс-форма булевой функции (см. раздел 11.7, задача 548). Однако надо понимать, что трейс-форма обычной булевой функции — лишь один из возможных способов её алгебраического представления.

**Задача 650. Алгебраическое представление векторной функции типа  $2n \rightarrow n$ .** Докажите, что произвольная векторная булева

функция  $F : GF(2^n) \times GF(2^n) \rightarrow GF(2^n)$  однозначно представляется в виде

$$F(x, y) = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \delta_{ij} x^i y^j, \text{ где } \delta_{ij} \in GF(2^n).$$

При этом справедливо, что  $\deg(f) = \max_{i,j: \delta_{ij} \neq 0} \{wt(i) + wt(j)\}$ .

**Задача 651.** **Линейная и аффинная функции.** Определите вид алгебраического представления произвольной линейной  $L$  и аффинной  $A$  векторной булевой функции над полем  $GF(2^n)$ .

**Задача 652.** Покажите, что алгебраическое представление векторной булевой функции  $F$  типа  $n \rightarrow n$  можно получить с помощью значений  $F$ , раскрыв скобки в следующем выражении:

$$\sum_{a \in GF(2^n)} F(a)(1 + (x + a)^{2^n - 1}).$$

**Задача 653.** Установите соответствие между набором значений функции типа  $3 \rightarrow 3$  и её алгебраическим представлением над полем  $GF(2^3)$  в виде полинома от переменной  $x$ . Поле  $GF(2^3)$  построено с помощью неприводимого многочлена  $z^3 + z + 1$  и примитивного элемента  $\alpha = z$ .

- |                       |  |
|-----------------------|--|
| а) (0 1 2 3 4 5 6 7); | 1) $x^7$ ;                                 |
| б) (0 1 0 6 0 2 0 4); | 2) $\alpha^4 + \alpha^2 x^3$ ;             |
| в) (2 4 6 0 6 0 2 4); | 3) $\alpha^5$                              |
| г) (0 1 1 1 1 1 1 1); | 4) $x$ ;                                   |
| д) (0 7 5 2 1 6 4 3); | 5) $\alpha + \alpha^3 x^6$ ;               |
| е) (6 2 1 0 4 3 7 5); | 6) $\alpha + \alpha^3 x + \alpha^6 x^2$ ;  |
| ж) (6 3 1 5 7 6 7 7); | 7) $\alpha^5 x$ ;                          |
| з) (2 1 6 3 0 4 7 5); | 8) $x + x^3 + x^7$ ;                       |
| и) (7 7 7 7 7 7 7 7); | 9) $\alpha + \alpha^3 x^6$ ;               |
| к) (6 5 0 6 5 3 0 3); | 10) $\alpha^4 + \alpha x + \alpha^5 x^5$ . |

# ГЛАВА 14. КРИПТОАНАЛИЗ СИММЕТРИЧНЫХ ШИФРОВ

В данной главе читатель на практике познакомится с такими методами криптоанализа симметричных шифров, как линейный, дифференциальный, алгебраический. Их краткое описание можно найти в пособии [33], более основательное — в книге [18], см. также справочник С. П. Панасенко [23]; подробно линейный и дифференциальный методы криптоанализа изложены на простом примере в статье [46], практическому применению этих методов посвящена книга Л. К. Бабенко и Е. А. Ищуковой [8]. Для детального знакомства с алгебраическим криптоанализом рекомендуем книгу G. Bard [40].

Многие задачи этой главы потребуют программных решений.

## 14.1 Частотный анализ

**Задача 654.** Сообщение было составлено на русском языке и зашифровано с помощью шифра простой замены. Восстановите его по шифртексту:

R eSkSrt7m +mrI1SoS z1q5 rwmx5kt tv oSqS+5.

2Shhm awkS hzxS, eqmbq5h7Sm 5eqmkhbSm hSk7цм htkb7S oqmkS,  
7S r b575r5x t r kmhz km85k тщм h7mo. Vtj5, vk5l, 1mj75l, +kt775l,  
awk5 тщм 15b 7m+5r7S, rmh75 eqt2k5 r+qzo, 7S +kl J5qьt R5htkьmr7w,  
bS1Sq5l ht+mk5 1memqь r 1mkmom, 7m eqm+h15rklt 7tчмоS 7SrSoS  
t t71mqmh7SoS 7t 1mekS, 7t 1Sj7wm, hSoqm1wm +wx57tmj rmh7w  
eqSvq5ч7wm kmh5, 7t чmq7wm h15t, km15r2tm r eSkm 75+ oqSj5+7wjt  
kz85jt, eSxS8tjt 75 Svmq5, 7t ə1S 7maS, cz+7Sm, amv+S77Sm, bz+5,  
b58m1hl, z2mk aw h 15bSю q5+Sh1ью. RS1 z8 1qt75+q51b km1, b5b S75  
zut1mkb7tcmj, t 7m hS41m2b, hbSkbbS q5v v5 rhm ə1t oS+w S75 mv+tk5  
r oSqS+ v5 85kSr57ьmj; t awk5 kt rmh75, b5b 1memqь, tkt Shm77тг гмчмq  
h +S8+mj, tkt vtj5, - +kl 7mm awkS rhm q5r7S, t rhmo+5 7mtvjm77S  
xS1mkShb S+7SoS: eShbSqmm aw +Smx51b.

Z 7mm awkS 15bSm 4zrh1rS, b5b az+1S S75 8tk5 г ə1tx bq5lx z8m  
+5r7S-+5r7S, km1 h1S, t b5v5kShb мй, ч1S 75 rhmj ez1t S1 oSqS+5  
+S hrSmj 2bSkwS75 v75k5 b58+wй b5jm7b, b58+Sm +mqmrS. 1z1  
awkS mm eqS2kSm, mm 75h1Sицmm; t +qzoSoS az+zщмоS S75 7m  
jSok5 eqm+h15rt1b hmam, b5b 1SkbbS 2bSk5, +SqSo5 r oSqS+ t Saq517S,  
t Se11b 2bSk5, t Se11b +SqSo5...

## 14.2 А попробуем и мы!

В этом вводном разделе предлагаем вам попробовать свои силы в криптоанализе шифра DES. Методы криптоанализа, необходимые для поставленных задач, придумайте сами!

DES — алгоритм симметричного шифрования с интересной историей. Национальное бюро стандартов (NBS) США в 1973 г. объявило первый в истории открытый конкурс на стандарт шифрования. Претендентом стал алгоритм шифрования Lucifer, разработанный фирмой IBM. В результате совместной деятельности IBM, NBS и NSA (Агентство национальной безопасности США) алгоритм был существенно доработан и в январе 1977 г. DES был опубликован как стандарт США на шифрование данных (кроме информации повышенной степени секретности). Подробно об алгоритме написано в [3] и [33]. С последней версией этого стандарта можно ознакомиться в документе FIPS 46-3. Data Encryption Standard ([www.csrc.nist.gov](http://www.csrc.nist.gov)). Напомним, что DES — 16-раундовый блочный шифр Фейстеля; алгоритм осуществляет шифрование блоков длины 64 бита; длина ключа составляет 56 битов, но ключ обычно представляется 64-битовым числом, где каждый восьмой бит используется для проверки чётности и игнорируется. Мы будем представлять ключ в виде 64-битного числа.

**Задача 655. DES.** Для того чтобы проводить атаки на шифр, нужно его реализовать. Запрограммируйте алгоритм шифрования DES и заполните таблицу.

|    | Открытый текст   | Шифртекст        | Ключ             |
|----|------------------|------------------|------------------|
| 1  | 0123456789abcde7 | c95744256a5ed31d | 0123456789abcdef |
| 2  | eff0e8e2e5f2ece8 | ?                | 68656c6c6f776f72 |
| 3  | ?                | ed70bc5f05110e50 | 68656c6c6f776f72 |
| 4  | ?                | f3f0eee1eef0eef1 | fefefefefefefefe |
| 5  | f3f0eee1eef0eef1 | ?                | fefefefefefefefe |
| 6  | ?                | 1b4acf1c0ee11f84 | e0e0e0e0f1f1f1f1 |
| 7  | ?                | 3596522dbc5b1ae9 | f3f0eee1eef0eef1 |
| 8  | 3596522dbc5b1ae9 | ?                | f3f0eee1eef0eef1 |
| 9  | e7ece5fff1e5e1ff | ?                | f3f0eee1eef0eef1 |
| 10 | ?                | 0ba3dd24c394072a | eceeede8f2eef0e0 |

**Задача 656. Разные ключи.** В программе шифрования DES, которую использует Микеланджело, ключ задаётся в виде шестнадцати шестнадцатеричных цифр. При задании ключа Микеланджело нажимал только две клавиши. Найдите ключ по известной паре «открытый текст — шифртекст». Во всех шести случаях использовались разные ключи.

|   | Открытый текст                        | Шифртекст                            |
|---|---------------------------------------|--------------------------------------|
| 1 | f1efeb8edf2e5f0<br>eae0e2e0e1e0ede3   | c3f781e52fd1f73f<br>0d43be18785622c0 |
| 2 | ebe5eeede0f0e4ee<br>eaeeece0ede4e8f0  | 1092d1474fd348a1<br>624df233dce5e206 |
| 3 | f8f0e5e9e4e5f038<br>f2e5f5edeee4f0ec  | 3573e79a64886a63<br>fbec9ed6449b28ff |
| 4 | efe8f6f6e0eaf0e5<br>ede3e2eaeeff1f2fe | 6e6b207a63584c84<br>2037c53731d34a51 |
| 5 | 35fbe9eae0ede0eb<br>fde9eff0ebeeeeeb  | 92bfd01ed5ad7d6<br>87a40f1673cb3612  |

**Задача 657. Меняем S-блоки.** Узнав, что шифр DES был взломан, Леонардо решает изменить алгоритм: поменять какие-то два S-блока местами. Определите, какие S-блоки были переставлены и найдите ключ по известной паре «открытый текст — шифртекст». Во всех шести случаях использовался один алгоритм, но различные ключи. Ключ опять вводит Микеланджело (помните, он нажимает лишь на две клавиши?).

|   | Открытый текст                        | Шифртекст                            |
|---|---------------------------------------|--------------------------------------|
| 1 | f1efeb8edf2e5f0<br>eae0e2e0e1e0ede3   | 271f42c0dc15d98e<br>b60857fcfd3e6996 |
| 2 | ebe5eeede0f0e4ee<br>eaeeece0ede4e8f0  | 1575a6511f5ffb4a<br>93885599e80fdf98 |
| 3 | f8f0e5e9e4e5f038<br>f2e5f5edeee4f0ec  | ff4287b3a035a708<br>b1f866c65a356be0 |
| 4 | efe8f6f6e0eaf0e5<br>ede3e2eaeeff1f2fe | a7dc976ee8141938<br>91a81d0e00598c58 |
| 5 | 35fbe9eae0ede0eb<br>fde9eff0ebeeeeeb  | 55201d3dd730a4f7<br>3cf1b1c5cc547ac8 |

**Задача 658. (\*) Усложнение!** Для повышения стойкости шифра Донателло решает использовать стандартный алгоритм шифрования DES два раза. Длина ключа увеличилась вдвое, и Микеланджело при задании ключа шифра пришлось совершать в два раза больше нажатий на какие-то две кнопки. Но вопреки ожиданиям, стойкость шифра повысилась совсем незначительно. Почему? Восстановите ключ по известной паре «открытый текст — шифртекст» в каждом из шести случаев.

|   | Открытый текст  | Шифртекст  |
|---|---|--|
| 1 | f1efebe8edf2e5f0<br>eae0e2e0e1e0ede3<br>ebe5eede0f0e4ee   | f1efebe8edf2e5f0<br>eae0e2e0e1e0ede3<br>ebe5eede0f0e4ee  |
| 3 | f8f0e5e9e4e5f038<br>f2e5f5edeee4f0ec<br>eaeeece0ede4e8f0  | 1e215f61c9558908<br>6b66d1a817a98bf8<br>452be9d509a24470 |
| 4 | efe8f6f6e0eaf0e5<br>ede3e2eaeeff1f2fe<br>35fbe9eae0ede0eb | a437e353ebdce3af<br>625097f240248954<br>a48355e5678169f6 |
| 6 | e8e7ece5f0e5ede8<br>e5e8eaf16c6f7365<br>fde9eff0ebbeeedeb | 005d6537a0b2db29<br>636ef778079d05ee<br>b70757c6daa88ba6 |

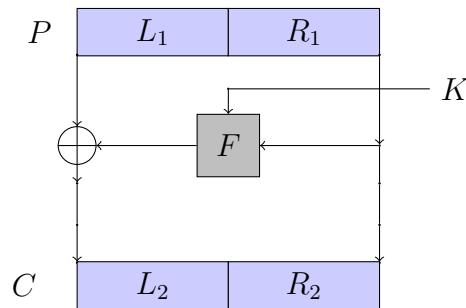
### 14.3 Линейный криптоанализ

Одним из наиболее известных статистических методов криптоанализа симметричной криптографии является *линейный криптоанализ*. Он требует знания структуры шифра и достаточного объёма выборки, состоящей из пар открытого и зашифрованного текстов, полученных на одном и том же *неизвестном* ключе. Предложил его японский криптограф Мицуру Мацуи в 1992—1993 гг., см. [47], [48].

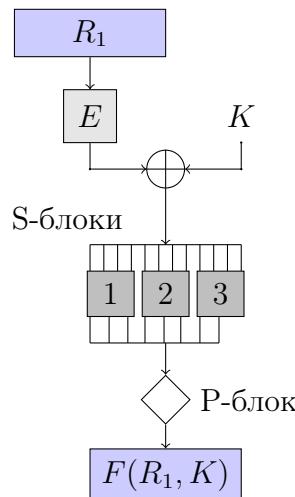
Читателю предлагается провести линейный криптоанализ шифра, являющегося сетью Фейстеля. Назовём этот шифр, например, TwoFly. Для удобства шаги криптоанализа разделены и сформулированы в виде задач. Открытый текст  $P$  длины 16 бит делится на левую  $L_1$  и правую  $R_1$  половины. Шифртекст



$C$  получается объединением  $L_2 = L_1 \oplus F(R_1, K)$  и  $R_2 = R_1$ . Биты нумеруются начиная с первого слева направо.



Функция  $F$  типа  $8 \rightarrow 8$  выглядит следующим образом



Нелинейные S-блоки заданы таблицами:

S-блок 1 ( $4 \rightarrow 3$ )

|   | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|-----|-----|-----|-----|-----|-----|-----|-----|
| 0 | 7   | 6   | 1   | 3   | 4   | 2   | 6   | 1   |
| 1 | 5   | 7   | 3   | 5   | 1   | 4   | 3   | 2   |

S-блок 2 ( $4 \rightarrow 3$ )

|   | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|-----|-----|-----|-----|-----|-----|-----|-----|
| 0 | 5   | 0   | 2   | 7   | 3   | 4   | 6   | 5   |
| 1 | 6   | 3   | 5   | 6   | 4   | 7   | 2   | 1   |

S-блок 3 ( $4 \rightarrow 2$ )

|   | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|-----|-----|-----|-----|-----|-----|-----|-----|
| 0 | 3   | 1   | 2   | 0   | 2   | 0   | 1   | 1   |
| 1 | 1   | 2   | 3   | 1   | 3   | 2   | 0   | 3   |

Например, первый S-блок переводит вектор (0001) в вектор (110), поскольку значение на пересечении первой строки и второго столбца равно 6 = (110).

Расширяющая перестановка  $E$  задаётся таблицей:

E — расширяющая подстановка

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 3 | 4 | 7 | 1 | 6 | 3 | 5 | 3 | 8 | 5 | 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|

Так, вторым битом расширенного блока будет 3-й бит блока  $R_1$  и т. д. Аналогично определяется и перестановка в P-блоке.

Перестановка в P-блоке

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 6 | 4 | 1 | 8 | 5 | 7 | 2 | 3 |
|---|---|---|---|---|---|---|---|

Напомним, что  $\langle x, y \rangle = x_1y_1 \oplus \dots \oplus x_ny_n$  обозначает скалярное произведение двоичных векторов по модулю 2.

Линейный криптоанализ заключается в поиске линейного приближения шифра. *Линейным приближением шифра* называется ненулевое соотношение  $L$  вида

$$\langle P, \alpha \rangle \oplus \langle C, \beta \rangle = \langle K, \gamma \rangle, \quad (14.1)$$

которое выполняется с вероятностью  $1/2 + \varepsilon$ , отличной от  $1/2$ . Величина  $\varepsilon$  называется *преобладанием* линейного соотношения.

Для построения линейных приближений в общем случае необходимо рассматривать всевозможные значения векторов  $\alpha, \beta, \gamma$  и отдельно находить вероятности выполнения каждого соотношения. Но

так как это требует огромных вычислительных затрат, то обычно пользуются методом «от простого — к сложному». Метод заключается в анализе отдельных компонент шифра, начиная с S-блоков, и поэтапном переходе к приближению всего шифра.

Криптоанализ шифра начинается с анализа S-блоков. Результат анализа S-блока удобно представлять в виде *таблицы линейного преобладания*. Рассмотрим построение таблицы линейного преобладания первого S-блока. Обозначим вход и выход S-блока 1 через  $x = (x_1, x_2, x_3, x_4)$  и  $y = (y_1, y_2, y_3)$  соответственно. В таблице линейного преобладания на пересечении строки  $u$  и столбца  $v$  находится число  $\lambda$  такое, что соотношение  $\langle u, x \rangle = \langle v, y \rangle$  выполняется с вероятностью  $(8+\lambda)/16$ . Модуль числа  $\lambda$  описывает отклонение вероятности от  $1/2$ , число  $\lambda/16$  — *преобладание* соотношения.

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  |
|---|----|----|----|----|----|----|----|----|
| 0 | +8 | -2 | -1 | -1 | 0  | -2 | -1 | -1 |
| 1 | 0  | -2 | +1 | +1 | 0  | -2 | +1 | +1 |
| 2 | 0  | +2 | +1 | +1 | -4 | +2 | +1 | -3 |
| 3 | 0  | -2 | +3 | -1 | 0  | +2 | -1 | -1 |
| 4 | 0  | -4 | -1 | +1 | -2 | +2 | +1 | +3 |
| 5 | 0  | 0  | +1 | -1 | 2  | +2 | -1 | -3 |
| 6 | 0  | 0  | -3 | -1 | -2 | +2 | +3 | +1 |
| 7 | 0  | 0  | -1 | +1 | -2 | +2 | -3 | +3 |
| 8 | 0  | +2 | -1 | -1 | 0  | -2 | +3 | -1 |
| 9 | 0  | +2 | +1 | +1 | -4 | +2 | +1 | -3 |
| a | 0  | +2 | -3 | +1 | 0  | +2 | -3 | +1 |
| b | 0  | -2 | -1 | +7 | 0  | -2 | -1 | -1 |
| c | 0  | 0  | -1 | +1 | +2 | -2 | +1 | -1 |
| d | 0  | -4 | +1 | -1 | +2 | +2 | +3 | -3 |
| e | 0  | 0  | +1 | -1 | -2 | -2 | +3 | +1 |
| f | 0  | 0  | -5 | +1 | +2 | +2 | +1 | -1 |

Таблица линейного преобладания S-блока 1

Соотношение  $0 \cdot x = 0 \cdot y$  выполняется при каждом значении входа  $x$ , значит его вероятность равна 1. Поэтому элемент на пересечении нулевых строк в таблице преобладания равен +8. Рассмотрим соотношение  $b \cdot x = 3 \cdot y$ . После перехода к двоичным представлениям элементов  $b = (1011)$  и  $3 = (011)$  соотношение приобретает вид

$x_1 \oplus x_3 \oplus x_4 = y_2 \oplus y_3$ . Проверив это соотношение для каждой из 16 пар вход-выход S-блока, получим, что оно выполняется для 15 таких пар. Значит, данное соотношение задаёт приближение S-блока, выполняющееся с преобладанием +7, и это преобладание записывается в таблицу. Обратим внимание, что приближение  $b \cdot x = 3 \cdot y$  является лучшим среди приближений S-блока 1, так как нет других с большим отклонением. Приближение  $0 \cdot x = 0 \cdot y$  является тривиальным и не рассматривается.

**Задача 659.** Напишите программную реализацию шифра TwoFly.

**Задача 660. Шаг 1.** Проанализируйте S-блоки шифра TwoFly. Вероятность линейного приближения какого из S-блоков имеет наибольшее отклонение от  $1/2$ ? Определите лучшее приближение для каждого из S-блоков.

Теперь, после анализа S-блоков, можно строить линейные приближения всего описанного выше шифра. Для этого нужно отслеживать преобразования битов открытого текста, ключа и шифртекста, проходящих через S-блоки, перемешивающие перестановки и подстановки.

Для примера отследим следующие биты открытого текста  $p_9, p_{10}, p_{11}$ , а точнее построим линейное приближение шифра, в которое бы входила сумма  $p_9 \oplus p_{10} \oplus p_{11}$ .

Биты  $p_9, p_{10}, p_{11}$  являются первыми тремя битами вектора  $R_1$ , который подаётся на вход функции  $F$ . После расширяющей подстановки  $E$  бит  $p_9$  оказывается на 5-м и 9-м, бит  $p_{10}$  — на 8-м и 12-м, бит  $p_{11}$  — на 2-м и 7-м местах вектора, складываемого с ключом  $K$ . После сложения с ключом сумма подаётся на S-блоки. Используем следующие приближения S-блоков:

| S-блок  | соотношение                                | вероятность | преобладание |
|---------|--|-------------|--------------|
| $S_1$ : | $x_2 = y_3$                                | $12/16$     | $+4/16$      |
| $S_2$ : | $x_1 \oplus x_3 = y_2$                     | $11/16$     | $+3/16$      |
| $S_3$ : | $x_1 \oplus x_4 = y_1 \oplus y_2 \oplus 1$ | $11/16$     | $+3/16$      |

Выход S-блоков после перестановки (Р-блока) даёт результат действия функции  $F$ . Отслеживая перестановки битов, получаем следующие приближения раундовой функции:

| соотношение  | вероятность |
|--|-------------|
| $R_1[3] \oplus F(R_1, K)[8] \oplus 1 = K[2]$           | 12/16       |
| $R_1[1, 3] \oplus F(R_1, K)[5] = K[5, 7]$              | 11/16       |
| $R_1[3, 2] \oplus F(R_1, K)[6, 4] \oplus 1 = K[9, 12]$ | 11/16       |

Сложением этих трёх соотношений мы получим приближение раундовой функции, в котором будет сумма первых трёх битов  $R_1$ . Действительно,  $R_1[3] \oplus R_1[1, 3] \oplus R_1[3, 2] = R_1[1, 2, 3]$ . Здесь числа в квадратных скобках обозначают соответствующий бит вектора (или их сумму, если чисел несколько). Приближение будет задаваться соотношением следующего вида

$$R_1[1, 2, 3] \oplus F(R_1, K)[8, 5, 6, 4] = K[2, 5, 7, 9, 12].$$

Для подсчёта вероятности, с которой будет выполняться это соотношение, используется лемма Мацуи.

**Лемма 4. (Лемма Мацуи)** Пусть  $X_i$ , где  $1 \leq i \leq n$ , — независимые случайные величины, принимающие значения из  $\mathbb{Z}_2$ . Пусть

$$\mathbf{P}\{X_i = 0\} = 1/2 + \varepsilon_i, \text{ где } 0 \leq |\varepsilon_i| \leq 1/2.$$

Тогда случайная величина  $X_1 \oplus X_2 \oplus \dots \oplus X_n$  принимает значение 0 с вероятностью  $1/2 + \varepsilon$ , где  $\varepsilon = 2^{n-1} \prod_{i=1}^n \varepsilon_i$ .

**Задача 661.** Докажите лемму Мацуи.

Полученное выше соотношение согласно лемме Мацуи выполняется с вероятностью

$$\frac{1}{2} + 2^2 \cdot \frac{4}{16} \cdot \frac{3}{16} \cdot \frac{3}{16} = \frac{1}{2} + \frac{12^2}{16^3} \approx 0,535156.$$

Преобладание соотношения равно  $\varepsilon = 12^2/16^3 \approx 0,035$ . При вычислении мы считаем, что случайные величины, определенные соотношениями, которые мы складываем, независимы. Хотя на самом деле это может быть не так.

Применим полученное приближение раунда для приближения всего шифра. Для этого вспомним, что шифртекст  $C$  получается объединением  $L_2 = L_1 \oplus F(R_1, K)$  и  $R_2 = R_1$ , где  $L_1$  и  $R_1$  — соответственно левая и правая половины открытого текста  $P$ .

| соотношение  | $p$   |
|--|-------|
| $R_1[1, 2, 3] \oplus F(R_1, K)[8, 5, 6, 4] = K[2, 5, 7, 9, 12]$  | 0, 53 |
| $L_1[8, 5, 6, 4] \oplus F(R_1, K)[8, 5, 6, 4] = L_2[8, 5, 6, 4]$ | 1     |

После сложения линейных соотношений из таблицы получаем линейное приближение всего шифра:

$$L_1[8, 5, 6, 4] \oplus R_1[1, 2, 3] \oplus L_2[8, 5, 6, 4] = K[2, 5, 7, 9, 12].$$

Как правило, его вероятность также считается по лемме Мацуи, но в данном случае видно, что она совпадает с вероятностью раундового приближения.

В терминах соотношения (14.1) полученное приближение задаётся соотношением  $\langle P, \alpha \rangle \oplus \langle C, \beta \rangle = \langle K, \gamma \rangle$ , где  $\alpha = (0001110111100000)$ ,  $\beta = (0001110100000000)$ ,  $\gamma = (010010101001)$ .

**Задача 662.** Наилучшим ли образом выбраны приближения S-блоков шифра TwoFly для построения приближения? Постройте приближение, в котором бы участвовали биты открытого текста  $p_9, p_{10}, p_{11}$  и которое бы выполнялось с большей вероятностью.

Объём выборки необходимый для успешного проведения криптоанализа зависит от преобладания линейного приближения шифра. Согласно [17] мощность выборки  $N$  необходимой для успешной работы алгоритма 1 Мацуи [47] можно находить из таблицы

| $N$     | $\frac{1}{4} \varepsilon ^{-2}$ | $\frac{1}{2} \varepsilon ^{-2}$ | $ \varepsilon ^{-2}$ | $2 \varepsilon ^{-2}$ |
|---------|---------------------------------|---------------------------------|----------------------|-----------------------|
| $\xi_0$ | 0, 841                          | 0, 921                          | 0, 977               | 0, 998.               |

Здесь  $\xi_0$  — математическое ожидание вероятности того, что в результате работы алгоритма будет найден правильный ключ.

**Задача 663. Шаг 2.** Используя приближения S-блоков, найденные в задаче 660, найдите линейные приближения шифра TwoFly. С какой вероятностью они будут выполняться? Какое приближение будет наилучшим, т. е. выполняться с наибольшей вероятностью?

**Задача 664. Шаг 3.** Как правило, во время криптоанализа криптоаналитик располагает некоторой выборкой — набором пар «открытый текст — шифртекст»  $(P, C)$ . Сколько пар «открытый текст — шифртекст» достаточно для того, чтобы с вероятностью близкой к единице (например, 0,977) утверждать, что лучшее линейное приближение шифра TwoFly даёт верную информацию о ключе? Выразите биты ключа, насколько это возможно, через биты открытого текста.

**Задача 665. (\*)** Предложите S-блоки, которые обеспечат большую криптографическую стойкость шифра TwoFly к линейному криптоанализу. Что именно можно улучшить в имеющихся S-блоках?

**Задача 666.** Найдите лучшие линейные приближения шифра TwoFly, в которых бы участвовали следующие биты открытого текста:

- а)  $p_{13}, p_{14}, p_{15}$ ,
- б)  $p_9, p_{12}, p_{14}$ ,
- в)  $p_1, p_{13}$ ,
- г)  $p_5, p_{10}, p_{15}$ .

А если биты шифртекста:

- д)  $c_1, c_2, c_3$ ,
- ж)  $c_4, c_6, c_8$ ,
- з)  $c_2, c_{14}$ ,
- и)  $c_4, c_9, c_{14}$ ?

Одновременно биты открытого текста и шифртекста:

- к)  $p_8, c_1$ ,
- л)  $p_1, p_{15}, c_2, c_{12}$ .

**Задача 667. (\*) Линейный криптоанализ простого шифра.** Проведите линейный криптоанализ трёхраундового блочного шифра:

$P = (p_1, p_2, p_3, p_4, p_5, p_6)$  — открытый текст длины 6,

$K = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9)$  — ключ шифрования длины 9,

$C = (c_1, c_2, c_3, c_4, c_5, c_6)$  — шифртекст длины 6,

Подключи

$K_1 = (k_1, k_2, k_3, k_4, k_5, k_6)$  — подключ 1-го раунда,

$K_2 = (k_4, k_5, k_6, k_7, k_8, k_9)$  — подключ 2-го раунда,

$K_3 = (k_7, k_8, k_9, k_1, k_2, k_3)$  — подключ 3-го раунда,

S-блоки: вход и выход — векторы длины 3

$$S_1 = (0, 5, 7, 2, 3, 4, 1, 6),$$

$$S_2 = (6, 1, 2, 0, 5, 4, 3, 7).$$

Пусть  $C_0 = P$ . Опишем раунд шифрования номер  $i$ , где  $i = 1, 2, 3$ .

Полагаем  $C_i = (S_1(L_i), S_2(R_i))$ , где  $(L_i, R_i) = C_{i-1} \oplus K_i$  и векторы  $L_i, R_i$  имеют длину 3. Результат зашифрования  $C = C_3$ .

Определите, какой объём выборки потребуется для работы алгоритма с надежностью 0,84; 0,92; 0,99. Предложите свои идеи по возможности нелинейного криптоанализа этого шифра.

**Задача 668. (\*) Модификация.** Проведите криптоанализ блочного шифра, описанного выше, но с несколько изменённым раундом — положим

$$C_i = V_i <<< 2 \text{ (циклический сдвиг влево на две позиции)},$$

$$V_i = (S_1(L_i), S_2(R_i)).$$

Результат зашифрования по-прежнему  $C = C_3$ .

Как возрос объём выборки, требующийся для работы алгоритма с надёжностью 0,84; 0,92; 0,99. Почему?

**Задача 669.** Восстановите ключи, используемые в шифре, описанном в предыдущей задаче. Используйте для этого найденные линейные приближения шифра. Пары «открытый текст — шифртекст» приведены в ниже (здесь двоичный вектор длины шесть  $(x_1, \dots, x_6)$  записан десятичным числом  $\sum_{i=1}^6 x_i 2^{n-i}$ ):

| a)      | б)      |         |         |         |         |         |         |
|---------|---------|---------|---------|---------|---------|---------|---------|
| 10 - 62 | 39 - 23 | 19 - 59 | 53 - 16 | 12 - 55 | 22 - 28 | 30 - 25 | 40 - 16 |
| 21 - 17 | 43 - 58 | 52 - 61 | 51 - 25 | 15 - 51 | 23 - 36 | 33 - 26 | 48 - 4  |
| 23 - 15 | 47 - 14 | 55 - 45 | 60 - 8  | 18 - 43 | 25 - 11 | 35 - 42 | 51 - 33 |
| 33 - 36 | 48 - 11 | 13 - 18 | 61 - 37 | 19 - 12 | 26 - 31 | 36 - 63 | 54 - 24 |
| 35 - 35 | 50 - 20 | 16 - 40 | 63 - 57 | 20 - 35 | 28 - 21 | 38 - 34 | 62 - 1  |

**Задача 670. Обратный анализ S-блока.** Найдите S-блок, таблицей линейного преобразования которого является следующая таблица. Будет ли он единственным? Почему?

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | a  | b  | c  | d  | e  | f  |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | +8 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 1 | 0  | +4 | 0  | -2 | 0  | 0  | -2 | +6 | +2 | +2 | 0  | 0  | +2 | +2 | 0  | 0  |
| 2 | 0  | 0  | -2 | -2 | 0  | 0  | -2 | -2 | 0  | 0  | +2 | +2 | 0  | 0  | -6 | +2 |
| 3 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | +2 | -2 | -2 | -2 | +2 | +2 | -2 | -2 | -2 |
| 4 | 0  | +2 | 0  | -2 | -2 | -4 | -2 | 0  | 0  | -2 | 0  | +2 | +2 | -4 | +2 | 0  |
| 5 | 0  | -2 | -2 | 0  | -2 | 0  | +4 | +2 | -2 | 0  | -4 | +2 | 0  | -2 | -2 | 0  |
| 6 | 0  | +2 | -2 | +4 | +2 | 0  | 0  | +2 | 0  | -2 | +2 | +4 | -2 | 0  | 0  | -2 |
| 7 | 0  | -2 | 0  | +2 | +2 | -4 | +2 | 0  | -2 | 0  | +2 | 0  | +4 | +2 | 0  | +2 |
| 8 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | -2 | +2 | +2 | -2 | +2 | -2 | -2 | -6 | -2 |
| 9 | 0  | 0  | -2 | -2 | 0  | 0  | -2 | -2 | -4 | 0  | -2 | +2 | 0  | +4 | +2 | -2 |
| a | 0  | +4 | -2 | +2 | -4 | 0  | +2 | -2 | +2 | +2 | 0  | 0  | +2 | +2 | 0  | 0  |
| b | 0  | +4 | 0  | -4 | +4 | 0  | +4 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| c | 0  | -2 | +4 | -2 | -2 | 0  | +2 | 0  | +2 | +2 | +4 | 0  | +2 | 0  | -2 | -2 |
| d | 0  | +2 | +2 | 0  | -2 | +4 | 0  | +2 | -4 | -2 | +2 | 0  | +2 | 0  | 0  | +2 |
| e | 0  | +2 | +2 | 0  | -2 | -4 | 0  | +2 | -2 | 0  | 0  | -2 | -4 | +2 | 0  | 0  |
| f | 0  | -2 | -4 | -2 | -2 | 0  | +2 | 0  | 0  | -2 | +4 | -2 | -2 | 0  | 0  | 0  |

**Задача 671. (\*) Линейный криптоанализ S-AES.** Проведите линейный криптоанализ шифра S-AES. Рассмотрите два случая: когда раундовые ключи одинаковые и когда они разные. Оцените необходимый объём выборки для надёжной работы метода.

**Задача 672. Свойство таблицы.** Докажите, что таблица линейного преобладания любого взаимно однозначного S-блока не содержит нечётных чисел. Что меняется, если S-блок не взаимно однозначен?

## 14.4 Дифференциальный криптоанализ

Другим статистическим методом криптоанализа в блочных шифров является *дифференциальный криптоанализ*. Он похож на линейный и так же требует знания структуры шифра и достаточного объёма выборки, состоящей из пар открытого и шифрованного текстов, полученных на одном и том же *неизвестном* ключе. Предложен он был в 1990 г. Эли Бихамом и Ади Шамиром.

Пусть  $P$  и  $P'$  — пара открытых текстов. Вектор, на который отличаются тексты, будем обозначать  $\Delta P = P \oplus P'$ . Аналогично вектор, на который отличаются шифртексты, обозначим  $\Delta C = C \oplus C'$ .

*Дифференциалом шифра* называется пара  $(\Delta P, \Delta C)$  такая, что пара открытых текстов отличающихся на вектор  $\Delta P$ , после зашифрования может перейти в пару шифртекстов, отличающихся на вектор  $\Delta C$ . Если пара переходит, то говорят, что дифференциал сохра-

нился. Дифференциальный криптоанализ заключается в поиске дифференциалов шифра, сохраняющихся с наибольшей вероятностью.

Так же как и в линейном криптоанализе, анализ шифра начинается с изучения S-блоков. Результат удобно представлять в виде таблицы дифференциалов. Рассмотрим построение таблицы дифференциалов следующего S-блока:

S-блок ( $4 \rightarrow 4$ )

|   | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|-----|-----|-----|-----|-----|-----|-----|-----|
| 0 | 14  | 4   | 13  | 1   | 2   | 15  | 11  | 8   |
| 1 | 3   | 10  | 6   | 12  | 5   | 9   | 0   | 7   |

Заметим, что это S-блок типа  $4 \rightarrow 4$ , поэтому таблица будет размера  $2^4$  на  $2^4$ . Обозначим вход и выход S-блока через  $x = (x_1, x_2, x_3, x_4)$  и  $y = (y_1, y_2, y_3, y_4)$  соответственно. Дифференциалом S-блока назовём пару  $(\Delta x, \Delta y)$ . Все дифференциалы S-блока могут быть протестиированы и вероятность того, что  $\Delta y$  обусловлена  $\Delta x$ , может быть получена путём рассмотрения пар  $(x, x')$ , таких что  $x \oplus x' = \Delta x$ . Строки таблицы дифференциалов это разности входов S-блока ( $\Delta x$ ), столбцы — разности выходов ( $\Delta y$ ).

|   | 0  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0  | 0 | 0 | 8 | 0 | 6 | 0 | 2 | 0 | 0 | 8 | 0 | 6 | 0 | 2 | 2 |
| 2 | 0  | 2 | 0 | 2 | 0 | 4 | 4 | 4 | 2 | 0 | 2 | 0 | 4 | 4 | 4 | 4 |
| 3 | 2  | 0 | 6 | 0 | 0 | 4 | 4 | 0 | 0 | 6 | 0 | 0 | 4 | 4 | 0 | 0 |
| 4 | 0  | 0 | 4 | 0 | 6 | 0 | 2 | 4 | 0 | 4 | 0 | 6 | 0 | 2 | 4 | 0 |
| 5 | 0  | 6 | 0 | 2 | 4 | 0 | 0 | 4 | 6 | 0 | 2 | 4 | 0 | 0 | 4 | 0 |
| 6 | 0  | 6 | 2 | 4 | 2 | 2 | 0 | 0 | 6 | 2 | 4 | 2 | 2 | 0 | 0 | 2 |
| 7 | 2  | 2 | 4 | 0 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 0 | 4 | 2 | 4 |
| 8 | 0  | 2 | 0 | 6 | 4 | 0 | 0 | 4 | 2 | 0 | 6 | 4 | 0 | 0 | 4 | 0 |
| 9 | 2  | 0 | 2 | 0 | 4 | 0 | 4 | 4 | 0 | 2 | 0 | 4 | 0 | 4 | 4 | 0 |
| a | 2  | 2 | 4 | 0 | 4 | 2 | 2 | 0 | 2 | 4 | 0 | 4 | 2 | 2 | 0 | 2 |
| b | 0  | 8 | 2 | 2 | 0 | 2 | 2 | 0 | 8 | 2 | 2 | 0 | 2 | 2 | 0 | 0 |
| c | 2  | 2 | 0 | 4 | 0 | 2 | 2 | 4 | 2 | 0 | 4 | 0 | 2 | 2 | 4 | 4 |
| d | 6  | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 |
| e | 4  | 2 | 2 | 0 | 0 | 0 | 6 | 2 | 2 | 2 | 0 | 0 | 0 | 6 | 2 | 0 |
| f | 0  | 2 | 2 | 4 | 2 | 6 | 0 | 0 | 2 | 2 | 4 | 2 | 6 | 0 | 0 | 0 |

Таблица дифференциалов S-блока

В таблице дифференциалов на пересечении строки  $u$  и столбца  $v$  находится число  $\lambda$  такое, что  $S(x \oplus u)$  совпадает с  $y \oplus v$  (при условии, что  $S(x) = y$ ) для  $\lambda$  различных  $x$ .

**Задача 673. Шаг 1.** Постройте таблицы дифференциалов для S-блоков шифра TwoFly, заданного в параграфе 14.3. Какой из S-блоков допускает дифференциал с наибольшей вероятностью? Определите лучший дифференциал для каждого из S-блоков.

**Задача 674. Шаг 2.** Используя дифференциалы S-блоков, полученные в задаче 673, найдите дифференциалы шифра TwoFly. С какой вероятностью шифр допускает эти дифференциалы? Какой дифференциал будет наилучшим, т. е. допускаться с наибольшей вероятностью?

**Задача 675. Шаг 3.** Как правило, во время криптоанализа криптоаналитик располагает некоторой выборкой. Какой объём выборки необходим, чтобы с вероятностью близкой к единице (например, 0,977) утверждать, что лучший дифференциал шифра TwoFly даёт верную информацию о ключе? Выразите биты ключа, насколько это возможно, через биты известных текстов.

**Задача 676. (\*)** Предложите S-блоки, которые обеспечат большую криптографическую стойкость шифра TwoFly к дифференциальному криптоанализу. Что именно можно улучшить в имеющихся S-блоках?

**Задача 677. (\*) Дифференциальный криптоанализ S-AES.** Проведите дифференциальный криптоанализ шифра S-AES. Рассмотрите два случая: когда раундовые ключи одинаковы и когда они разные. Оцените необходимый объём выборки для работы алгоритма с надежностью 0,8; 0,95; 0,99.

**Задача 678. Обратный анализ S-блока.** Найдите S-блок, таблицей дифференциалов которого является следующая таблица. Будет ли он единственным? Почему?

|   | 0  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0  | 0 | 0 | 8 | 0 | 6 | 0 | 2 | 0 | 0 | 8 | 0 | 6 | 0 | 2 | 2 |
| 2 | 0  | 2 | 0 | 2 | 0 | 4 | 4 | 4 | 2 | 0 | 2 | 0 | 4 | 4 | 4 | 4 |
| 3 | 2  | 0 | 6 | 0 | 0 | 4 | 4 | 0 | 0 | 6 | 0 | 0 | 4 | 4 | 0 | 0 |
| 4 | 0  | 0 | 4 | 0 | 6 | 0 | 2 | 4 | 0 | 4 | 0 | 6 | 0 | 2 | 4 | 0 |
| 5 | 0  | 6 | 0 | 2 | 4 | 0 | 0 | 4 | 6 | 0 | 2 | 4 | 0 | 0 | 4 | 0 |
| 6 | 0  | 6 | 2 | 4 | 2 | 2 | 0 | 0 | 6 | 2 | 4 | 2 | 2 | 0 | 0 | 2 |
| 7 | 2  | 2 | 4 | 0 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 0 | 4 | 2 | 4 |
| 8 | 0  | 2 | 0 | 6 | 4 | 0 | 0 | 4 | 2 | 0 | 6 | 4 | 0 | 0 | 4 | 0 |
| 9 | 2  | 0 | 2 | 0 | 4 | 0 | 4 | 4 | 0 | 2 | 0 | 4 | 0 | 4 | 4 | 0 |
| a | 2  | 2 | 4 | 0 | 4 | 2 | 2 | 0 | 2 | 4 | 0 | 4 | 2 | 2 | 0 | 2 |
| b | 0  | 8 | 2 | 2 | 0 | 2 | 2 | 0 | 8 | 2 | 2 | 0 | 2 | 2 | 0 | 0 |
| c | 2  | 2 | 0 | 4 | 0 | 2 | 2 | 4 | 2 | 0 | 4 | 0 | 2 | 2 | 4 | 4 |
| d | 6  | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 |
| e | 4  | 2 | 2 | 0 | 0 | 0 | 6 | 2 | 2 | 2 | 0 | 0 | 0 | 6 | 2 | 0 |
| f | 0  | 2 | 2 | 4 | 2 | 6 | 0 | 0 | 2 | 2 | 4 | 2 | 6 | 0 | 0 | 0 |

**Задача 679. Дифференциальный криптоанализ простого блочного шифра.** Реализуйте дифференциальный криптоанализ следующего четырёхраундового блочного шифра:

$P = (p_1, p_2, p_3, p_4, p_5, p_6)$  — открытый текст длины 6,

$K = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$  — ключ шифрования длины 8,

$C = (c_1, c_2, c_3, c_4, c_5, c_6)$  — шифртекст длины 6,

Подключи

$K_1 = (k_1, k_2, k_3, k_4, k_5, k_6)$  — подключ 1-го раунда,

$K_2 = (k_3, k_4, k_5, k_6, k_7, k_8)$  — подключ 2-го раунда,

$K_3 = (k_5, k_6, k_7, k_8, k_1, k_2)$  — подключ 3-го раунда,

$K_4 = (k_7, k_8, k_1, k_2, k_3, k_4)$  — подключ 4-го раунда,

S-блоки: вход и выход — векторы длины 3

$S_1 = (0, 5, 7, 2, 3, 4, 1, 6)$ ,

$S_2 = (6, 1, 2, 0, 5, 4, 3, 7)$ .

Пусть  $C_0 = P$ . Опишем раунд шифрования номер  $i$ , где  $i = 1, 2, 3, 4$ .

Полагаем  $C_i = (S_1(L_i), S_2(R_i))$ , где  $(L_i, R_i) = C_{i-1} \oplus K_i$  и векторы  $L_i$ ,  $R_i$  имеют длину 3. Результат зашифрования  $C = C_4$ .

## 14.5 Алгебраический криптоанализ

Идея алгебраического криптоанализа шифра заключается в описании шифра с помощью системы булевых уравнений на биты открытого

того текста, ключа и шифртекста, при условии, что криптоаналитик заранее знает, как устроен шифр. Обладая дополнительной информацией, например, некоторыми известными битами открытого или зашифрованного сообщения, либо дополнительными связями между битами, криптоаналитик пытается её решить и восстановить секретное сообщение и ключ. Не всегда решение может восстанавливаться единственным образом, однако заведомо известно, что хотя бы одно решение существует.

**Задача 680.** При анализе шифра возникла следующая система линейных булевых уравнений на биты ключа:

$$\left\{ \begin{array}{l} x_2 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_8 = b_1 \\ x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_8 = b_2 \\ x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 = b_3 \\ x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 = b_4 \\ x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8 = b_5 \\ x_1 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_8 = b_6 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_8 = b_7 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7 = b_8, \end{array} \right.$$

Решите её, если вектор  $b = (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)$  имеет вид:

- |                      |                      |
|----------------------|----------------------|
| а) $b = (00000000);$ | б) $b = (11111111);$ |
| в) $b = (11110110);$ | г) $b = (01100111);$ |
| д) $b = (10101010);$ | е) $b = (01000011);$ |
| ж) $b = (10101001);$ | з) $b = (11100001).$ |

**Задача 681.** Проверьте, является ли каждая из следующих систем булевых уравнений совместной. Если да, найдите все её решения.

|  |  |
|--|--|
| а) $\left\{ \begin{array}{l} x_1x_2x_3 = 0, \\ x_1 \oplus x_2 \oplus x_3 = 0, \\ x_1x_2 \oplus x_3 = 1, \\ x_2x_3 \oplus x_1 = 0; \end{array} \right.$           | б) $\left\{ \begin{array}{l} x_1x_2x_3 = 0, \\ x_1 \oplus x_2 \oplus x_3 = 0, \\ x_1x_2 \oplus x_3 = 0, \\ x_2x_3 \oplus x_1 = 0; \end{array} \right.$ |
| в) $\left\{ \begin{array}{l} x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2 = 1, \\ x_2x_4x_5 \oplus x_2x_4 \oplus x_4x_5 \oplus x_4 = 1; \end{array} \right.$ |  |

$$\begin{array}{ll}
 \text{г) } \left\{ \begin{array}{l} x_1x_2 \oplus x_3x_4 = 0, \\ x_2x_4 \oplus x_1x_3 = 0, \\ x_1 \oplus x_2x_3x_4 = 0, \\ x_1 \oplus x_2 \oplus x_4 = 1, \\ x_1 \oplus x_3 \oplus x_4 = 1; \end{array} \right. & \text{д) } \left\{ \begin{array}{l} x_1x_2 \oplus x_3x_4 = 0, \\ x_2x_4 \oplus x_1x_3 = 0, \\ x_1 \oplus x_2x_3x_4 = 1, \\ x_1 \oplus x_2 \oplus x_4 = 1, \\ x_1 \oplus x_3 \oplus x_4 = 1; \end{array} \right. \\
 \text{е) } \left\{ \begin{array}{l} (x_1 \oplus x_2)(x_5 \oplus x_6) = 1, \\ (x_3 \oplus x_4)(x_7 \oplus x_8) = 1, \\ (x_2 \oplus x_3)(x_6 \oplus x_7) = 1, \\ (x_4 \oplus x_5)(x_8 \oplus x_1) = 1; \end{array} \right. & \text{ж) } \left\{ \begin{array}{l} (x_1 \oplus x_2)(x_5 \oplus x_6) = 1, \\ (x_3 \oplus x_4)(x_7 \oplus x_8) = 1, \\ (x_2 \oplus x_3)(x_6 \oplus x_7) = 1, \\ (x_4 \oplus x_5)(x_7 \oplus x_1) = 1. \end{array} \right. 
 \end{array}$$

**Задача 682.** Найдите все решения систем булевых уравнений

$$\begin{array}{ll}
 \text{а) } \left\{ \begin{array}{l} x_1x_2 \oplus x_1 \oplus 1 = 0, \\ x_3x_4 \oplus x_2 \oplus x_1 = 0; \end{array} \right. & \text{б) } \left\{ \begin{array}{l} x_1 \oplus x_2 \oplus x_3 = 0, \\ x_2 \oplus x_3 \oplus x_4 = 0, \\ x_1 \oplus x_2x_3 = 1; \end{array} \right. \\
 \text{в) } \left\{ \begin{array}{l} x_1x_2x_3x_4 \oplus x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_2x_3 = 1, \\ x_5x_6x_7x_8 \oplus x_5x_6x_8 \oplus x_6x_7x_8 \oplus x_6x_8 = 1; \end{array} \right. & \\
 \text{г) } (x_1 \oplus 1)(x_1x_2 \oplus 1)(x_1x_3 \oplus 1)(x_2x_4 \oplus 1) = 1; & \\
 \text{д) } \left\{ \begin{array}{l} x_1x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3 = 1, \\ x_2x_3x_4 \oplus x_3x_4 \oplus x_2 \oplus x_3 = 0; \end{array} \right. & 
 \end{array}$$

**Задача 683. Алгебраический криптоанализ блочного шифра.** Опишем простой блочный шифр. Пусть  $P = (p_1, p_2, p_3)$  — открытый текст,  $K = (k_1, k_2, k_3)$  — ключ,  $C = (c_1, c_2, c_3)$  — шифртекст, который получается следующим образом:  $C = S(P \oplus K)$ , где  $S$  — векторная  $3 \rightarrow 3$  функция такая, что  $S(x_1, x_2, x_3) = (x_2, x_1, x_1x_2 \oplus x_3)$ . Методом алгебраического криптоанализа определите неизвестный ключ  $K$  по известной паре «открытый текст — шифртекст»:  $P = (101)$ ,  $C = (111)$ .

**Задача 684. Криптоанализ поточного шифра.** Опишем простой поточный шифр. Пусть  $P = (p_1, p_2, \dots)$  — последовательность битов открытого текста. Каждый бит  $p_i$  складывается по модулю 2 с битом  $\gamma_i$  гаммы  $\Gamma = (\gamma_1, \gamma_2, \dots)$  и таким образом получается шифртекст  $C$ , т. е.  $C = (p_1 \oplus \gamma_1, p_2 \oplus \gamma_2, \dots)$ . Гамма порождается с помощью шестибитового ключа  $K = (k_1, k_2, k_3, k_4, k_5, k_6)$  следующим образом: первые шесть битов гаммы совпадают с соответствующими битами ключа,

$\gamma_n = k_n$  при  $n = 1, \dots, 6$ , а дальше гамма генерируется с помощью рекуррентного соотношения  $\gamma_n = \gamma_{n-1} \oplus \gamma_{n-3} \oplus \gamma_{n-6}$  при  $n \geq 7$ .

Злоумышленнику удалось перехватить часть информации об открытом тексте  $P$  и шифртексте  $C$ . Биты, оставшиеся неизвестными, помечены знаком \*. Восстановите ключ по следующей информации:

- а)  $P = (\ast\ast\ast\ast 1 * 111011 \ast\ast\ast 11 \ast \dots)$ ,  $C = (\ast\ast 0 \ast\ast\ast 000111 * 1 \ast\ast\ast \dots)$ ;
- б)  $P = (01 * 10 * 10101111 \ast\ast\ast \dots)$ ,  $C = (\ast 1 * 1 \ast\ast 0 \ast\ast 11 * 1 \ast\ast 01 \ast \dots)$ ;
- в)  $P = (0 * 1 * 001 \ast\ast 101 \ast\ast\ast\ast\ast \dots)$ ,  $C = (01 \ast\ast 0 * 1 * 1011 \ast\ast 110 \ast \dots)$ .

**Задача 685. Фильтрующий генератор.** Опишем простую модель фильтрующего генератора и построенного на его основе поточного шифра. Пусть  $P = (p_1, p_2, \dots)$  — последовательность битов открытого текста. Каждый бит  $p_i$  складывается по модулю 2 с битом  $\gamma_i$  гаммы  $\Gamma = (\gamma_1, \gamma_2, \dots)$  и таким образом получается шифртекст  $C$ , т. е.  $C = (p_1 \oplus \gamma_1, p_2 \oplus \gamma_2, \dots)$ .

Гамма порождается следующим образом.

Сначала с помощью четырёхбитового ключа  $K = (k_1, k_2, k_3, k_4)$  порождается последовательность битов  $\beta = (\beta_1, \beta_2, \dots)$  так, что первые четыре бита последовательности совпадают с соответствующими битами ключа,  $\beta_n = k_n$  при  $n = 1, \dots, 4$ , а дальше элементы  $\beta$  генерируются с помощью рекуррентного соотношения

$$\beta_n = \beta_{n-1} \oplus \beta_{n-3} \oplus \beta_{n-4} \text{ при } n \geq 5.$$

Заметим, что выработку последовательности  $\beta$  можно смоделировать работой регистра сдвига с линейной обратной связью длины 4.

Гамма  $\Gamma$  порождается по последовательности  $\beta$  с помощью нелинейной функции (так называемая фильтрующая модель генератора):

$$\gamma_n = \beta_n \beta_{n+2} \oplus \beta_{n+3} \text{ при } n \geq 1.$$

При передаче информации злоумышленнику удалось перехватить часть битов открытого текста  $P$  и шифртекста  $C$ . Биты, оставшиеся неизвестными, помечены знаком \*. Можно ли восстановить ключ  $K$  по имеющейся информации? Если да, проделайте это. В каждом случае восстановите максимум информации о ключе.

- а)  $P = (\ast\ast\ast\ast\ast\ast 1 \ast\ast\ast 0 \ast\ast\ast 0 \ast\ast\ast 1 \ast\ast\ast 1 \ast\ast\ast\ast\ast \dots)$ ,  
 $C = (\ast\ast 0 \ast\ast\ast\ast\ast\ast\ast\ast 1 \ast\ast\ast 0 \ast\ast\ast 1 \ast\ast\ast 0 \ast\ast\ast\ast\ast \dots)$ ;

- б)  $P = (* 0 1 1 1 0 * 0 * * 1 1 * * 0 0 * * * 0 1 1 1 0 1 * * * * 1 1 * \dots)$ ,  
 $C = (* * * * * * 1 * 1 0 * * 0 * * * 1 1 * * * * * * 1 0 0 1 * * * \dots)$ ;
- в)  $P = (* * * * * * * 0 * * * * * * * * * * * 0 * 0 * * 1 * * * * \dots)$ ,  
 $C = (* * * * * * * * * * * * * * * * * * 1 0 * 1 * * 1 * * * * \dots)$ ;
- г)  $P = (* 0 1 1 1 0 * 0 * * 1 1 * * 0 0 * * * 0 1 1 1 0 1 * * * * 1 1 * \dots)$ ,  
 $C = (* * * * * * 1 * 1 0 * 0 0 * * * 1 1 * * * * * * 1 0 0 1 * * * \dots)$ .

**Задача 686. «Многоразовый» блокнот.** Абонент зашифровал двоичный вектор  $P = (p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9)$  длины 9 с помощью шифра «одноразовый блокнот». Правда, он допустил оплошность: для зашифрования он три раза подряд использовал один и тот же ключ  $K = (k_1, k_2, k_3)$  длины 3. Шифртекст, который перехватил злоумышленник, выглядел так:  $C = (001 101 011)$ . В каждом случае восстановите ключ  $K$  и открытый текст  $P$  по дополнительной известной информации:

- а)  $p_1 = 1, k_3 = 0$ ;
- б)  $(p_1 \oplus p_2)(p_4 \oplus p_6) = 1$ ;
- в)  $p_1 p_3 p_8 \oplus p_5 p_7 \oplus p_4 = 0$ ;
- г)  $p_2 p_4 p_5 p_6 \oplus p_2 p_4 p_6 p_9 \oplus p_2 p_4 p_6 \oplus p_1 p_4 p_5 \oplus p_1 p_4 p_9 \oplus p_1 p_4 = 1$ ;
- д)  $p_3 p_4 p_8 \oplus p_4 p_6 \oplus p_5 p_9 \oplus p_3 \oplus p_9 = 1$ ;
- е)  $p_1 p_2 p_3 \oplus p_1 p_2 \oplus p_1 p_3 \oplus p_2 p_3 \oplus p_1 \oplus p_2 \oplus p_3 = 0$ .

**Задача 687. Алгебраический криптоанализ SP-сети.** Рассмотрим следующий блочный шифр. Пусть число раундов равно трём.

$$\begin{aligned} P &= (p_1, p_2, p_3, p_4, p_5, p_6) — \text{открытый текст длины 6}, \\ K &= (k_1, k_2, k_3, k_4, k_5, k_6) — \text{ключ шифрования длины 6}, \\ C &= (c_1, c_2, c_3, c_4, c_5, c_6) — \text{шифртекст длины 6}. \end{aligned}$$

Подключи:

$$\begin{aligned} K_1 &= (k_1, k_2, k_3, k_4, k_5, k_6) — \text{подключ 1-го раунда}, \\ K_2 &= (k_4, k_5, k_6, k_3, k_1, k_2) — \text{подключ 2-го раунда}, \\ K_3 &= (k_2, k_6, k_1, k_5, k_3, k_4) — \text{подключ 3-го раунда}. \end{aligned}$$

S-блок: вход и выход — векторы длины 3,

$$S = (1, 0, 3, 6, 7, 4, 5, 2).$$

Пусть  $C_0 = P$ . Опишем раунд шифрования номер  $i = 1, 2, 3$ .

$$(L_i, R_i) = C_{i-1} \oplus K_i, \text{ где } L_i, R_i — \text{векторы длины 3},$$

$$V_i = (S(L_i), S(R_i)),$$

$$C_i = V_i \lll 2.$$

Шифртекст  $C = C_3$ .

Методом алгебраического криптоанализа найдите ключ  $K$ , если

- а) был выполнен один раунд шифрования, в результате чего вектор  $P = (101001)$  перешёл в  $C_1 = (110111)$ .
- б) были проведены два раунда шифрования, при этом вектор  $P = (100001)$  перешёл в  $C_2 = (100101)$ .

# ГЛАВА 15. ТРУДНЫЕ И НЕРЕШЁННЫЕ ЗАДАЧИ О БУЛЕВЫХ ФУНКЦИЯХ

В этой главе мы предлагаем вам подборку трудных и нерешённых задач о криптографических свойствах булевых функций. Чтобы вдохновить вас, отметим, что решение каждой задачи с тремя звёздочками заслуживает представления на криптографической конференции и публикации в научном журнале. Успехов!



## 15.1 Экстремальные булевые функции

Для использования булевых функций в криптографических целях требуется находить такие их конструкции, которые бы позволили совместить и оптимизировать сразу несколько криптографических свойств. Среди них — высокая нелинейность, алгебраическая иммунность и другие свойства (подробно мы рассматривали их в главе 12).

**Задача 688. (\*\*\*) Нерешённая: максимальная нелинейность.** Определите максимально возможное значение нелинейности булевой функции от  $n$  переменных в случае, если  $n$  нечётно.

Серия вопросов возникает в связи с алгебраическими конструкциями бент-функций (см. алгебраическое представление булевых функций в разделе 11.7).

Бент-функции, имеющие вид  $f(c) = \text{tr}(ac^d)$ , где  $a \in GF^*(2^n)$  — некоторый параметр, называются *мономиальными*, а целое число  $d$  называется *бент-показателем*. Известен следующий результат.

**Теорема 15. (Мономиальные конструкции.)** Следующие значения  $d$  являются бент-показателями:

$$d = 2^{n/2} - 1;$$

$$d = 2^i + 1, \text{ где } \overline{\text{НОД}}_{(n,i)}^n \text{ чётно;}$$

$$d = 2^{2k} - 2^k + 1, \text{ где } \text{НОД}(k, n) = 1 \text{ и } n \text{ не делится на } 3;$$

$$d = (2^k + 1)^2, \text{ где } n = 4k, k \text{ нечётно;}$$

$$d = 2^{2k} + 2^k + 1, \text{ где } n = 6k.$$

**Задача 689. (\*\*\*) Нерешённая: бент-показатели.** Найдите другие бент-показатели или докажите, что их не существует.

**Задача 690. (\*\*\*) Нерешённая: бент-конструкции.** Предложите новые конструкции бент-функций от  $n$  переменных. Обзор известных конструкций можно найти в [42].

**Задача 691. (\*\*\*) Нерешённая: оценки бент-функций.** Получите новые нижние и верхние оценки числа всех бент-функций от  $n$  переменных.

**Задача 692. (\*\*\*) Нерешённая: сумма бент-функций.** Верно ли, что любая булева функция от  $n$  переменных ( $n$  чётно) степени не выше  $n/2$  представима в виде суммы двух бент-функций от  $n$  переменных? Если нет, постройте контрпример.

Детальные обзоры по бент-функциям и их конструкциям можно найти в книгах [44], [32].

Приведём подборку задач, связанных с алгебраической иммунностью булевой функции.

**Задача 693. (\*\*)  $AI +$  Лемма о милиционерах.** Пусть  $g_1, g_2$  — булевые функции от  $n$  переменных ( $n$  чётно) такие, что их алгебраическая иммунность максимальна, т. е.  $AI(g_1) = AI(g_2) = n/2$ . Пусть

$f$  — булева функция от  $n$  переменных такая, что для её носителя выполнены условия:  $\text{supp}(f) \supseteq \text{supp}(g_1)$ ,  $\text{supp}(f \oplus 1) \supseteq \text{supp}(g_2)$ .

Докажите, что алгебраическая иммунность функции  $f$  также является максимальной, т. е.  $AI(f) = n/2$ . Функции  $g_1$  и  $g_2$  называются *ограничивающими* для функции  $f$ .

**Задача 694. (\*\*)** *AI + Существование границ.* Докажите, что для любой булевой функции  $f$  от  $n$  переменных ( $n$  чётно) такой, что  $AI = n/2$ , существуют ограничивающие функции  $g_1, g_2$ .

Многие задачи совмещения высокой алгебраической иммунности с другими криптографическими свойствами остаются нерешёнными.

**Задача 695. (\*\*\*)** *Нерешённая: AI + сбалансированность.* Определите максимально возможное значение алгебраической иммунности функции в классе сбалансированных булевых функций от  $n$  переменных. Получите классификацию/описание множества всех сбалансированных булевых функций с максимальной алгебраической иммунностью.

**Задача 696. (\*\*)** *AI + бент.* Определите максимально возможное значение алгебраической иммунности функции в классе булевых бент-функций от  $n$  переменных ( $n$  чётно).

**Задача 697. (\*\*\*)** *Нерешённая: AI + бент.* Получите классификацию/описание множества всех бент-функций с максимальной алгебраической иммунностью.

**Задача 698. (\*\*\*)** *Нерешённая: AI + бент. Оценки.* Получите нетривиальную верхнюю оценку алгебраической иммунности произвольной бент-функции от  $n$  переменных из какого-либо специального класса, например из класса Мэйорана — МакФарланда,  $\mathcal{PS}$ , класса мономиальных функций и др.

**Задача 699. (\*\*\*)** *Нерешённая: AI + максимальная нелинейность.* Определите максимально возможное значение алгебраической иммунности функции в классе максимально нелинейных булевых функций от  $n$  переменных ( $n$  нечётно). Получите классификацию/описание множества всех максимально нелинейных булевых функций с максимальной алгебраической иммунностью.

Векторные булевые функции являются ещё более загадочными объектами. При исследовании их криптографических свойств гораздо больше вопросов, чем ответов.

**Теорема 16. (Мономиальные APN-функции.)** Пусть  $F = x^d$ ,  $F : GF(2^n) \rightarrow GF(2^n)$ , — мономиальная функция. Тогда при показателях  $d$ , приведённых в таблице,  $F$  — APN-функция.

| Функция   | $d$   | Условия          | $\deg(F)$              |
|-----------|---|------------------|------------------------|
| Gold      | $d = 2^i + 1$   | $\gcd(i, n) = 1$ | 2                      |
| Kasami    | $d = 2^{2i} - 2^i + 1$  | $\gcd(i, n) = 1$ | $i + 1$                |
| Welch     | $2^t + 3$   | $n = 2t + 1$     | 3                      |
| Niho      | $2^t + 2^{\frac{t}{2}} - 1$ , если $t$ чётно<br>$2^t + 2^{\frac{3t+1}{2}} - 1$ , если $t$ нечётно | $n = 2t + 1$     | $(t + 1)/2$<br>$t + 1$ |
| Inverse   | $2^{2t} - 1$  | $n = 2t + 1$     | $n - 1$                |
| Dobbertin | $2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$  | $n = 5t$         | $i + 3$                |

**Задача 700.** (\*\*\*) Докажите теорему 16.

**Задача 701.** (\*\*\*)  
Нерешённая: мономиальные APN-функции.  
Найдите другие мономиальные APN-функции или докажите, что их не существует.

**Задача 702.** (\*\*) Взаимно однозначные APN-функции при нечётном  $n$ . Докажите, что при любом нечётном  $n \geq 3$  существуют взаимно однозначные APN-функции от  $n$  переменных.

**Задача 703.** (\*\*\*)  
Нерешённая: взаимно однозначные APN-функции.  
Определите, существуют ли взаимно однозначные APN-функции от  $n$  переменных при чётном  $n$  таком, что  $n \geq 8$ ?

**Задача 704.** (\*\*\*)  
Нерешённая: итеративные конструкции APN-функций.  
Предложите итеративную конструкцию APN-функций, т. е. способ построения APN-функции от большего числа переменных с помощью известных APN-функций от меньшего числа переменных. Отдельно рассмотрите случаи чётного и нечётного  $n$ .

## 15.2 Автоморфизмы различных классов булевых функций

Отображение  $\varphi$  множества всех булевых функций от  $n$  переменных в себя называется *изометричным*, если оно сохраняет расстояния между булевыми функциями, т. е.  $dist(\varphi(f), \varphi(g)) = dist(f, g)$ . Известно, что любое такое отображение однозначно представляется в виде

$$g(x) \rightarrow g(s(x)) \oplus f(x), \quad (15.1)$$

где  $s : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  — любая подстановка,  $f$  — произвольная функция от  $n$  переменных.

*Группой автоморфизмов* подмножества булевых функций  $\mathcal{M}$  называется группа изометричных отображений множества всех булевых функций в себя, оставляющих неподвижным множество  $\mathcal{M}$ . Обозначим эту группу через  $Aut(\mathcal{M})$ .

**Задача 705.** Докажите, что класс  $\mathcal{B}_n$  бент-функций замкнут относительно любого невырожденного аффинного преобразования переменных, а также прибавления любой аффинной функции.

**Задача 706. (\*\*)** Докажите, что для любой неаффинной булевой функции  $f$  от  $n$  переменных ( $n$  чётно) найдется такая бент-функция  $g$  от  $n$  переменных, что функция  $f \oplus g$  не является бент-функцией.

**Задача 707. (\*) Группа автоморфизмов бент-функций.** Опираясь на задачу 706, докажите, что любой автоморфизм множества всех бент-функций является комбинацией невырожденного аффинного преобразования переменных и прибавления аффинной функции. Другими словами, если отображение (15.1) переводит класс бент-функций в себя, то оно имеет вид  $g(x) \rightarrow g(Ax \oplus b) \oplus \langle c, x \rangle \oplus d$ .

**Задача 708. (\*\*\*) Нерешённая.** Найдите группу автоморфизмов множества булевых функций с максимальной алгебраической иммунностью. Рассмотрите случаи чётного и нечётного  $n$ .

**Задача 709. (\*\*\*) Нерешённая.** Найдите группу автоморфизмов множества корреляционно-иммунных функций порядка  $r$ .

### 15.3 Бент-функции и сильно регулярные графы

Пусть  $f$  — булева функция от  $n$  переменных. Через  $\text{supp}(f)$  обозначим её *носитель*, т. е. множество всех двоичных векторов длины  $n$ , на которых функция  $f$  принимает значение 1. Напомним, что мощность носителя называется *весом* функции  $f$ .

Рассмотрим *граф Кэли*  $G_f = G(\mathbb{Z}_2^n, \text{supp}(f))$  булевой функции  $f$ . Вершинами графа являются все векторы длины  $n$ . Две вершины  $x, y$  соединяются ребром, если вектор  $x \oplus y$  принадлежит множеству  $\text{supp}(f)$ . Граф  $G$  называется *сильно регулярным с параметрами*  $(v, k, \lambda, \mu)$ , если он содержит  $v$  вершин, степень каждой вершины равна  $k$  и для любых двух вершин  $x, y$  число общих смежных им вершин равно  $\lambda$  или  $\mu$  в зависимости от того, соединены вершины  $x, y$  ребром или нет.

Напомним, что булева функция  $f$  от чётного числа переменных  $n$  называется *бент-функцией*, если её производная по любому ненулевому направлению  $u \in \mathbb{Z}_2^n$  уравновешена, т. е. выполняется

$$\sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus f(x \oplus u)} = 0.$$

Отметим, что вес произвольной бент-функции равен  $2^{n-1} \pm 2^{\frac{n}{2}-1}$ .

**Теорема 17.** *Булева функция  $f$  — бент-функция тогда и только тогда, когда граф  $G_f$  сильно регулярный, причём  $\lambda = \mu$ .*

Теорема 17 следует из задач 710, 711 и 712. Решите их.

**Задача 710. (\*) Свойства графа Кэли бент-функции.** Докажите, что график Кэли  $G_f$  бент-функции  $f$  от  $n$  переменных сильно регулярный с параметрами  $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, \lambda = \mu = 2^{n-2} \pm 2^{\frac{n}{2}-1})$ . Знаки  $\pm$  согласованы, т. е. одинаковы в обоих случаях.

**Задача 711.** Докажите, что если график Кэли  $G_f$  булевой функции от  $n$  переменных имеет параметры из задачи 710, то  $f$  — бент-функция.

**Задача 712. (\*\*)** *Свойства графа Кэли на  $2^n$  вершинах.* Докажите, что если  $G$  — сильно регулярный график на  $2^n$  вершинах,  $n \geq 2$ , такой, что  $\lambda = \mu > 0$ , то он имеет параметры из задачи 710.

**Задача 713.** (\*\*). Верно ли, что произвольный сильно регулярный граф на  $2^n$  вершинах изоморчен графу Кэли некоторой булевой функции от  $n$  переменных?

Дадим геометрическую интерпретацию задач 710, 711 и 712.

Подмножество  $M \subseteq \mathbb{Z}_2^n$  назовём *сильно*  $(k, \lambda)$ -*регулярным*, если его мощность равна  $k$  и мощность пересечения  $M$  с любым его сдвигом  $M+y$ , где  $y \neq 0$ , равна  $\lambda$ . Назовём такое множество *собственным*, если  $0 < k < 2^n$ ,  $0 < \lambda < 2^n$ . Решите следующие задачи.

**Задача 714.** Докажите, что множество  $M \subseteq \mathbb{Z}_2^n$  сильно  $(k, \lambda)$ -регулярно тогда и только тогда, когда график Кэли функции  $f$  такой, что  $supp(f) = M$ , является сильно регулярным с параметрами  $(2^n, k, \lambda, \lambda)$ .

**Задача 715.** Докажите, что носитель произвольной бент-функции является сильно регулярным множеством.

**Задача 716.** Покажите, что каждое собственное сильно регулярное множество в  $\mathbb{Z}_2^n$  является носителем некоторой бент-функции от  $n$  переменных и имеет параметры  $(2^{n-1} \pm 2^{(n/2)-1}, 2^{n-2} \pm 2^{(n/2)-1})$ .

# ГЛАВА 16. ЗАДАЧИ НА ПРОГРАММИРОВАНИЕ

При решении задач по криптографии часто требуется хорошее знание программирования. В первом разделе этой главы мы собрали задачи, которые помогут вам получить простые навыки программирования. Во втором — серию задач, рассчитанных на уверенных программистов, желающих приложить свои силы в новой области.

## 16.1 Простые навыки

Изучите основную структуру программы, раздел описаний и раздел операторов, операторы присваивания, ввода-вывода, основные типы переменных и операции  $+, -, *, /$  и др. над переменными различных типов. Научитесь компилировать программу и запускать её на исполнение.

**Задача 717. Обмен значениями.** Напишите программу, которая обменивает значения двух переменных  $x$  и  $y$  целого типа с использованием дополнительной переменной  $z$  и без неё.

**Задача 718. Сумма чисел.** Напишите программу, вычисляющую для натурального числа  $n$ , введённого с клавиатуры, сумму всех натуральных чисел от 1 до  $n$  (включительно). Изучите циклические конструкции языка программирования.

**Задача 719. Возведение в степень.** Напишите программу возведения целого числа  $0 < x < 10$  в натуральную степень  $k$ . Оба числа вводятся пользователем с клавиатуры. Выполните это задание тремя различными способами — используя конструкции цикла со счетчиком, цикла с условием и цикла с постусловием.

**Задача 720. Число дней в месяце.** Напишите программу, которая по введённому номеру месяца високосного или невисокосного года выводит количество дней в месяце.

**Задача 721. Делители.** Для введённого пользователем натурального числа  $n$  программа выводит на печать все делители числа  $n$  (в том числе 1 и  $n$ ). Преобразуйте программу так, чтобы число выполняемых итераций цикла было минимальным (чemu оно будет равно?). Изучите операции целочисленного деления и деления с остатком над переменными целых типов.

**Задача 722. Работа с файлами.** В текстовом файле `input.txt` через пробел записаны целые числа. Напишите программу, которая считывала бы их из файла и печатала на экран.

**Задача 723. Шифр Цезаря.** Пусть в текстовом файле `input.txt` Алиса сохранила секретное текстовое сообщение в алфавите из следующих 32 букв:

|                              |                              |                              |                              |
|------------------------------|------------------------------|------------------------------|------------------------------|
| 0, 1, 2, 3<br>А, Б, В, Г     | 4, 5, 6, 7<br>Д, Е, Ж, З     | 8, 9, 10, 11<br>И, –, К, Л   | 12, 13, 14, 15<br>М, Н, О, П |
| 16, 17, 18, 19<br>Р, С, Т, У | 20, 21, 22, 23<br>Ф, Х, Ц, Ч | 24, 25, 26, 27<br>Ш, Щ, Ъ, Ы | 28, 29, 30, 31<br>Ь, Э, Ю, Я |

Напишите программу, которая производит зашифрование этого сообщения с помощью шифра Цезаря с шагом  $k$  (это общий секрет Алисы и Боба) и записывает результат в файл `output.txt`. Составьте программу-десифратор и попробуйте себя в роли криптоаналитика: десифруйте перехваченное сообщение от Боба (при неизвестном ключе  $k$ ):

ФЮАЮУ РПЩРЫ ШБРЩЬ ЭХЩЪР ЦХВБП  
ЩЭРБЩ ЯЮФБЫ ГИШТР ОВЩВТ ЮЩСЮС.

Изучите работу с массивами и текстовыми файлами.

**Задача 724. Треугольник Паскаля.** Напечатайте  $n$  строк треугольника Паскаля. Модифицируйте программу так, чтобы результат записывался в отдельный файл.

**Задача 725. (\*) Сортировка массива.** Заполните массив целыми числами из входного файла.

а) Отсортируйте массив по возрастанию (или убыванию) одним из методов сортировки (методом пузырька, простыми вставками, простым выбором или более сложными методами, такими как метод Шелла, quick-sort, пирамидалная сортировка).

б) Осуществите в отсортированном массиве бинарный поиск некоторого заданного элемента  $x$ . Покажите, что его сложность пропорциональна  $\log_2 n$ , где  $n$  — число элементов массива.

в) Осуществите в отсортированном массиве пропорциональный поиск некоторого заданного элемента  $x$ . В каком случае сложность поиска будет пропорциональна  $\log_2 \log_2 n$ , где  $n$  — число элементов массива?

**Задача 726. (\*) Перестановки.** Для заданного  $n$ ,  $2 \leq n \leq 10$ , выведите на печать все перестановки на  $n$  элементах и их число. Например, для  $n = 3$ , должно получаться

$$6 : \{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}.$$

Изучите способы организации программы с помощью процедур и функций, а также рекурсивные алгоритмы.

**Задача 727. Рекурсивный факториал.** Напишите рекурсивную программу вычисления факториала числа  $n$ , введённого пользователем.

**Задача 728. Двоичное представление.** Напишите программу, которая для натурального числа  $N$ , введённого пользователем, находит и печатает на экран его двоичное представление. Например, число 75 раскладывается следующим образом:  $75 = 64 + 8 + 2 + 1 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ . Тогда на экран выводится 1001011.

**Задача 729. Факториальное представление.** Известно, что любое натуральное число  $N$  можно единственным способом представить с помощью последовательности неотрицательных целых чисел  $a_1, \dots, a_n$  в виде:  $N = a_n \cdot n! + a_{n-1} \cdot (n-1)! + \dots + a_1 \cdot 1!$ , где  $0 \leq a_i \leq i$  для всех  $i = 1, \dots, n$ . Требуется перевести десятичное число в факториальную систему счисления.

Формат входных данных: во входном файле (`input.txt`) записано одно десятичное число  $N$ . Формат выходных данных: выведите в выходной файл (`output.txt`) представление числа  $N$  в факториальной системе счисления. Например, число 55 раскладывается следующим образом:  $55 = 2 \cdot 4! + 1 \cdot 3! + 0 \cdot 2! + 1 \cdot 1!$  Тогда в выходном файле в новой строке следует написать:  $5510 = 2.1.0.1!$

**Задача 730. День недели.** Напишите программу, выводящую на экран день недели по введённой точной дате. Не забудьте учесть високосные годы.

**Задача 731. (\*) Шахматная доска.** Задана шахматная доска размера  $n \times n$  (для любого  $n$ ,  $4 \leq n \leq 8$ ) и выбрана начальная клетка с координатами  $(x, y)$ . Начиная с указанной клетки найдите такой обход конем шахматной доски, в котором каждая клетка проходилась бы ровно один раз (если такой обход существует). Выведите на печать последовательность шагов обхода доски. Используйте для этого рекурсивную процедуру. Как найти все различные обходы?

**Задача 732. Поиск короткого пути.** Пусть во входном файле заданы число городов  $n$  и матрица размера  $n \times n$ , в которой элемент  $i$ -й строки и  $j$ -го столбца (целое число) равен длине прямой дороги, соединяющей  $i$ -й и  $j$ -й города, или  $-1$ , если прямой дороги между ними нет. Напишите программу, которая по двум введённым номерам городов определяет самый короткий путь между ними. Например, для введённых городов 2 и 9 выводит цепочку вида  $2 \rightarrow 3 \rightarrow 6 \rightarrow 15 \rightarrow 8 \rightarrow 9$ , длина пути 28.

**Задача 733. Быки и коровы.** Пользователь загадывает число из  $n$  цифр (например,  $n = 4$ ), каждая из которых от 1 до  $m$  (например,  $m = 6$ ), причём все цифры различны. Разработайте алгоритм, который угадывает число по следующим правилам: выводится число и пользователь сообщает, сколько в нём «быков» и «коров», т. е. сколько цифр стоят на своих местах и сколько цифр содержатся в обоих числах, но совпадают лишь по значению. Например, пусть пользователь загадал число 1264, компьютер спрашивает 1256. В этом случае два быка (1, 2) и одна корова (6).

**Задача 734. Числа Фибоначчи I.** Выведите на экран  $n$ -е число Фибоначчи.

**Задача 735. Числа Фибоначчи II.** Пусть числа Фибоначчи определяются начальными значениями  $U[1] = 1$ ,  $U[2] = 2$  и соотношением  $U[N + 1] = U[N] + U[N - 1]$ . Рассмотрим систему счисления с двумя цифрами 0 и 1, в которой, в отличие от двоичной системы, весами являются не степени двойки  $1, 2, 4, 8, 16, \dots$ , а числа Фибоначчи  $1, 2, 3, 5, 8, 13, \dots$  В этой системе счисления каждое положительное целое число единственным образом представляется в виде строки нулей и единиц, которая начинается с 1 и в которой нет двух единиц, стоящих рядом.

Даны две строки, представляющие числа  $A$  и  $B$ . Найдите строку, представляющую число  $A + B$ . Пример: исходные строки '10101' и '100' представляют числа  $8 + 3 + 1 = 12$  и 3. Ответом является строка '100010', представляющая строку  $13 + 2 = 15 = 12 + 3$ .

Примечание. Строки могут быть столь длинны, что числа  $A$  и  $B$  превысят максимально допустимое на вашем компьютере целое число.

**Задача 736. Возведение в степень.** Выведите на экран число  $2^n$ , где  $n \leq 10000$ ,  $n$  — натуральное.

**Задача 737. Вычисление функции.** Функция  $f$  с натуральными аргументами и значениями определена так:

$$f(0) = 0, f(1) = 1, f(2n) = f(n), f(2n + 1) = f(n) + f(n + 1).$$

Составьте программу вычисления  $f(n)$  по заданному  $n$ , требующую порядка  $\log_2 n$  операций.

**Задача 738. Частота встречаемости букв.** Пусть во входном файле `input.txt` содержится некоторый текст (например, отрывок из романа Л. Н. Толстого «Война и мир»). Определите частоту встречаемости символов в этом тексте.

**Задача 739. (\*) Код Хаффмана.** Закодируйте заданное в файле сообщение с помощью кода Хаффмана. Для этого:

- 1) определите кратности появления всех использующихся букв;
- 2) постройте дерево Хаффмана и определите коды букв;

3) закодируйте сообщение и выведите его в новый файл типа Boolean.

Форматы файлов:

input.txt (входной файл)

сообщение

key.txt (ключ для чтения выходного файла)

буква1-код1 буква2-код2 ... буквам-код $m$

code.dat (выходной файл типа Boolean)

код сообщения

Например, если

input.txt (входной файл)

кол около колокола.

то имеем: длина сообщения  $n = 19$ , число используемых символов  $m = 6$ , кратности символов  $p('о') = 7$ ,  $p('к') = 4$ ,  $p('л') = 4$ ,  $p(' ') = 2$ ,  $p('а') = 1$ ,  $p('.) = 1$ . И результатом должны быть файлы:

key.txt (ключ для чтения выходного файла)

о-00 к-01 л-10 пробел-110 а-1110 .-1111

code.dat (закодированный файл)

01001011000010010001100100100001001011101111

Напишите программу-декодер, которая по закодированному файлу code.dat и ключу key.txt восстанавливает сообщение и выводит его в файл output.txt.

**Задача 740. Простая кодировка.** Научитесь работать с кодировками, а именно сопоставлять последовательностям из нулей и единиц (битов) символы из конечного алфавита (элементов текста: букв, цифр, знаков, символов). Будем рассматривать 8-битную кодировку cp1251, которая сопоставляет символам байт (8 бит). Для нас она удобна, так как часто используется и содержит в себе коды практически всех символов, использующихся в русской типографике для обычного текста. Результат сопоставления также можно называть двоичным представлением. Байт будем записывать в виде двух шестнадцатеричных цифр. Например букве 'п' в кодировке cp1251 соответствуют следующие 8 битов 11101111, которые можно записать как ef. Заполните таблицу:

|    |                              |  |
|----|------------------------------|--|
| 1  | Hello World!                 | 48656c6c6f20576f726c6421                                   |
| 2  | Привет Мир!                  | cff0e8e2e5f220cce8f021                                     |
| 3  | ?                            | f3f7e5e1edeee520efeeef1eee1e8e5                            |
| 4  | алгоритмы шифрования         | ?  |
| 5  | Симметричная криптография    | ?  |
| 6  | ?                            | caf0e0f2ea8e920eaf3f0f1                                    |
| 7  | ?                            | cdf320e7e0fff62c20edf320efeee3ee<br>e4e821                 |
| 8  | Сборник задач по             | ?  |
| 9  | криптографии и криptoанализу | ?  |
| 10 | ?                            | 63703132353120f1e8edeeede8ec2077<br>696e646f77732d31323531 |

## 16.2 Криптографические задачи

**Задача 741. Координаты штаба.** Отряд «Каппа» провалил операцию по захвату шифрблокнота. Но зато удалось узнать некоторый открытый текст, соответствующий шифртекст и информацию о некомпетентности лиц, ответственных за информационную безопасность. Помогите «Каппе» не ударить в грязь лицом, восстановите ключ и расшифруйте сообщение.

|                   |  |
|-------------------|--|
| открытый текст I  | послезавтра старт малый адронный коллайдер   |
| шифртекст I       | 0315d11a0e1c18021918cc0006000ed00ac81810cb<br>390cd00d041c0ecd001ec9c20d050b071b0b04001c |
| открытый текст II | ?  |
| шифртекст II      | 0615ce010f13150019130cc31c120ccd160b1ad0d8<br>3005110dc0d9d40ed5d118dacbd3d3c2cad3d1d4d9 |

**Задача 742. (\*) Многоразовый блокнот.** В задаче 420 мы доказали, что одноразовый блокнот совершенно секретен. Но что будет, если использовать один и тот же ключ много раз? Ниже приведены 11 сообщений, зашифрованных с использованием одного и того же ключа. Дешифруйте последний шифртекст. Используется шестнадцатеричная система счисления.

|    |   |
|----|---|
| 1  | 12191607fe09c5ce1b06d11f0519c81ae6351b011317060e17fd207<br>14ca8e6d37862e7f8fad8b8fbfaf8e4212c000000cf8c87a20208ca  |
| 2  | 08cbcfcce2cd6130d110cd3cd0d1f1900e9e7021edb00190019f7e07<br>954a0f5d3ae78e134e3ca7837faf4ec3b2317c700ca879aad131dd0 |
| 3  | 1d0e12d7f804d806120dc9000b031a0e21f402071e130509d4e7f36<br>44cbefadb7872f2ecf71eb8e5f1f936352914d0cdc58c57b31300cb  |
| 4  | 09050f0535cc13001b00cdcd0d15c81fe1fd100210140ec013f3e36<br>942a6e5dea36529ecfac668f9f63936262f18c1c8ca499567d7ddd4  |
| 5  | cacbde1af509d200140dc5cd0d150a17f0e71c1712d104101cfffe57<br>986b9f7c1b0b0fdf1fbc36af2ffea363933110cd8c89d8767848852 |
| 6  | 1b051913f513d60517c852848f9c8c936479d1c49a9498c9d43e206<br>048a8ff13bc70e0f8f7dfb8ff34f7fe29301ac1d200998aae0c08cc  |
| 7  | 05050c19e20cc807df10c81915d289c721f704021f1919c01633f16<br>157baf7dfabb0e8f1f5dc77f7e5f8f83533170cd1d2899aa3001dd3  |
| 8  | 08cbcfcce2cd1130d110cd3cd181900d2e0fd040c17d103c014f7e8a<br>95ea8fedba8b0e6e4f7d673f9f2fdfd2ce11bc4d4d48c87a20d1bc9 |
| 9  | 9d9c89d97d80519c9e80418f97dc9a8721e80302db10000e1733e2a<br>94ca6e0dda87ee534fcc07de0f1e4e4262412c1dbc54986a8051bc9  |
| 10 | 0005151cf002dbce1506d2080e0e051aebfb130cdb1f190c11e4e06<br>24e68f7d0b6b0ebeff6d266eefcf0e73be114c4d7cd9292670a0dd6  |
| 11 | 1b0e1407f013de001ac8d1030b131117ecfd14d6db1c0ec01ce2ef6<br>74db4f5c0b162ec34fcfd670fa34fd36362f0d0cc6c5499dac1e1a01 |

**Задача 743. (\*) Математическая лингвистика I.** Пусть  $A$  — некоторый конечный алфавит мощности  $q$ ,

$$A = \{a_0, \dots, a_{q-1}\}.$$

Определим операции сложения и вычитания букв в алфавите:

$$\begin{aligned} a_i + a_j &= a_{(i+j) \bmod q}, \\ a_i - a_j &= a_{(i-j) \bmod q}. \end{aligned}$$

Пусть  $A^*$  — множество всевозможных конечных слов в алфавите  $A$ .

Пусть задан некоторый язык  $L \subseteq A^*$ . На языке  $L$  составлен текст  $M$  длины  $N$ . Считаем, что

$$M = (m_1, m_2, \dots, m_N), \text{ где } m_i \in A, i = 1, \dots, N.$$

Пусть  $\gamma$  — некоторая секретная последовательность (гамма) длины  $N$  в алфавите  $A$ ,

$$\gamma = (\gamma_1, \gamma_2, \dots, \gamma_N), \text{ где } \gamma_i \in A, i = 1, \dots, N.$$

При этом известно, что гамма сгенерирована с помощью ключа  $K$  (или лозунга — конечного слова в алфавите  $A$ ) путём его последовательной записи:

$$\gamma = (K, K, K, \dots, K, K'),$$

$$K = (k_1, k_2, \dots, k_n), \text{ где } k_i \in A, i = 1, \dots, n.$$

Через  $K'$  обозначена начальная часть ключа  $K$  такая, чтобы гамма имела длину  $N$  (в случае, если  $N$  не делится на  $n$ ). Отметим, что длина ключа  $n$  и сам ключ  $K$  считаются неизвестными.

**Шифрование.** Пусть текст  $M$  подвергается шифрованию путём по буквенного наложения гаммы:

$$C = M + \gamma = (m_1 + \gamma_1, m_2 + \gamma_2, \dots, m_N + \gamma_N).$$

**Задача.** Пусть  $M$ ,  $n$  и  $K$  неизвестны. Всё остальное (в том числе структура языка) полагается известным криptoаналитику. Предложите подход к определению (или оценке) длины ключа  $n$ , основывая свои рассуждения на анализе полученного шифртекста  $C$  и знании принципа шифрования. При каких условиях можно не только определить длину ключа  $n$ , но и восстановить сам ключ  $K$ , а значит, дешифровать текст  $M$ ? Можно ли определить принадлежность ключа  $K$  языку  $L$ ? Попробуйте рассмотреть в качестве языка  $L$  естественный язык, например, русский, английский и др.

Приведём таблицу частот (в порядке убывания) букв русского языка. Считаем, что буквы Е и Ё, а также Ъ и Ї отождествляются. Кроме того, рассматривается дополнительный символ «пробел». Эта таблица, как и таблицы распределения биграмм, взяты из книги [3].

| -     | О     | Е,Ё   | А     | И     | Т     | Н     | С     |
|-------|-------|-------|-------|-------|-------|-------|-------|
| 0,175 | 0,090 | 0,072 | 0,062 | 0,062 | 0,053 | 0,053 | 0,045 |
| P     | В     | Л     | К     | М     | Д     | П     | У     |
| 0,040 | 0,038 | 0,035 | 0,028 | 0,026 | 0,025 | 0,023 | 0,021 |
| Я     | Ы     | З     | Ь,Ї   | Б     | Г     | Ч     | Ї     |
| 0,018 | 0,016 | 0,016 | 0,014 | 0,014 | 0,013 | 0,012 | 0,010 |
| X     | Ж     | Ю     | Ш     | Ц     | Щ     | Э     | Ф     |
| 0,009 | 0,007 | 0,006 | 0,006 | 0,004 | 0,003 | 0,003 | 0,002 |

**Задача 744. (\*) Математическая лингвистика II.** В условиях задачи 743 определите, знания шифртекста какой длины достаточно для того, чтобы восстановить исходный открытый текст при условии, что длина ключа  $n$  равна 1, 2, 3, … Рассмотрите различные случаи:

- 1)  $A$  — алфавит русского языка (с пробелом),  $M$  — отрывок художественного литературного произведения;
- 2)  $A$  — алфавит русского языка (с пробелом),  $M$  — отрывок научной статьи, например, по математике.

Обратите внимание, что характер текста влияет на распределение частот букв языка (а также биграмм, триграмм и т. д.).

Ниже приводятся таблицы частот биграмм русского языка.

| Часть 1  |    |    |    |    |    |    |   |    |    |    |    |    |    |    |    |    |  |  |
|----------|----|----|----|----|----|----|---|----|----|----|----|----|----|----|----|----|--|--|
|          | А  | Б  | В  | Г  | Д  | Е  | Ж | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  |  |  |
| <b>А</b> | 2  | 12 | 35 | 8  | 14 | 7  | 6 | 15 | 7  | 7  | 19 | 27 | 19 | 45 | 5  | 11 |  |  |
| <b>Б</b> | 5  |    |    |    |    | 9  | 1 |    | 6  |    |    | 6  |    | 2  | 21 |    |  |  |
| <b>В</b> | 35 | 1  | 5  | 3  | 3  | 32 |   | 2  | 17 |    | 7  | 10 | 3  | 9  | 58 | 6  |  |  |
| <b>Г</b> | 7  |    |    |    | 3  | 3  |   |    | 5  |    | 1  | 5  |    | 1  | 50 |    |  |  |
| <b>Д</b> | 25 |    | 3  | 1  | 1  | 29 | 1 | 1  | 13 |    | 1  | 5  | 1  | 13 | 22 | 3  |  |  |
| <b>Е</b> | 2  | 9  | 18 | 11 | 27 | 7  | 5 | 10 | 6  | 15 | 13 | 35 | 24 | 63 | 7  | 16 |  |  |
| <b>Ж</b> | 5  | 1  |    |    | 6  | 12 |   |    | 5  |    |    |    |    | 6  |    |    |  |  |
| <b>З</b> | 35 | 1  | 7  | 1  | 5  | 3  |   |    | 4  |    | 2  | 1  | 2  | 9  | 9  | 1  |  |  |
| <b>И</b> | 4  | 6  | 22 | 5  | 10 | 21 | 2 | 23 | 19 | 11 | 19 | 21 | 20 | 32 | 8  | 13 |  |  |
| <b>Й</b> | 1  | 1  | 4  | 1  | 3  |    | 1 | 2  | 4  |    | 5  | 1  | 2  | 7  | 9  | 7  |  |  |
| <b>К</b> | 24 | 1  | 4  | 1  |    | 4  | 1 | 1  | 26 |    | 1  | 4  | 1  | 2  | 66 | 2  |  |  |
| <b>Л</b> | 25 | 1  | 1  | 1  | 1  | 33 | 2 | 1  | 36 |    | 1  | 2  | 1  | 8  | 30 | 2  |  |  |
| <b>М</b> | 18 | 2  | 4  | 1  | 1  | 21 | 1 | 2  | 23 |    | 3  | 1  | 3  | 7  | 19 | 5  |  |  |
| <b>Н</b> | 54 | 1  | 2  | 3  | 3  | 34 |   |    | 58 |    | 3  |    | 1  | 24 | 67 | 2  |  |  |
| <b>О</b> | 1  | 28 | 84 | 32 | 47 | 15 | 7 | 18 | 12 | 29 | 19 | 41 | 38 | 30 | 9  | 18 |  |  |
| <b>П</b> | 7  |    |    |    |    | 15 |   |    | 4  |    |    | 9  |    | 1  | 46 |    |  |  |

| Часть 2  |    |    |    |    |   |    |   |    |    |   |    |    |   |   |    |  |
|----------|----|----|----|----|---|----|---|----|----|---|----|----|---|---|----|--|
|          | Р  | С  | Т  | У  | Ф | Х  | Ц | Ч  | Ш  | Щ | Ы  | Ь  | Э | Ю | Я  |  |
| <b>А</b> | 26 | 31 | 27 | 3  | 1 | 10 | 6 | 7  | 10 | 1 |    |    | 2 | 6 | 9  |  |
| <b>Б</b> | 8  | 1  |    | 6  |   |    |   |    |    | 1 | 11 |    |   |   | 3  |  |
| <b>В</b> | 6  | 19 | 6  | 7  |   | 1  | 1 | 2  | 4  | 1 | 18 | 1  | 2 |   | 3  |  |
| <b>Г</b> | 7  |    |    | 2  |   |    |   |    |    |   |    |    |   |   |    |  |
| <b>Д</b> | 6  | 8  | 1  | 10 |   |    | 1 | 1  | 1  |   | 5  | 1  |   |   | 1  |  |
| <b>Е</b> | 39 | 37 | 33 | 3  | 1 | 8  | 3 | 7  | 3  | 3 |    |    | 1 | 1 | 2  |  |
| <b>Ж</b> |    | 1  |    |    |   |    |   |    |    |   |    |    |   |   |    |  |
| <b>З</b> | 3  | 1  |    | 2  |   |    |   |    |    | 4 |    |    |   | 4 |    |  |
| <b>И</b> | 11 | 29 | 29 | 3  | 1 | 17 | 3 | 11 | 1  | 1 |    |    | 1 | 3 | 17 |  |
| <b>Й</b> | 3  | 10 | 2  |    |   |    | 1 | 3  | 2  |   |    |    |   |   |    |  |
| <b>К</b> | 10 | 3  | 7  | 10 |   |    | 1 |    |    |   |    |    |   |   |    |  |
| <b>Л</b> | 3  | 1  | 6  |    | 4 |    | 1 |    |    |   | 3  | 20 |   | 4 | 9  |  |
| <b>М</b> | 2  | 5  | 3  | 9  | 1 |    |   | 2  |    |   | 5  | 1  | 1 |   | 3  |  |
| <b>Н</b> | 1  | 9  | 9  | 7  | 1 |    | 5 | 2  |    |   | 36 | 3  |   |   | 5  |  |
| <b>О</b> | 43 | 50 | 39 | 3  | 2 | 5  | 2 | 12 | 4  | 3 |    |    | 2 | 3 | 2  |  |
| <b>П</b> | 41 | 1  |    | 6  |   |    |   |    |    |   | 2  |    |   |   | 2  |  |

|   | Часть 3 |   |    |   |    |    |   |   |    |   |    |    |   |    |    |    |
|---|---------|---|----|---|----|----|---|---|----|---|----|----|---|----|----|----|
|   | А       | Б | В  | Г | Д  | Е  | Ж | З | И  | Й | К  | Л  | М | Н  | О  | П  |
| Р | 55      | 1 | 4  | 4 | 3  | 37 | 3 | 1 | 24 |   | 3  | 1  | 3 | 7  | 56 | 2  |
| С | 8       | 1 | 7  | 1 | 2  | 25 |   |   | 6  |   | 40 | 13 | 3 | 9  | 27 | 11 |
| Т | 35      | 1 | 27 | 1 | 3  | 31 |   | 1 | 28 |   | 5  | 1  | 1 | 11 | 56 | 4  |
| У | 1       | 4 | 4  | 4 | 11 | 2  | 6 | 3 | 2  |   | 8  | 5  | 5 | 5  | 1  | 5  |
| Ф | 2       |   |    |   |    | 2  |   |   | 2  |   |    |    |   |    | 1  |    |
| Х | 4       | 1 | 4  | 1 | 3  | 1  |   | 2 | 3  |   | 4  | 3  | 3 | 4  | 18 | 5  |
| Ц | 3       |   |    |   |    | 7  |   |   | 10 |   | 2  |    |   |    | 1  |    |
| Ч | 12      |   |    |   |    | 23 |   |   | 13 |   | 2  |    |   | 6  |    |    |
| Ш | 5       |   |    |   |    | 11 |   |   | 14 |   | 1  | 2  |   | 2  | 2  |    |
| Щ | 3       |   |    |   |    | 8  |   |   | 6  |   |    |    |   | 1  |    |    |
| Ы |         | 1 | 9  | 1 | 3  | 12 |   | 2 | 4  | 7 | 3  | 6  | 6 | 3  | 2  | 10 |
| Ь |         | 2 | 4  | 1 | 1  | 2  |   | 2 | 2  |   | 6  |    | 3 | 13 | 2  | 4  |
| Э |         |   |    |   |    |    |   |   |    | 1 |    |    | 1 |    |    |    |
| Ю |         | 2 | 1  | 2 | 1  |    |   | 3 | 1  |   | 1  |    | 1 | 1  | 1  | 3  |
| Я | 1       | 3 | 9  | 1 | 3  | 3  | 1 | 5 | 3  | 2 | 3  | 3  | 4 | 6  | 3  | 6  |

|   | Часть 4 |    |    |    |   |    |   |   |   |   |    |    |   |   |    |
|---|---------|----|----|----|---|----|---|---|---|---|----|----|---|---|----|
|   | Р       | С  | Т  | У  | Ф | Х  | Ц | Ч | Ш | Щ | Ы  | Ь  | Э | Ю | Я  |
| Р | 1       | 5  | 9  | 16 |   | 1  | 1 | 1 | 2 |   | 8  | 3  |   |   | 5  |
| С | 4       | 11 | 82 | 6  |   | 1  | 1 | 2 | 2 |   | 1  | 8  |   |   | 17 |
| Т | 26      | 18 | 2  | 10 |   |    |   | 1 |   |   | 11 | 21 |   |   | 4  |
| У | 7       | 14 | 7  |    |   | 1  |   | 8 | 3 | 2 |    |    |   | 9 | 1  |
| Ф | 1       | 1  |    |    |   |    |   |   |   |   |    |    |   |   |    |
| Х | 3       | 4  | 2  | 2  | 1 |    |   | 1 |   |   |    |    |   |   |    |
| Ц |         |    |    | 1  |   |    |   |   |   |   | 1  |    |   |   |    |
| Ч |         |    | 7  | 1  |   |    |   |   | 1 |   |    | 1  |   |   |    |
| Ш |         |    |    | 1  |   |    |   |   |   |   |    | 1  |   |   |    |
| Щ |         |    |    | 1  |   |    |   |   |   |   |    |    |   |   |    |
| Ы | 3       | 9  | 4  | 1  |   | 16 |   | 1 | 2 |   |    |    |   |   |    |
| Ь | 1       | 11 | 3  |    |   |    |   | 1 | 4 |   |    | 1  | 3 | 1 |    |
| Э |         | 1  | 9  |    |   |    |   |   |   |   |    |    |   |   |    |
| Ю | 1       | 1  | 7  |    |   |    |   | 1 | 1 |   | 4  |    |   |   |    |
| Я | 3       | 6  | 10 |    |   | 2  | 1 | 4 | 1 | 1 |    |    | 1 | 1 | 1  |

**Задача 745. (\*) Конвертация векторных булевых функций.**

Напишите программу, которая по заданному представлению векторной булевой функции будет выдавать другие её представления. Список представлений: в виде алгебраической нормальной формы, в виде набора значений (S-блока), алгебраическое представление. Подробнее о представлениях см. главу 13.

**Задача 746. (\*) Шифр A5/1 системы GSM.** Реализуйте поточный шифр A5/1, входящий в систему безопасности сотовой связи GSM. Описание алгоритма можно найти, например, в пособии [33].**Задача 747. (\*\*)** Шифр Grain. Реализуйте поточный шифр Grain из числа финалистов проекта eSTREAM. При ключе  $K=aaff\ aaff$

`aaff aaff aaff` и векторе инициализации  $IV=0d20\ fbc5\ 0278\ a67c$  зашифруйте сообщение `ffff 0000 1234 5678`. Вся информация здесь представлена в шестнадцатеричной системе счисления.

Описание шифра можно найти в следующей статье:

[http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain\\_p3.pdf](http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf),  
а также на странице <http://www.ecrypt.eu.org/stream/>. Опишите возможности криptoанализа шифра Grain.

**Задача 748. (\*\*)** **Шифр Trivium.** Реализуйте поточный шифр Trivium из числа финалистов проекта eSTREAM. При ключе  $K=aaff\ aaff\ aaff\ aaff$  и векторе инициализации  $IV=4fa0\ 0d20\ fbc5\ 0278\ a67c$  зашифруйте текст `ffff 0000 1234 5678`. Вся информация здесь представлена в шестнадцатеричной системе счисления.

Описание шифра можно найти в следующей статье:

[http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium\\_p3.pdf](http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf),  
а также на странице <http://www.ecrypt.eu.org/stream/>. Приведите характеристики известных методов криptoанализа шифра Trivium.

**Задача 749. (\*\*)** **Хэш-функция SHA-3.** Разберите и реализуйте одну из хэш-функций — финалистов конкурса SHA-3. Описания функций можно найти здесь:

|        |   |
|--------|---|
| BLAKE  | <a href="http://131002.net/blake/blake.pdf">— http://131002.net/blake/blake.pdf</a>   |
| Grøstl | <a href="http://www.groestl.info/Groestl.pdf">— http://www.groestl.info/Groestl.pdf</a>   |
| JH     | <a href="http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf">— http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf</a>   |
| Keccak | <a href="http://keccak.noekeon.org/Keccak-main-2.1.pdf">— http://keccak.noekeon.org/Keccak-main-2.1.pdf</a>                             |
| Skein  | <a href="http://www.skein-hash.info/sites/default/files/skein1.2.pdf">— http://www.skein-hash.info/sites/default/files/skein1.2.pdf</a> |

Напомним, что в октябре 2013 г. победителем конкурса была выбрана функция Keccak.

Какие методы криptoанализа применялись к выбранному вами кандидату? Приведите их характеристики. А может быть, у вас есть свои идеи? Поделитесь!

**Задача 750. (\*\*)** **Шифрмашина «Фиалка».** Подготовьте программную реализацию шифрования с помощью советской шифрмашины «Фиалка» М-125.

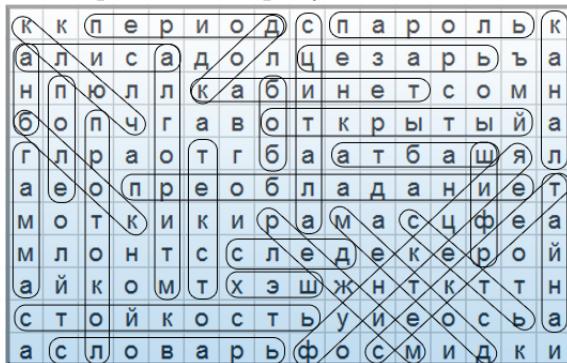


## Шифрмашина «Фиалка» М-125.

## ОТВЕТЫ К ЗАДАЧАМ

# Криптография: основные понятия и история

1. Ответ приведён на рисунке:



**2. a) THIS MESSAGE SERVES TO PROVE HOW OUR MINDS CAN DO AMAZING THINGS! IMPRESSIVE THINGS! IN THE BEGINNING IT WAS HARD BUT NOW, ON THIS LINE YOUR MIND IS READING IT AUTOMATICALLY WITH PRACTICALLY NO THINKING INVOLVED RIGHT? BE VERY PROUD! YOU DESERVE A PAT ON THE BACK! REPOST IF YOU CAN READ IT :)**

б) У лукоморья дуб зелёный; / Златая цепь на дубе том: / И днём и ночью кот учёный / Всё ходит по цепи кругом.

**3.** Ветер забирался в пустые комнаты и в печные воюющие трубы, и старый дом, весь расшатанный, дырявый, полуразвалившийся, вдруг оживлялся странными звуками, к которым я прислушивался с невольной тревогой. Вот точно вздохнуло что-то в белой зале, вздохнуло глубоко, прерывисто, печально. Вот заходили и заскрипели где-то далеко высохшие гнилые половицы под чьими-то тяжелыми и бесшумными шагами. (А. И. Куприн «Олеся»)

4. Безобразный почерк — вот абсолютно нераскрываемый шифр!

5. В сердце каждой трудности кроется возможность. А. Эйнштейн

6. По несчастью или к счастью, / Истина проста: / Никогда не возвращайся / В прежние места. / Даже если пепелище / Выглядит вполне, / Не найти того, что ищем, / Ни тебе, ни мне.

7. 1) в; 2) д; 3) а.

8. 1) б; 2) г; 3) б.

**9.** 1) в; 2) а; 3) б. Правильный порядок: 3, 2, 1.

**10.** 1) б; 2) в; 3) г; 4) а.

**11.** 1) Котельников; 2) Ривест; 3) имитовставка; 4) Петр; 5) Тьюринг; 6) Остерман; 7) Грибоедов; 8) Ришелье; 9) Адлеман; 10) Фридман; 11) Ирландия; 12) Ярдли.

**12.** Мариан Раевский, Генрих Зыгальский, Ежи Розицкий.

**13.** 1) правило; 2) ключ; 3) алгоритм; 4) протокол; 5) линеаризация; 6) Ева; 7) аналитические; 8) атакую; 9) число; 10) дифференциальный; 11) маскирование; 12) шифр; 13) функциональная; 14) раунд; 15) Поллард; 16) Винер; 17) блок; 18) слайдовый; 19) бит; 20) посередине; 21) Ультра; 22) факторизация; 23) разностный; 24) Бомба; 25) словарь; 26) парадокс; 27) алгебраический; 28) энергопотребление; 29) пассивный; 30) лицензия; 31) линейный; 32) ноль; 33) корреляционный; 34) абонент; 35) злоумышленник; \*\*) Где твои семнадцать лет?

**14.** 1) RSA; 2) Shamir; 3) Micali; 4) Goldwasser; 5) AES; 6) DES; 7) RC4.

**15.** 1) М-125 Фиалка (СССР); 2) Japanese-Enigma cipher machine (Япония); 3) Purple (Япония); 4) М-105 Агат (СССР); 5) Энигма (Германия); 6) М-209 (США); 7) Hagelin/Crypto AG CD-57 (Nato C-1-0) — карманная механическая шифромашинка (Швейцария).

**16.** 1) б, в, г; 2) а, в, е; 3) в.

**17.** 1) з; 2) е; 3) и; 4) г; 5) а; 6) ж; 7) к; 8) л; 9) д; 10) б; 11) в.

**18.** 1) а; 2) в; 3) а, г, д; 4) б, г, д, е; 5) е.

**19.** а, б, г, и, м, н, о.

**20.** 1) Фрагмент раундовой функции AES; 2) Шифр, использовавшийся масонами; 3) Кодовая книга шифра «Одноразовый блокнот»; 4) Раундовая функция шифра ГОСТ 28147-89; 5) Поточный шифр Trivium; 6) Сцитала; 7) Шифр Цезаря; 8) RSA; 9) Раундовая функция шифра SAFER+.

**21.** а) Вилли Леман; б) Павел Макаров.

**22.** 1) А. Н. Рыбаков, роман «Дети Арбата». Арестованный — студент Саша Панкратов. Описанный шифр — квадрат Полибия, или тюремный шифр. 2) Ю. С. Семёнов, роман «Семнадцать мгновений весны». Книжный шифр. 3) А. И. Солженицын, роман «В круге первом». Работа Марфинской шарашки. 4) Э. А. По, рассказ «Золотой жук». Зашифрован текст: «A good glass in the bishop's hostel in the devil's

seat twenty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's head a bee line from the tree through the shot fifty feet out.», перевод: «Хорошее стекло в трактире епископа на чёртовом стуле двадцать один градус и тринадцать минут северо-северо-восток главный сук седьмая ветвь восточная сторона стреляй из левого глаза мёртвой головы прямая от дерева через выстрел на пятьдесят футов.» В тексте указан путь к сокровищам капитана Кидда. 5) Ю. В. Трифонов, роман «Нетерпение». Ваничка — Иван Окладников, провокатор «Народной воли». Время подготовки несостоявшегося покушения на Александра II на железной дороге под г. Александровском. 6) Я. Гашек, роман «Похождения бравого солдата Швейка». Капитан Сагнер объясняет офицерам «совершенно новый» «дополнительный цифровой метод», который, как выясняется, был взят из известной в то время книги Керкгоффса по военной криптографии. Кроме того, вместо нужного для шифрования второго тома книги «Грехи отцов» офицерами был получен первый том.

## Олимпиадные задачи по криптографии

### Математические задачи

**23.** 19.

**24.** а) 14 секунд; в) 23 секунды.

**26.** 64416.

**27.** На всех шарах написано число 0.

**28.**  $n = 3k$ , где  $k$  — произвольное натуральное число.

**29.** Потребуется вывести из строя 5 линий.

**30.**  $3^{20} + 3^4 + 1 = 7^2 \cdot 13 \cdot 73 \cdot 167 \cdot 449$

**32.** а)  $p = 200007$ ,  $q = 200009$ ; б)  $p = 1999961$ ,  $q = 200041$ .

**33.** Да.

**34.** При  $a < -1$  два решения  $x = -1 \pm \sqrt{4-a}$ ;

при  $a = -1$  три решения  $x = 0$  и  $x = -1 \pm \sqrt{5}$ ;

при  $a = 0$  три решения  $x = -1$ ,  $x = -3$ ,  $x = 1$ ;

при  $a = 3$  три решения  $x = -2$ ,  $x = 0$ ,  $x = 2$ ;

при  $a = 4$  три решения  $x = -1$ ,  $x = \pm\sqrt{5}$ ;

при  $-1 < a < 0$ , при  $0 < a < 3$  и при  $3 < a < 4$  четыре решения  $x = -1 \pm \sqrt{4-a}$  и  $x = \pm\sqrt{1+a}$ ;

при  $a > 4$  два решения  $x = \pm\sqrt{1+a}$ .

**35.**  $a \in (-\infty; 1) \cup (-1; -\frac{1}{9}) \cup (1; \frac{5}{4})$ .

**36.** 812.

**38.** 13 и 5.

**39.** При  $a \leq -1$  нет решений;

при  $-1 < a \leq 1$  система имеет 1 решение;

при  $1 < a < 2$  система имеет 2 решения;

при  $a = 2$  система имеет 3 решения;

при  $a > 2$  система имеет 4 решения.

**41.** 16 пар (пары  $(a, b)$  и  $(b, a)$  разные). В общем случае число упорядоченных пар равно  $2^k$ , где  $k$  — число всех простых делителей  $m/d$ .

**42.** 100091 и 200089.

**44.**  $AP : PQ : QC = (\sqrt{4\sqrt{3} - 3} - 1) : 2 : (3 - \sqrt{4\sqrt{3}})$ .

**45.**  $x = \frac{1+\sqrt{4a^2+1}}{2a}$  при  $0 < a < 1$ ;

$x_1 = \frac{1+\sqrt{4a^2+1}}{2a}, x_2 = \frac{-1-\sqrt{4a^2+1}}{2a}$  при  $a \geq 1$ .

**46.** Комбинации  $(13, 18, 12)$ ,  $(13, 17, 17)$ ,  $(12, 16, 11)$ .

**48.** 481.

**49.** 1995003.

**51.** 1996.

**53.** Квадрат со стороной 1 м; площадь границы —  $404 \text{ см}^2$ .

### Интересные задачи разных типов

**54.** а) 515355128523864354, б) СИСТЕМА.

**55.** ШИФРЗАМЕНЫ.

**56.** ТЕЛЕГРАФ.

**57.** 01011

**58.** АМПЛИТУДА.

**59.** ТИШЕ ЕДЕШЬ ДАЛЬШЕ БУДЕШЬ.

**60.** Первая и вторая.

**61.** МОРОЗНОРАВНИНЫБЕЛЕЮТПОДСНЕГОМЧЕРНЕЕТСЯЛЕСВПЕРЕДИ.

**62.** Указание. Рассмотрите атаку «человек посередине».

**64.** Условие: чтобы в каком-нибудь из двух текстов было как минимум семь цифр, отличных от нуля.

**65.** 420 км.

**66.**  $\{1, 2, 4, 5, 8, 11\}$ .

**67.** Например:

| №  | Город   | №  | Город   | №   | Город   | №   | Город   |
|----|---------|----|---------|-----|---------|-----|---------|
| 1. | 0 0 0 1 | 5. | 0 1 1 1 | 9.  | 1 1 0 1 | 13. | 1 0 1 1 |
| 2. | 0 0 1 1 | 6. | 0 1 0 1 | 10. | 1 1 1 1 | 14. | 1 0 0 1 |
| 3. | 0 0 1 0 | 7. | 0 1 0 0 | 11. | 1 1 1 0 | 15. | 1 0 0 0 |
| 4. | 0 1 1 0 | 8. | 1 1 0 0 | 12. | 1 0 1 0 | 16. | 0 0 0 0 |

№ — это номер поездки.

**68.** Число различных ключей шифра «поворотная решётка» при чётных значениях  $n$  равно  $4^{n^2/4}$ .

**69.** Начиная с 54.

**70.** Например,  $cbsacabc$ .

**71. Указание.** Рассмотрите один виток ленты.

**72.**  $a$  любое,  $b$  не должно делиться на 2 и на 5.

**73. Указание.** Рассмотрите остатки от деления на 26 сумм числовых значений первых  $k$  букв.

**74.** Нельзя.

**75.**  $\cos 36^\circ = (1 + \sqrt{5})/4 \approx 0,8$ .

**76. КАВАЛЕРГАРДОВ ВЕК НЕДОЛОГ**

И ПОТОМУ ТАК СЛАДОК ОН  
ТРУБА ТРУБИТ ОТКИНУТ ПОЛОГ

**77.**  $N$  чётное.

**78.** 15.

## Шифры перестановки

|    |    |    |    |
|----|----|----|----|
| 16 | 3  | 2  | 13 |
| 5  | 10 | 11 | 8  |
| 9  | 6  | 7  | 12 |
| 4  | 15 | 14 | 1  |

, ПЕРЕСТАВЬТЕ БУКВЫ.

**80.**  $a = 7, b = 2$ . Мороз воеводы зором обходит вladenъ ясвои.

**81.** Смещение трафарета в шифре поворотная решётка позволяет прочитать текст!

**82.** ЧТО БЫ ПОЛУЧИТЬ ПЯТЬ НУЖНО ОТЛИЧНО ЗНАТЬ ПОЛУЧИЛОСЬ НЕ ПЛОХО.

**83. Д О Л Г О Е В Р Е М Я З А Н Я Т И Е К Р**

И П Т О Г Р А Ф И Е Й Б Y Л O У Д E Л O

М О Д И Н О Ч Е К Т Ч К С Р Е Д И Н И Х

Б Y Л I O Д A R E Н Н Y E У Ч E N Y E Z

П Т Д И П Л О М А Т Ы З П Т С В Я Щ Е Н

Н О С Л У Ж И Т Е Л И Т Ч К - - - - -

84. ПОЛЬЗУЯСЬШИФРОМРЕШЕТКАНЕЛЬЗЯОСТАВЛЯТЬПУСТЫЕМЕСТА.

### Шифры замены

85. Умом Россию не понять,  
Аршином общим не измерить:  
У ней особенная стать —  
В Россию можно только верить.

86. ШИФРЗАМЕНЫ.

|     |                                |   |   |    |   |    |    |    |
|-----|--------------------------------|---|---|----|---|----|----|----|
|     | шифрованное сообщение          | K | E | H  | 3 | Э  | P  | E  |
|     | числовое шифрованное сообщение | 9 | 5 | 12 | 7 | 27 | 15 | 5  |
| 87. | шифрующий отрезок              | 0 | 3 | 12 | 3 | 12 | 15 | 18 |
|     | числовое исходное сообщение    | 9 | 2 | 0  | 4 | 15 | 0  | 17 |
|     | исходное сообщение             | K | B | A  | Д | P  | A  | T  |

88. Рыбак рыбака видит издалека.

89. 5, 12, 19, 26, 33.

90. Первая строка: 74769734797897, вторая строка: 74373975977039, вторая и третья строки: 71749835949098.

91. Первый текст.

92. Бегают по лесу стаи зверей —  
Не за добычей, не на водопой:  
Денно и нощно они егерей  
Ищут веселой толпой.

93. 2730.

94. С О В Р Е М Е Н Н А Я -  
К Р И П Т О Г Р А Ф И Я  
Э Т О - Н А У К А - О -  
С Е К Р Е Т Н О С Т И -  
Ш И Ф Р О В А Л Ъ Н Ы Х  
С И С Т Е М - С В Я З И

95. НАУКА.

96. ШЕСТАЯОЛИМПИАДАПОКРИПТОГРАФИИПОСВЯЩЕНАСЕМИДЕСЯТИПЯТИЛЕТИЮ СПЕЦИАЛЬНОЙСЛУЖБЫРОССИИ.

97. В БЕЗМОЛВИИ САДОВ ВЕСНОЙ ВО МГЛЕ НОЧЕЙ ПОЕТ НАД РОЗОЮ ВОСТОЧНЫЙ СОЛОВЕЙ.

98. ПАРОХОД.

- 99.** Семнадцатая олимпиада по математике и криптографии посвящена столетию Ивана Яковлевича Верченко.
- 100.** ВЕЧОРЫПОМНИШЬВЪЮГАЗЛИСЬ  
НАМУТНОМНЕБЕМГЛАОСИЛАСЬ
- 101.** Дождусь тебя, моё творенье.
- 102.** БЫК ВЯЗ ГНОЙ ДИЧЬ ПЛЮЩ СЪЁМ ЦЕХ ШУРФ ЭТАЖ.

### «Восстановите секретное сообщение...»

- 103.** Ключевое слово — КРЫША, сообщение — ВЕРБЛЮДЫИДУТНАСЕВЕР-ВЕРБЛЮДЫИДУТНАСЕВЕР.
- 104.** Исходное сообщение — ПОЗДРАВЛЯЮ С НОВЫМ ГОДОМ. Используемая дата — 31.12.2007.
- 105.** DQTTR EBRTT KVLQR. **Указание.** Для решения задачи надо понять сам процесс зашифрования. Пронумеруйте столбцы и строки таблицы, которая является ключом.
- 106.** INTER ARMA SILENT MUSAE (интер а́рма си́лент мұзә — когда гремит оружие, музы молчат).
- 107.** Первой и третьей криптограмме соответствует исходное сообщение ПОВТОРЕНИЕМАТЬЧЕНИЯ. Второе исходное сообщение СМОТРИВКОРЕНЬ.
- 108.** ТАКДЕРЖАТЬ.
- 109.** 4470416411 либо 2371640978.
- 110.** КОГДАОТХОДЯТКОРАБЛИ и КОРАБЛИОТХОДЯТВЕЧЕРОМ.
- 111.** НАШКОРРЕСПОНДЕНТ.
- 112.** СВЯЗЬ-ПО-РАДИО.
- 113.** КВАДРАТ.
- 114.** Пароль: 5393511; его расшифровка: 5830829.
- 115.** ЧТОБЫПОЛУЧИТЬПЯТЬНУЖНООТЛИЧНОЗНАТЬПОЛУЧИЛОСЬНЕПЛОХО.

### Задачи последних олимпиад ИКСИ

#### 8–9 классы. 2010 год

- 116.** Я завтра уезжаю в Санкт-Петербург на две недели. Пароль: Бургундия.
- 117.** 1,1,1,1,0.

**10 класс 2010. год****118.** 21.**119.** Гномы сообщили неверное значение.**11 класс 2010. год****120.** 840.**121.**  $6 \cdot 4^n$ .**122.** Например:  $a_1 = 2$ ,  $a_2 = -2$ ,  $a_3 = 3$ ,  $a_4 = 1$ .**123.** ОКЕАН ОБНИМАЕТ КОРАБЛИ.**124.**  $x = 117337$ .**125.**  $4^{20} - 2^9$ .**8–9 классы. 2011 год****126.** У ПОДНОЖИЯ ГОРЫ.**127.** (0,1,1,0).**128.** Поставим в соответствие каждой провинции с номером  $i$  города с названиями  $(a_1, a_2, a_3, a_4)$ , удовлетворяющие условиям: сумма  $a_1 + a_2 + a_3 + a_4$  кратна  $i$ .**129.** В СУЕТЕ ГОРОДОВ.**130.** УДАР МАСТЕРА СТОИТ ТЫСЯЧИ ДРУГИХ УДАРОВ.**131.** 1.**10 класс. 2011 год****132.** ДЛИННАЯ ЦЕПОЧКА ИЗ СИМВОЛОВ.**133.** 4.**134.** См. задачу 128.**135.** КРАЙ ЛЬДОВ ГРЕНЛАНДИЯ.**136.** (1,1,1,0).**137.**  $\frac{16}{3}$ .**11 класс. 2011 год****138.** МАРСИАНЕ ЖДУТ СНЕГА.**139.** 252.**140.** (1; 1; 0; 1; 0; 1).

**141.** НАШЕ СУДНО ПОТЕРЯЛОСЬ В ОКЕАНЕ.

**142.** МАДАГАСКАР.

**143.**  $\frac{22+2\sqrt{91}}{5}$ .

### 9 класс. 2012 год

**144.** 7.

**145.** ПАРОЛЬ МЕДВЕЖАТА.

**146.**  $a_1 = r_{36}(17y_1)$ ,  $a_2 = r_{36}(17y_2 - 17y_1)$ .

**147.** 25.

**148.** фишинг.

### 10 класс. 2012 год

**149.**  $(0, 0)$ .

**150.** ЛЕДНИКОВЫЙ ПЕРИОД.

**151.** ПАРОЛЬ МЕДВЕЖАТА.

**152.** 2608; 72.

**153.**  $(x, y) = (102, 72)$ .

**154.** взлом сайта.

### 11 класс. 2012 год

**155.** Указание. Рассмотрите остатки от деления.

**156.**  $(x, y) = (77, 763)$ .

**157.** МЕДВЕЖОНOK В ПОДАРКЕ.

**158.** 78.

**159.** 2072; 72.

**160.** БЕРЛИН.

### 8–9 классы. 2013 год

**161.** 30, 32, 35, 36 или 30, 31, 34, 36.

**162.** 7

**163.** КОНФЕТЫ В НАШЕЙ КОМНАТЕ.

**164.** а)  $a = 2, b = 5, c = 6$ .

**165.** 7832.

**166.** УЛИТКА.

**10 класс. 2013 год****168.** 3.**169.** У МЕНЯ ЕСТЬ СЕНОКОСИЛКА.**170.** 2037, 7342, 2417, 7102.**171.** а)  $a = 3, b = 5, c = 6$ .**172.** ПОЛИНЕЗИЯ.**11 класс. 2013 год****173.** ПОЛЕТ СОСТОИТСЯ ЗАВТРА В СЕМЬ ЧАСОВ.**174.** 50, 52, 53, 57, 63 или 50, 56, 60, 61, 63.**175.** 4 при  $n = 65, m = 78, k = 18$ .**176.** ЯШМАЯШМА.**177.** а)  $a = 3, b = 6, c = 8, d = 10$ .**178.** ЗОНД ПРИЗЕМЛЕН.**Задачи олимпиады по информатике и компьютерной безопасности**

**179.** Покажем, что в каждый момент времени при распространении вируса зараженных компьютеров будет нечётное количество. Пусть в некоторый момент поражено нечётное количество компьютеров  $n$  и  $k$  из них распространяют вирус дальше. Независимо от того, чётное или нечётное количество компьютеров распространяет вирус в данный момент, количество вновь заражённых компьютеров  $x$  всегда будет чётно (по условию). Следовательно, в итоге получаем опять нечётное количество зараженных компьютеров  $n + x$ . Поскольку заражение сети начнётся с одного компьютера (нечётное число), то и максимальное число зараженных компьютеров будет нечётно и вся сеть фирмы не будет выведена из строя.

**180.** При основании 7. Исходный ребус выглядит так:

$$\begin{array}{r} 4350 \\ + \quad 43050 \\ \hline 50430 \end{array}$$

**181.** Пронумеруем комнаты по кругу от 1 до 44. Сумма номеров комнат, где располагаются документы, либо не меняется, либо уменьшается на 44, либо увеличивается на 44. Тем самым остаток от деле-

ния этой суммы номеров на 44 не меняется. Изначально этот остаток равен 22, поскольку сумма номеров комнат — это сумма элементов арифметической прогрессии, которая равна (общая формула  $S_n = n * a_1 + (n - 1)nd/2$ , где  $n$  — длина подпоследовательности,  $a_1$  — первый элемент последовательности,  $d$  — разность арифметической прогрессии)  $S_{44} = 44 \cdot 1 + (44 - 1)44 \cdot 1/2 = 990$ ,  $990 \bmod 44 = 22$ . Если все документы будут перемещены в одну комнату, то он будет равен 0, т.е. сумма номера комнаты  $N$  по числу документов составит  $N \cdot 44(N \cdot 44) \bmod 44 = 0$ . Поскольку от пути перемещения документов, как мы логически рассудили, остаток от деления меняться не должен, то это позволяет сделать заключение, что все документы не смогут быть перемещены в одну комнату.

**182.** Система не будет надежной. Например, если для указанного в задаче случая взять слово АААЛ, то для него сумма будет равна также 15 (АААЛ: А — 1, А — 1, А — 1, Л — 12). То есть можно подобрать такое сочетание букв, что рассчитанная в результате сумма будет совпадать с искомой. Кроме того пары, АБВГ и БББГ, также МНОП и АМБЬ образуют коллизии.

**183.** Длина текста составляет  $K = 36 \cdot 6 = 216$  символов. Число бит информации  $I = 81$  байт = 648 бит. Для кодирования одного символа использовалось  $i = 648/216 = 3$  бита. Число различных сочетаний из трех бит, которые могут кодировать знаки алфавита шифровки  $N = 2^3 = 8$  символов.

### Задачи Белорусского государственного университета

**184. Решение.** Идея взята из статьи академика В. Арнольда в журнале «Квант» (1998 г., № 1, см. <http://kvant.mccme.ru/1998/>).

Пусть  $A^B$  является  $m$ -разрядным десятичным числом с первой цифрой  $r$ :

$$A^B = r10^{m-1} + s, \quad r \in \{1, 2, \dots, 9\}, \quad s < 10^{m-1}.$$

Тогда

$$B \lg A = (m - 1) + \lg \left( r + \frac{s}{10^{m-1}} \right),$$

где  $\lg$  — логарифм по основанию 10. Из этого получаем

$$\{B \lg A\} = \left\{ \lg \left( r + \frac{s}{10^{m-1}} \right) \right\},$$

где через  $\{z\}$  обозначается дробная часть  $z$ . Следовательно,  $r = i$ , если

$$\lg i \leq \{B \lg A\} < \lg(i+1).$$

Число  $\lg A$  является иррациональным. Действительно, если  $\lg A = u/v$ , где  $u$  и  $v$  — целые, то  $A^v = 10^u$ . Это противоречит тому, что  $A$  не кратно 10. Согласно результатам Г. Вейля, которые цитируются в статье Б. Арнольда, при случайному выборе  $B$  величина  $\{B \lg A\}$  имеет распределение, близкое к равномерному на интервале  $(0, 1)$ . Поэтому вероятность  $\mathbf{P}\{r = i\}$  близка к величине

$$p_i = \lg(i+1) - \lg i.$$

В следующей таблице приводятся значения  $p_i$ :

| i | $p_i$ | i | $p_i$ | i | $p_i$ |
|---|-------|---|-------|---|-------|
| 1 | 0,301 | 4 | 0,097 | 7 | 0,058 |
| 2 | 0,176 | 5 | 0,079 | 8 | 0,051 |
| 3 | 0,125 | 6 | 0,067 | 9 | 0,046 |

Виктор обрадован тем, что распределение  $r$  сильно отличается от равномерного на  $\{1, 2, \dots, 9\}$ . Это упрощает подбор кода сейфа.

Конкретнее, энтропия (по основанию 9) цифры  $r$  составляет

$$H(r) = - \sum_{i=1}^9 p_i \log_9 p_i \approx 0,91.$$

Если код сейфа состоит из  $n$  цифр, то для подбора кода достаточно перебрать

$$9^n H(r) \approx (7,38)^n$$

высоковероятных вариантов (вместо  $9^n$  вариантов при равномерном распределении  $r$ ).

**185. Решение.** Будем использовать многочлены над полем из  $p$  элементов. При сложении, умножении и делении таких многочленов операции с их коэффициентами будем выполнять по модулю  $p$ .

Пусть  $f_n(x) = a_n + b_n x$  — остаток от деления многочлена  $x^{n+1}$  на многочлен  $x^2 - x - 1$ . Имеем:

$$f_0(x) = 0 + 1 \cdot x, \quad f_1(x) = 1 + 1 \cdot x, \quad f_2(x) = 1 + 2 \cdot x, \quad f_3(x) = 2 + 3 \cdot x, \dots$$

и вообще для  $n \geq 1$ :

$$f_n(x) = x f_{n-1}(x) \bmod (x^2 - x - 1) = b_{n-1} + ((a_{n-1} + b_{n-1}) \bmod p)x.$$

Отсюда следует, что  $a_n = u_n$ ,  $b_n = u_{n+1}$ . Поэтому для определения  $K$  достаточно найти свободный член многочлена  $x^{2^{64}} \pmod{x^2 - x - 1}$ . Для этого можно воспользоваться следующим алгоритмом:

1. Установить  $f(x) := x$ .
2. Для  $i = 1, 2, \dots, 64$  выполнить  $f(x) := f(x)^2 \bmod (x^2 - x - 1)$ .
3. Возвратить свободный член  $f(x)$ .

Выполнив алгоритм (например, в системе компьютерной алгебры *Mathematica*), находим

$$K = 137973196247803287452671646795669768529,$$

или `67ccabc7cffd05dbdeec654abb5d0951` в шестнадцатеричной системе счисления.

Интересно, что период последовательности Фибоначчи  $\{u_n\}$  составляет  $2(p+1)$ . Период можно найти как порядок неприводимого над полем из  $p$  элементов многочлена  $x^2 - x - 1$ . Подробнее см. книгу *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2 т. М.: Мир, 1988. 822 с.

**186. Решение.** Пусть  $\{s_t^*\}$  — линейная рекуррентная последовательность над полем из двух элементов, заданная соотношением

$$s_{t+128}^* = s_t^* \oplus s_{t+1}^* \oplus s_{t+2}^* \oplus s_{t+7}^*.$$

Характеристический многочлен этой последовательности имеет вид  $f(x) = x^{128} + x^7 + x^2 + x + 1$ . С помощью систем компьютерной алгебры можно убедиться, что этот многочлен является неприводимым. Для этого достаточно проверить, что многочлены  $x^{2^{64}} - x$  и  $f(x)$  взаимно просты и что  $f(x)$  делит  $x^{2^{128}} - x$ .

Для всех простых  $p$ , которые делят

$$2^{128} - 1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 274177 \cdot 6700417 \cdot 67280421310721,$$

выполняется

$$x^{(2^{128}-1)/p} \neq 1 \pmod{f(x)}$$

и, следовательно, порядок  $f(x)$  равняется  $2^{128} - 1$ , т. е.  $f(x)$  является примитивным. Примитивность  $f(x)$  означает, что при ненулевых начальных значениях минимальный период последовательности  $\{s_t^*\}$  равняется  $2^{128} - 1$ . При согласовании начальных условий последовательность  $\{s_t\}$  получается из  $2^{128} - 1$  вставкой нуля после фрагмента 100...0 длины 128. Это значит, что минимальный период последовательности  $\{s_t\}$  равняется  $2^{128}$ .

Отметим, что  $\{s_t\}$  — это известная в комбинаторике последовательность де Брёйна. Первые  $2^{128}$  её фрагментов  $s_1s_2\dots s_{128}, s_2s_3\dots s_{129}\dots$  различны.

**187. Решение.** В нашем распоряжении оказалось следующее письмо. Публикуем его по разрешению Трента.

«Уважаемый Виктор,  
предлагаю следующий протокол.

1. Я выбираю различные большие простые  $p$  и  $q$  так, что  $n$  и  $(p-1)(q-1)$  взаимно просты. Затем отправляю Вам модуль  $N = pq$ .
2. Вы выбираете случайное число  $d \in \{1, 2, \dots, N-1\}$  и отправляете мне замаскированное решение, состоящее из следующих чисел:  $X = dx \pmod{N}$ ,  $Y = dy \pmod{N}$ ,  $Z = dz \pmod{N}$ . Если одно из полученных чисел  $X, Y, Z$  совпадает с нулём, то Вы генерируете другое  $d$  или предлагаете мне выслать другой модуль  $N$ .

3. Я проверяю, что  $X, Y, Z \neq 0$  и что  $X^n + Y^n = Z^n \pmod{N}$ .

Данный протокол обладает следующими свойствами.

*Полнота.* По известному решению  $(x, y, z)$  Вы без труда сможете найти подходящую тройку  $(X, Y, Z)$ .

*Корректность.* Нахождение подходящей тройки  $(X, Y, Z)$  без знания  $(x, y, z)$  представляется непростой задачей. Можно выбрать два элемента тройки, например  $X$  и  $Y$ , и определить  $Z$  как корень  $n$ -й степени из  $X^n + Y^n$  по модулю  $N$ . Но извлечение корней по составному модулю при неизвестной факторизации модуля является трудной вычислительной задачей. На этой задаче базируется знаменитая криптосистема RSA. Возможно, существуют более простые способы

нахождения  $(X, Y, Z)$ , но они мне неизвестны. Важно, что координаты решения должны быть ненулевыми. Если снять это требование, то можно построить тривиальные решения, например  $\{X = Z, Y = 0\}$ .

Модуль  $N$  может оказаться не взаимно прост с  $x, y, z$  или  $d$ . В этом случае Вы получаете факторизацию  $N$  и предыдущие аргументы о корректности протокола не действуют. Но возможностью факторизации  $N$  можно пренебречь, потребовав, чтобы  $p$  и  $q$  были достаточно велики.

*Неразглашение.* Важно не разгласить любое решение уравнения Ферма, в том числе решение  $(dx, dy, dz)$ . Вы предъявляете остатки от деления компонент этого решения на  $N$ . Я не вижу эффективного способа определения исходного решения по остаткам.

Приведенные аргументы не выглядят до конца исчерпывающими. Если у Вас есть возражения — давайте их обсудим. В противном случае предлагаю действовать по описанному протоколу.

С наилучшими пожеланиями, Трент.»

Насколько нам известно, Виктор с Трентом больше не связывался.

**188. Решение.** Задача возникла по мотивам одного из заданий ресурса Ponder this (см. <http://www.research.ibm.com/ponder/>).

Число  $a = 1 + 2 \cos(\pi/9) \approx 2,8793$  является корнем многочлена  $x^3 - 3x^2 + 1$ . Два других корня — это  $a_2 \approx -0,5321$  и  $a_3 \approx 0,6527$ . Пусть  $S_k = a^k + a_2^k + a_3^k$ . Используя формулы Ньютона, получаем:  $S_1 = 3$ ,  $S_2 = 9$ ,  $S_3 = 24$  и вообще  $S_k = 3S_{k-1} - S_{k-3}$  для  $k \geq 4$ . Это значит, что числа  $S_k$  — целые.

Поскольку  $|a_2| < 1$  и  $|a_3| < 1$ ,

$$S_k - a^k = a_2^k + a_3^k \longrightarrow_{k \rightarrow \infty} 0$$

причем  $S_k - a^k > 0$ . Следовательно, с ростом  $k$  в десятичной записи  $a^k$  после запятой встречаются только девятки. Гамма будет фиксированной и Виктор может определить открытый текст!

**189. Решение.** Если одна из вероятностей  $p_i$  равняется 0, то искомый ключ никогда не будет найден и порядок проверки свойств значения не имеет. Будем далее считать, что  $p_i \neq 0$ ,  $i = 1, 2, \dots, m$ .

Докажем, что свойства  $C_i$  следует проверять в порядке неубывания отношений

$$\frac{t_i}{q_i}, \quad \text{где } q_i = 1 - p_i.$$

Введём в рассмотрение производящие функции

$$f_i(x) = \sum_{m \geq 0} p_i q_i^{m-1} x^{mt_i} = \frac{p_i x^{t_i}}{1 - q_i x^{t_i}}.$$

Коэффициент при  $x^{mt_i}$  в  $f_i(x)$  есть вероятность того, что для определения ключа, удовлетворяющего  $C_i$ , потребуется проверить  $m$  случайных ключей. Используя свойства производящих функций, можно находить различные характеристики времени поиска. Например, среднее время поиска ключа, удовлетворяющего  $C_i$ , есть

$$f'_i(1) = \frac{t_i}{p_i}.$$

Время поиска объекта, удовлетворяющего сначала свойству  $C_i$ , а затем и свойству  $C_j$ , описывают композиции  $f_{ij}(x) = f_j(f_i(x))$ . Среднее время поиска в этом случае есть

$$f'_{ij}(x) = \frac{1}{p_j} \left( t_j + \frac{t_i}{p_i} \right).$$

Для сравнения, среднее время поиска ключа, удовлетворяющего сначала  $C_j$ , а затем и  $C_i$ , есть

$$f'_{ji}(x) = \frac{1}{p_i} \left( t_i + \frac{t_j}{p_j} \right).$$

Если  $t_i/q_i < t_j/q_j$ , то

$$\frac{1}{p_j} \left( t_j + \frac{t_i}{p_i} \right) < \frac{1}{p_i} \left( t_i + \frac{t_j}{p_j} \right).$$

Поэтому в этом случае  $C_i$  лучше проверять перед  $C_j$ . Проведённые рассуждения можно распространить на тройки, четвёрки, ...,  $n$ -ки свойств и получить нужный результат. Например, при рассмотрении троек мы имеем дело с композициями  $f_{ijk} = f_k(f_j(f_i(x)))$  и средними временами

$$\frac{1}{p_k} \left( t_k + \frac{1}{p_j} \left( t_j + \frac{t_i}{p_i} \right) \right).$$

Среднее время будет минимальным (относительно перестановок  $C_i$ ,  $C_j$ ,  $C_k$ ), если

$$\frac{t_i}{q_i} \leq \frac{t_j}{q_j} \leq \frac{t_k}{q_k}.$$

**190. Решение.** В случайном пароле встретится  $k$  единиц и, соответственно,  $n - k$  нулей с вероятностью  $2^{-n} \binom{n}{k}$ . Для такого пароля Виктору потребуется проверить  $\binom{n}{k}$  вариантов. Таким образом, среднее число вариантов есть  $2^{-n} S(n)$ , где

$$S(n) = \sum_{k=0}^n \binom{n}{k} \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} \binom{n}{n-k}.$$

Сумма  $S(n)$  совпадает с коэффициентом при  $x^n$  в произведении

$$(x+1)^n (1+x)^n = \left( \sum_{k=0}^n \binom{n}{k} x^k \right) \left( \sum_{k=0}^n \binom{n}{n-k} x^{n-k} \right).$$

Но  $(x+1)^n (1+x)^n = (1+x)^{2n}$  и, следовательно,

$$S(n) = \binom{2n}{n}.$$

Воспользовавшись формулой Стирлинга, получаем

$$2^{-n} S(n) \sim \frac{2^n}{\sqrt{\pi n}}.$$

Как видим, среднее число паролей, которые требуется проверить Виктору, уменьшается (асимптотически) в  $\sqrt{\pi n}$  раз.

**191. Решение.** Докажем, что Боб должен проверять сигнатуры вирусов в порядке неубывания отношений  $t_i/p_i$ . Пусть  $\mathcal{V}_i$  — признак заражения вирусом  $V_i$ . Требуется минимизировать среднее время вычисления предиката

$$\mathcal{V}_1 \vee \mathcal{V}_2 \vee \dots \vee \mathcal{V}_n$$

(«программа заражена некоторым из вирусов») или его отрицания

$$\overline{\mathcal{V}}_1 \vee \overline{\mathcal{V}}_2 \vee \dots \vee \overline{\mathcal{V}}_n$$

(«программа не заражена ни одним из вирусов»).

При решении задачи 189 «Генерация ключа» мы доказали, что признаки  $\bar{\mathcal{V}}_i$  оптимально вычислять в порядке неубывания отношений

$$\frac{t_i}{1 - \mathbf{P}\{\bar{\mathcal{V}}_i = 1\}} = \frac{t_i}{p_i},$$

что и требовалось доказать.

**192. Решение.** Виктор поступает следующим образом:

1. Выбирает случайный блок  $X_B$  и посыпает его Алисе.
2. Получает от Алисы шифртекст  $(C_1, C_2)$ . Согласно правилам зашифрования в режиме сцепления блоков

$$C_1 = F_\theta(X_A), C_2 = F_\theta(C_1 \oplus X_B)$$

где  $F_\theta$  — зашифрование блока на ключе  $\theta$ .

3. Отправляет Алисе пару  $(O, C_1)$ , где  $O$  — нулевой блок.

Алиса выполняет расшифрование полученной пары:

$$X''_B = F_\theta^{-1}(O), \quad X''_A = F_\theta^{-1}(C_1) \oplus O = F_\theta^{-1}(F_\theta(X_A)) = X_A.$$

Равенство  $X''_A = X_A$  выполнено, и Алиса принимает Виктора за Боба.

**193. Решение.** Если  $M(a)$  — чётное, то  $v = g^{M(a)}$  — квадратичный вычет по модулю  $p$ , т. е.  $v^{(p-1)/2} = 1 \pmod{p}$ . Если  $M(a)$  — нечётное, то  $g^{M(a)}$  — квадратичный невычет. Перехватывая открытый ключ  $g^{M(a)}$ , проверяя его на вычет/невычет, Виктор по известной всем матрице  $M$  получает одно линейное соотношение для битов  $a$ . Это соотношение задаётся последним столбцом  $M$ .

Для того, чтобы определить ключ  $a$  полностью, Виктору требуется дождаться использования сеансовых матриц  $M_1, M_2, \dots, M_t$ , последние столбцы в совокупности имеют полный ранг.

Известно, что случайная двоичная матрица размера  $n \times (n + d)$  имеет полный ранг с вероятностью близкой к

$$\prod_{i=d+1}^{\infty} \left(1 - \frac{1}{2^i}\right),$$

например, близкой к  $p = 0,2887880951\dots$  при  $d = 0$ .

При  $t = 127 + 3$  Виктор действительно получит матрицу полного ранга с высокой вероятностью

$$\frac{p}{\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8}} \approx 0,880393$$

и определит личный ключ  $a$ .

Более того, если Виктор знает  $g^a$ , то у него есть ещё одно линейное соотношение и вероятность успеха повышается до  $\approx 0,880393/\frac{15}{16} \approx 0,939086$ .

**194. Решение.** Задача состоит в статистическом оценивании и, таким образом, не имеет однозначного решения. Рассмотрим различные оценки объёма серии, которые могут пригодиться Виктору.

Будем анализировать общий случай, когда пользователи получают машины с номерами  $m_1, m_2, \dots, m_k$ . Пусть  $m = \max m_i$ . Обозначим  $n^{\lfloor k \rfloor} = n(n-1)\dots(n-k+1)$  и пусть символ  $\propto$  означает «пропорционально».

1. *Байесовская оценка.* Предположим, что объём выпущенной серии — случайная величина с равномерным распределением на множестве  $\{1, 2, \dots, N\}$ , т. е. Трент произведёт  $n$  машин с вероятностью

$$\pi(n) = \frac{1}{N}.$$

Здесь  $N$  — максимальные производственные ресурсы Трента (уточним позднее).

Условная вероятность того, что пользователи получат машины с номерами  $m_1, m_2, \dots, m_k$  при объёме серии  $n$  есть

$$p(m_1, m_2, \dots, m_k | n) = \begin{cases} 1/n^{\lfloor k \rfloor}, & m \leq n \leq N, \\ 0, & \text{в противном случае.} \end{cases}$$

По формуле Байеса апостериорная вероятность (при  $m \leq n \leq N$ )

$$p(n | m_1, m_2, \dots, m_k) = \frac{p(m_1, m_2, \dots, m_k | n)\pi(n)}{p(m_1, m_2, \dots, m_k)} \propto 1/n^{\lfloor k \rfloor}.$$

Адекватной оценкой  $n$  является медиана распределения  $p(n | m_1, m_2, \dots, m_k)$ , т. е. такое  $n_1$ , что суммы

$$\sum_{n=m}^{n_1} 1/n^{\lfloor k \rfloor} \text{ и } \sum_{n=n_1}^N 1/n^{\lfloor k \rfloor}$$

максимально близки. Предполагая  $k \geq 2$ , считая  $n^{\lfloor k \rfloor} \approx n^k$ , заменяя суммы интегралами и устремляя  $N$  к бесконечности (ресурсы Трента неограничены), получаем условие

$$1/m^{k-1} - 1/n_1^{k-1} \approx 1/n_1^{k-1},$$

откуда

$$n_1 \approx m^{\frac{k-1}{k}}\sqrt{2} \approx m\frac{k}{k-1}.$$

В нашем случае  $n_1 \approx 734\sqrt{2} \approx 1038$ .

**2. Метод моментов.** Читатель сайта CryptoOfficer, где выкладывались данные задачи (<http://apmi.bsu.by/resources/tasks.html>), предложил воспользоваться следующим соображением: при объёме серии  $n$  среднее номеров выданных машин должно быть близко к  $(n+1)/2$ . Отсюда получаем оценку

$$n_3 = \frac{2}{k}(m_1 + m_2 + \dots + m_k) - 1.$$

В нашем случае  $n_3 \approx 996$ .

На самом деле. На самом деле Трент произвел  $n = 1000$  машин и выбирал случайные номера, используя знаки после запятой в разложении  $e\pi = 8,539734222\dots$

**195. Решение.** Докажем сначала теорему Диемитко. Пусть  $\text{ord}(a)$  — порядок  $a$  по модулю  $n$  (т. е.  $\text{ord}(a)$  — наименьшее натуральное число  $\ell$  такое, что  $a^\ell \equiv 1 \pmod{n}$ ). Условия 1) и 2) означают, что  $q|\text{ord}(a)$ . В свою очередь  $\text{ord}(a)$  делит значение функции Эйлера  $\varphi(n)$ . Таким образом,  $q|\varphi(n)$  и  $q$  либо совпадает с некоторым простым делителем  $p$  числа  $n$ , либо делит  $p-1$  (если  $p^2|n$ ). Первый случай невозможен, во втором случае  $p = qr + 1$  и

$$n = (qr + 1)(qs + 1),$$

где  $r, s$  — чётные,  $r \geq 2$ . Если  $n$  — составное, то  $s \geq 2$  и, следовательно,  $n \geq (2q + 1)^2$ . Однако последнее условие нарушается при  $R < 4(q + 1)$ , и теорема Диемитко доказана.

Боб строит  $n$  так, что условия 1), 2) могут выполняться, хотя условие  $R < 4(q + 1)$  будет нарушено и  $n$  окажется составным. Конкретнее, составное  $n$  Боб получит, если

- а)  $n = p^2$ , где  $p = 2q + 1$  — простое;  
 б)  $n$  является  $k$ -битовым числом, а  $q = \lfloor k/2 \rfloor$ -битовым ( $k$  должно быть нечётным);  
 в)  $\text{ord}(a) = q$  или  $\text{ord}(a) = 2q$ .

Например,  $n = 121 = (2 \cdot 5 + 1)^2$  — минимальное число, удовлетворяющее первым двум требованиям. Мультиплексивная группа кольца вычетов по модулю  $n = p^2 = (2q + 1)^2$  является циклической порядка  $\varphi(n) = 2pq$ . Пусть  $g$  — образующий этой группы. Тогда основания

$$a = g^{ip} \pmod{n}, \quad i = 1, 2, \dots, q-1, q+1, \dots, 2q-1,$$

имеют порядок  $q$  или  $2q$  и эти основания будут ошибочно свидетельствовать в пользу простоты составного  $n$ . Например, для  $n = 121$  и  $q = 5$  ложными свидетелями будут  $a \in \{3, 9, 27, 40, 81, 94, 112, 118\}$ .

**196. Решение.** В режиме гаммирования с обратной связью последовательные 16-байтовые блоки открытого текста  $X_1, \dots, X_T$  зашифровываются следующим образом:

$$Y_t = F_K(Y_{t-1} \oplus X_t), \quad t = 1, \dots, T.$$

Здесь  $Y_0$  — синхропосылка,  $Y_1, \dots, Y_T$  — блоки шифртекста,  $F_K$  — зашифрование отдельного блока на ключе  $K$  (подробнее см. СТБ 34.101.31).

Если Виктор умеет определять  $F_K(Y)$  для произвольного блока  $Y$ , то он сможет пройти аутентификацию перед Алисой или Бобом, а также расшифровать присланные ими данные:

$$X_t = F_K(Y_{t-1} \oplus Y_t), \quad t = 1, \dots, T.$$

Остается описать протокол определения  $F_K(Y)$ :

1. Виктор регистрируется под 16-байтовым именем  $Id$ , всякий раз новым.
2. Виктор как  $Id$  объявляет, что является поклонником The Group и у него есть треки песен, которые разыскивают Алиса и Боб.
3. Алиса и Боб обрадованы и обращаются к  $Id$  с запросом. Пусть первой обратилась Алиса.

4. Виктор как  $Id$  проверяет Алису, высыпая ей блок  $Y$  в качестве синхропосылки.

5. Алиса отвечает блоком  $Z = F_K(Y) \oplus Id$ .

6. Виктор определяет  $F_K(Y) = Z \oplus Id$  и обрывается связь с Алисой.

7. Алиса разочарована и выражает Виктору как  $Id$  своё недоумение.

8. Виктор, заметая следы, удаляет учётную запись  $Id$ .

**197. Решение.** Матрица  $M_1$  является клеткой Фробениуса с неприводимым характеристическим многочленом  $f(x) = x^4 + x + 1$ . Степени  $M_1^i$ ,  $i = 0, 1, \dots, 15$ , вместе с нулевой матрицей образуют поле из 16 элементов. Матрица  $M_2$  является элементом этого поля:  $M_2 = M_1^{14}$ .

В задаче требуется дополнить набор  $(M_0, M_1, M_2)$  до базиса поля. Дополнить можно матрицей

$$M_1^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

**198. Решение.** Бросив кубик дважды, Боб получает случайные числа  $r_0, r_1 \in \{0, 1, \dots, 5\}$ . По ним Боб может построить случайное число  $r = r_0 + 6r_1$  с равномерным распределением на  $\{0, 1, \dots, 35\}$ . Если  $r < 33$ , то Боб преобразует  $r$  в истинно-истинно случайный символ русского алфавита ( $A = 0$ ,  $B = 1, \dots, Я = 32$ ). Если же  $r \in \{33, 34, 35\}$ , то Боб снова бросает кубик дважды, снова формирует  $r$  и так далее, до тех пор, пока условие  $r < 33$  не будет выполнено.

Среднее число бросков для генерации одного символа:

$$\sum_{t \geq 1} 2t \cdot \mathbf{P}\{\text{потребуется } 2t \text{ бросков}\} = \\ = 2 \sum_{t \geq 0} \mathbf{P}\{\text{потребуется более } 2t \text{ бросков}\} = 2 \sum_{t \geq 0} \left(\frac{3}{36}\right)^t = 2 \cdot \frac{36}{33} < \sqrt{5},$$

и ответ на первый вопрос положительный.

При переходе к английскому алфавиту Бобу после двух бросков потребуется сделать еще по крайней мере один с вероятностью

$\frac{36 - 26}{36}$ . Поэтому среднее число бросков не меньше

$$2 + \frac{10}{36} > \sqrt{5}$$

и ответ на второй вопрос также положительный.

Описанный способ генерации случайных чисел соответствует методу исключения фон Неймана. Является ли способ оптимальным? Оказывается, что нет — существует алгоритм, в котором среднее число бросков меньше. Основная идея алгоритма — не игнорировать случайное число  $r$ , даже если оно не попадает в допустимое множество. Опишем алгоритм для общего случая. Пусть имеются истинно-истинно случайные цифры от 0 до  $a - 1$ . Покажем как, используя эти цифры, построить истинно-истинно случайное число от 0 до  $n - 1$ . На шагах алгоритма будем пересчитывать порог  $R$  и формировать случайное число  $r$  с равномерным распределением на  $\{0, 1, \dots, R - 1\}$ . Будем ожидать выполнения условия  $r < n$ . Конкретнее, алгоритм имеет следующий вид:

1. Установить  $r := 0$ ,  $R := 1$ .
2. Найти  $d := \lceil \log_a n / R \rceil$ .
3. Получить  $d$  очередных случайных цифр  $r_0, \dots, r_{d-1}$ .
4. Установить  $r := r_0 + ar_1 + \dots + a^{d-1}r_{d-1} + a^dr$ ,  $R := R \cdot a^d$  ( $r$  снова имеет равномерное распределение на  $\{0, 1, \dots, R - 1\}$ ).
5. Найти  $e := R \bmod n$ .
6. Если  $r \in \{0, 1, \dots, R - e - 1\}$ , т. е.  $r < n$ , то возвратить  $r$ .
7. Здесь  $r$  имеет равномерное распределение на  $\{R - e, \dots, R - 1\}$ . Учтём этот факт следующими образом:  $r := r - (R - e)$ ,  $R := e$ .
8. Вернуться к шагу 2.

Оценим сложность алгоритма. Пусть  $f_{a,n}(R)$  — среднее число цифр, которое потребуется использовать при наличии случайного числа  $r$  с равномерным распределением на  $\{0, 1, \dots, R - 1\}$ . Тогда

$$f_{a,n}(R) = d + \frac{Ra^d \bmod n}{Ra^d} f_{a,n}(Ra^d \bmod n), \quad d = \lceil \log_a n / R \rceil.$$

Например, в интересующем нас случае  $a = 6$ ,  $n = 33$  получаем систему уравнений:

$$\begin{aligned} f_{6,33}(1) &= 2 + \frac{1}{12}f_{6,33}(3), & f_{6,33}(3) &= 2 + \frac{1}{12}f_{6,33}(9), \\ f_{6,33}(9) &= 1 + \frac{7}{18}f_{6,33}(21), & f_{6,33}(21) &= 1 + \frac{3}{14}f_{6,33}(27), \\ f_{6,33}(27) &= 1 + \frac{5}{27}f_{6,33}(30), & f_{6,33}(30) &= 1 + \frac{1}{12}f_{6,33}(15), \\ f_{6,33}(15) &= 1 + \frac{4}{15}f_{6,33}(24), & f_{6,33}(24) &= 1 + \frac{1}{12}f_{6,33}(12), \\ f_{6,33}(12) &= 1 + \frac{1}{12}f_{6,33}(6), & f_{6,33}(6) &= 1 + \frac{1}{12}f_{6,33}(3). \end{aligned}$$

Решая эту систему, определяем интересующее нас среднее число бросков

$$f_{6,33}(1) = \frac{84653}{38885} < \frac{84653 - 1}{38885 - 1} = \frac{21163}{9721} \approx 2,177.$$

Для сравнения,

$$f_{6,26}(1) = \frac{544111}{233285} \approx 2,332.$$

**199. Решение.** Докажем, что  $D(p) \geq 10$ .

Справедлив один из случаев:  $p \equiv 1 \pmod{6}$  или  $p \equiv 5 \pmod{6}$ . Пусть  $p \equiv 1 \pmod{6}$ , т. е.  $p = 6k+1$ . Если  $k \neq q_0$ , то  $D(p) > (p-1)/q_0 \geq 12$ . Если же  $k = q_0$ , то  $(p+1)/q_1 \geq 4$ . Действительно,

- 1) если  $p+1 = 2q_1$ , то  $q_1 = 1 + 3q_0$  — чётное, противоречие;
- 2) если  $p+1 = 3q_1$ , то  $3(q_1 - 2q_0) = 2$ , снова противоречие.

В целом, при  $k = q_0$  справедлива оценка  $D(p) \geq 6 + 4 = 10$ . Случай  $p \equiv 5 \pmod{6}$  рассматривается аналогично.

**200. Решение.** Пусть

$$n = \prod_{i=1}^k p_i^{e_i},$$

где  $k$  — нечётное,  $p_i$  — различные простые,  $p_i = 2^s r_i + 1$ . Значение функции Эйлера

$$\varphi(n) = \prod_{i=1}^k p_i^{e_i-1} (p_i - 1)$$

и

$$d = \text{НОД}(n, \varphi(n)) = \prod_{i=1}^k p_i^{e_i-1}.$$

Поэтому

$$\frac{\varphi(n)}{d} = \prod_{i=1}^k (p_i - 1) = 2^{sk} r',$$

$$\frac{n}{d} = \prod_{i=1}^k (p_i) = \prod_{i=1}^k (2^s r_i + 1) = 2^s r'' + 1,$$

где  $r' = r_1 r_2 \dots r_k$  и  $r'' = r_1 + r_2 + \dots + r_k + 2^s r'''$  — нечётные.

Определяя максимальную степень 2, на которую делится  $\frac{n}{d} - 1$ , находим  $s$ . Определяя максимальную степень 2, на которую делится  $\frac{\varphi(n)}{d}$ , находим  $sk$ . После этого находим  $k = \frac{sk}{s}$ .

**201. Решение.** Число  $p = 10009$  — простое, а  $p - 1 = 2^3 \cdot 3^2 \cdot 139$ .

Ключ  $k$  должен выбираться так, что  $\text{НОД}(k, p - 1) = 8$ . Прямые расчёты показывают, что для всех таких  $k$  выполняется:

$$z^k \neq \tilde{z}^k \pmod{p}$$

для любых различных  $z, \tilde{z} \in \{10001, \dots, 10008\}$ . Поэтому результат зашифрования допустимого PIN-кода  $x \in \{0, 1, \dots, 9999\}$  может совпадать с (воображаемым) результатом зашифрования только одного недопустимого PIN-кода  $\tilde{x} \in \{10000, 10001, \dots, 10008\}$ .

Определить  $x$  по  $y = (x + 1)^k \pmod{p}$  можно следующим образом:

1. Представить  $k$  в виде  $8\ell$ , где  $\text{НОД}(\ell, p - 1) = 1$ .
2. Найти  $z = y^{\ell^{-1} \pmod{p-1}} = (x + 1)^8 \pmod{p}$ .
3. Применить алгоритм Тонелли — Шенкса и найти квадратные корни из  $z$  по модулю  $p$ . Пусть  $z_1, z_2$  — найденные корни.
4. Снова применить алгоритм Тонелли — Шенкса и найти квадратные корни из  $z_1, z_2$ . Пусть  $z_3, z_4, z_5, z_6$  — новые корни.
5. Наконец, ещё раз применить алгоритм Тонелли — Шенкса и найти квадратные корни из  $z_3, z_4, z_5, z_6$ . Пусть  $x_1, x_2, \dots, x_8$  — окончательные корни. Фактически это корни 8-й степени из  $z$  по модулю  $p$ .
6. Возвратить  $(x_i - 1) \pmod{p}, i = 1, 2, \dots, 8$ .

**202. Решение.** В вопросе указываются дроби  $\pi(10^n)/10^n$ , где  $\pi(x)$  — число простых, не превосходящих  $x$ . Следующий элемент последовательности будет  $\frac{9592}{100000}$ . Ответив на вопрос, Виктор устраивается на работу в некоторый филиал и передаёт дату очередной смены ключа самому себе как шифртекст. Результатом расшифрования будет новый парный ключ. Этот ключ позволит Виктору прочитывать весь трафик между филиалами, а также определять следующие парные

ключи. Интересно, что описанный механизм смены ключа определён в стандарте Интернет RFC 4357. Расшифровывается даже не дата, а фиксированная константа.

**203. Решение.** Трент посчитал, что Виктор разослал письма не в одну, а в  $2^{16} = 65536$  газет. В первых 256 письмах Виктор указал байт 0, во вторых 256 — байт 1, и так далее. После опубликования истинного ключа Виктор продолжил работать только с теми 256 газетами, в письмах которым первый байт был угадан. Во втором письме Виктор разослал 256 вариантов первого байта второго ключа и угадал этот байт в письме в Gnutiez. Атака Виктора была описана в заметках М. Гарднера применительно к предсказанию результатов скачек.

**205. Решение.** Будем рассматривать многочлены над полем  $GF(2)$ . Нам требуется перемножить многочлены  $a(x), b(x)$ , степени которых меньше 8. Многочлены представляются байтами.

Выберем примитивный многочлен  $f_1(x)$  степени 8. Если  $a(x) \neq 0$ , то  $a(x) = x^d \pmod{f_1(x)}$  для некоторого  $d \in \{0, 1, \dots, 254\}$ . Действительно, в противном случае  $x^{d_1} = x^{d_2} \pmod{f_1(x)}$  для некоторых  $0 \leq d_1 < d_2 \leq 254$ , т. е.  $f_1(x) \mid x^{d_2-d_1} - 1$ , что противоречит примитивности  $f_1(x)$ .

Величину  $d$ , которая фигурирует в представлении  $a(x)$  назовём логарифмом по модулю  $f_1(x)$  и обозначим через  $\log a(x) \pmod{f_1(x)}$ . Таблицу логарифмов сохраним в массиве `log1`.

Выберем ещё один примитивный многочлен  $f_2(x)$  степени 8, отличный от  $f_1(x)$ . Логарифмы по модулю  $f_2(x)$  сохраним в массиве `log2`.

Пусть

$$d_1 = (\log a(x) \pmod{f_1(x)} + \log b(x) \pmod{f_1(x)}) \pmod{255},$$

$$d_2 = (\log a(x) \pmod{f_2(x)} + \log b(x) \pmod{f_2(x)}) \pmod{255}.$$

Тогда

$$a(x)b(x) = x^{d_i} \pmod{f_i(x)}, \quad i = 1, 2.$$

мы имеем дело с китайской системой сравнений, которую можно решить методом Гаусса:

$$a(x)b(x) = (f_2^*(x)f_2(x)x^{d_1} + f_1^*(x)f_1(x)x^{d_2}) \pmod{f_1(x)f_2(x)}.$$

Здесь  $f_1^*(x) = f_1(x)^{-1} \pmod{f_2(x)}$ ,  $f_2^*(x) = f_2(x)^{-1} \pmod{f_1(x)}$ .

В программе решение системы реализовано обращение к массивам, задающим отображения

$$d \mapsto f_i^*(x)f_i(x)x^d \bmod f_1(x)f_2(x).$$

При  $f_1(x) = x^8 + x^4 + x^3 + x^2 + 1$  и  $f_2(x) = x^8 + x^6 + x^5 + x^4 + 1$  (возвратный к  $f_1$ ) получаем следующее заполнение массивов <http://apmi.bsu.by/assets/files/tasks/task11.zip>.

**206. Решение.** Пусть  $f(x) = a_{n-1}(x)x^{(n-1)w} + \dots + a_1(x)x^w + a_0(x)$ , где  $\deg a_i < w$ . Пусть  $g(x)$  делит  $f(x)$  и  $\deg g < w$ .

Предположим, что

$$f(x)/g(x) = b_{n-1}(x)x^{(n-1)w} + \dots + b_1(x)x^w + b_0(x),$$

где  $\deg b_i < w$ . Тогда

$$a_{n-1}(x)x^{(n-1)w} + a_0(x) = g(x)(b_{n-1}(x)x^{(n-1)w} + \dots + b_1(x)x^w + b_0(x)).$$

При этом

$$a(x) = g(x)b_0(x) \pmod{x^w}$$

и

$$b_0(x) = a(x)g^*(x) \bmod w^w,$$

где  $g^*(x) = g(x)^{-1} \bmod x^w$ .

После определения  $b_0$  можно определить  $b_1$ , использовав соотношение

$$(f(x) - g(x)b_0(x))/x^w = g(x)(b_{n-1}(x)x^{(n-2)w} + \dots + b_2(x)x^w + b_1(x)),$$

затем  $b_2$  и так далее.

В программе  $w = 8$ ,  $g^*(x) = (x^2 + 1)(x^4 + 1) = (x + 1)^6$  и следовательно,

$$g(x) = (x + 1)^2 = x^2 + 1.$$

**204. Решение.** Конечно, задачу можно решать «в лоб» путём перебора  $2^{32}$  сообщений. Предложим менее тривиальное решение, которое можно применить к функциям семейства FNV с длинами хэш-значений 64, 128, 256, 512 и 1024. Решение «в лоб» на таких длинах уже не пройдет.

Мультипликативные операции функции FNV ведутся в кольце  $\mathbb{Z}_{2^{32}} = \{0, 1, \dots, 2^{32} - 1\}$ . Мультипликативная группа  $\mathbb{Z}_{2^{32}}^*$  этого кольца состоит из нечётных чисел и имеет порядок  $2^{31}$ . По теореме Лагранжа все элементы  $a \in \mathbb{Z}_{2^{32}}^*$  имеют порядок, который делит  $2^{31}$ .

Множитель 16777619 функции FNV имеет порядок  $2^{30}$  и половину элементов  $a \in \mathbb{Z}_{2^{32}}^*$  можно представить как  $16777619^x \bmod 2^{32}$ . Числа 2166136261, 2166136263 так представить нельзя, а вот число 2166136265 можно:

$$2166136265 = 16777619^{695367386} \bmod 2^{32}.$$

Для нахождения искомого представления можно использовать логарифмирование по методу Поллига — Хэллмана. Логарифмирование будет быстрым, поскольку порядок основания 16777619 является степенью 2, т. е. не содержит больших простых делителей.

Рассмотрим обработку сообщения `msg` следующей структуры (умножения выполняются по модулю  $2^{32}$ ):

1. Первый байт равняется 12. После его обработки

$$\text{hash} = (2166136261 \oplus 12) \cdot 16777619 = 2166136265 \cdot 16777619.$$

2. Следующие  $2^{30} - 695367386 - 1$  байт нулевые. После их обработки

$$\text{hash} = 2166136265 \cdot 16777619^{2^{30}-695367386} = 1677619^{2^{30}} = 1.$$

3. Последний байт равняется 1. После его обработки

$$\text{hash} = (1 \oplus 1) \cdot 16777619 = 0.$$

чего и требовалось добиться.

**207. Решение.** В правой части оператора

```
((mul = b[i]) *= a[j]) += carry + c[i + j]
```

может произойти переполнение. Следует писать

```
((((mul = b[i]) *= a[j]) += carry) += c[i + j])
```

**208. Решение.** В книге Уоррена Генри мл. «Алгоритмические трюки для программистов» собраны примеры необычных манипуляций над машинными словами. В том числе представлены способы реализации предикатов сравнения  $x == y$  и  $x < y$  с помощью одних только арифметических операций и сдвигов.

Воспользуемся трюками Уоррена:

```
#define safeEq(x, y) \ (~((x) - (y) | (y) - (x)) >> (8
    * sizeof(word)
- 1))
#define safeLess(x, y) \ ((~(x) & (y) | ((~(x) |
    (y)) & (x) -
(y))) >> (8 * sizeof(word) - 1))

word zzAddSafe(word
c[], const word
a[], const word b[], size_t n) {
    register word carry = 0;
    register word w;
    size_t i;
    for (i = 0; i < n; ++i)
    {
        w = a[i] + b[i] + carry;
        carry &= safeEq(w, a[i]);
        carry |= safeLess(w, a[i]);
        c[i] = w;
    }
    w = 0;
    return carry;
}
```

**209. Решение.** Будем считать, что  $\text{val} < 2^{16}$ . Пусть  $B = 2^{32}$  и пусть  $a = (a_{n-1} \dots a_1 a_0)_B$  — запись числа  $a$  в системе счисления по основанию  $B$ :  $a = \sum_{i=0}^{n-1} a_i B^i, 0 \leq a_i < B$ .

Вот новая функция:

```
uint32 zzModVal2(const uint32 a[], size_t n, uint32
val) {
    uint32 r0 = 0;
    uint64 r1 = 0;
    uint32 b = (uint32)-1 % val + 1;
    if (b == val)
        return a[0] % val;
    while (n--)
        r1 *= b,
        r1 += r0,
```

```

r1 *= b,
r1 += a[n],
r0 = (uint32)r1,
r1 >>= 32;
while (r1 != 0)
    r1 *= b,
    r1 += r0 % val,
    r0 = (uint32)r1,
    r1 >>= 32;
return r0 % val;
}

```

В этой функции сначала определяется значение  $b = B \bmod \text{val}$ . Если  $b = 0$ , т. е.  $\text{val} \mid B$ , то возвращается  $a_0 \bmod \text{val}$ . Если же  $b \neq 0$ , то определяется и приводится по модулю  $\text{val}$  сумма

$$r = \sum_{i=0}^{n-1} a_i b^i, \quad a = \sum_{i=0}^{n-1} a_i B^i, \quad r = a \pmod{\text{val}}.$$

Реализован следующий алгоритм:

1.  $r = (r_1 r_0)_B \leftarrow 0$ .
2. Для  $i = n - 1, \dots, 0$ :
  - (a)  $r \leftarrow (r_1 b + r_0)b + a_i$ .
3. Пока  $r_1 \neq 0$ :
  - (a)  $r \leftarrow r_1 b + (r_0 \bmod \text{val})$ .
4. Возвратить  $r_0 \bmod \text{val}$ .

После каждой итерации 2а:

$$r \leq (B-1)(1+b+b^2) \leq (B-1)(\text{val}^2 - \text{val} + 1) < (B-1)(B+1) < B^2.$$

После первой итерации 3а:

$$r \leq (B-1)(\text{val}-1) + (\text{val}-1) = B(\text{val}-1).$$

После второй итерации 3а:

$$r \leq (\text{val}-1)(\text{val}-1) + (\text{val}-1) = \text{val}(\text{val}-1) < B.$$

Таким образом, будет выполнено не более двух итераций 3а, и требуемые в постановке задачи условия на число операций выполняются.

## Комбинаторные задачи

**214.**  $0; 2^{n-1}; 2^{n-1}$ .

**217.**  $n \cdot m; C_n^k \cdot C_m^l$ .

**218.**  $C_{n+m}^n$ .

**220.** а)  $C_n^2$ ; б)  $C_n^3$ ; в)  $(n^2 + n + 2)/2$ ; г)  $2n$ .

**222.** 6;  $10!/24$ .

**223.**  $(n!)^2$ .

**224.**  $8!$ .

**225.**  $(n - 2)!$ .

**226.**  $(n - 1)!$ .

**227.**  $C_{18}^7$ .

**228. Указание.** Закодируйте каждую выборку так:  $0^{k_1}10^{k_2}1\dots10^{k_n}$ , где  $k_i$  — количество элементов типа  $i$ ,  $1 \leq i \leq n$ ,  $k_1 + \dots + k_n = k$ .

**229.**  $C_{n+1}^2$ .

**230.** 56.

**231.** 147.

**232.**  $2^{nm}; 2^n(2^n - 1)\dots(2^n - m + 1)$ .

**233.** 20.

**234.** 20.

**235.** а) 6983776800 ; б)  $\sum_{k_1+k_2=5, \ell_1+\ell_2=4} \frac{20!}{k_1!k_2!2!3!\ell_1!\ell_2!}$ .

**236.** 36.

**237.** 20.

**238.** 14833.

**239.**  $\sum_{k=0}^n (-1)^k C_n^k (n - k)^m$ .

**240.**  $C_n^\ell \sum_{k=0}^{n-\ell} (-1)^k C_{n-\ell}^k (n - \ell - k)^m$ .

**241.**  $\sum_{s=\ell}^n C_n^s \sum_{k=0}^{n-s} (-1)^k C_{n-s}^k (n - s - k)^m$ .

**242.** 864.

**243. Указание.** Определите множества  $A_i$ ,  $1 \leq i \leq n$ , как множества рассадок рыцарей за столом так, что  $i$ -я пара враждующих не сидит рядом.

**244.**  $n! \sum_{k=0}^n (-1)^k / k!$ , что при  $n \rightarrow \infty$  равно  $n!/e$ .

**249.**  $\varphi = \frac{1+\sqrt{5}}{2}$ .

**257.** (123), (145), (167), (246), (257), (347), (356).

**258.** Нет. Либо  $n = 6k + 1$ , либо  $n = 6k + 3$  для любого  $k$ .

**259.** Не достраивается.

## Элементы алгебры и теории чисел

**266.** а) 1; б) 17; в) 382; г) 1; д) 117; е) 269.

**271.** а) нет; б) да; в) да.

**273. Указание.** Предположите, что существует наибольшее простое число. Постройте число, которое будет больше, но при этом также будет простым.

**274. Указание.** Рассмотрите  $n = (k+1)! + 1$ .

**276.** а) 200; б) 192; в) 432; г) 1848; д) 3840; е) 10752.

**277.** 143.

**279.**  $\sum_{i=1}^{\varphi(n)} a_i = \frac{1}{2}n\varphi(n)$ .

**280.** а) (10111); б) (100011011); в) (1010101010); г) (100000001111); д) (11...1) — вектор из  $n$  единиц.

**281.** а)  $16 \prec 25$ ; б)  $64 \prec 68$ ; в)  $167 \prec 255$ .

**282. Указание.** Установите связь  $C_n^k$  с  $C_{n_i}^{k_i}$ ,  $i = 0, \dots, \ell$ , где  $n = (n_\ell, \dots, n_0)$ ,  $k = (k_\ell, \dots, k_0)$  — двоичные представления.

**286. Указание.** Воспользуйтесь индукцией по числу  $a$ .

**287. Указание.** Рассмотрите все натуральные числа меньшие  $m$  и взаимно простые с  $m$ , а также их произведения на число  $a$ .

**288.** Количество раскрасок:  $\frac{a^p - a}{p} + a$ .

**292.** а) 8; б) 9; в) 33; г) нет; д) 129; е) 430.

**294.** а) 1; б) 1; в) 10; г) 1; д) 13; е)  $-1$ .

**298.** а) нет; б) да; в) да; г) нет.

**299.** а)  $2 \pmod{12}$ ,  $6 \pmod{12}$ ,  $10 \pmod{12}$ ; б)  $7 \pmod{15}$ ; в)  $7 \pmod{22}$ ,  $18 \pmod{22}$ ; г)  $2 \pmod{34}$ ,  $19 \pmod{34}$ ; д) решений нет; е)  $81 \pmod{337}$ .

**301. Указание.** Использовать метод математической индукции.

**302.** а)  $207 \pmod{210}$ ; б)  $157 \pmod{935}$ ; в)  $335 \pmod{924}$ ; г)  $8479 \pmod{15015}$ .

**304.** а)  $\frac{104}{5}$ ; б)  $\frac{37}{328}$ ; в)  $\frac{1393}{972}$ ; г)  $-\frac{175}{103}$ ; д)  $\sqrt{2}$ ; е)  $\frac{1+\sqrt{5}}{2}$ ; ж)  $\sqrt{13}$ ; з)  $-\sqrt{41}$ ; и)  $\frac{10783}{1761}$ .

**305.** а)  $[5, 2, 4]$ ; б)  $[-7, 1, 2, 1, 2]$ ; в)  $[4, 3, 2, 1, 2, 3, 4]$ ; г)  $[2, 5, 1, 2, 33]$ ; д)  $[0, (1)]$ ; е)  $[0, 1, (1, 6)]$ ; ж)  $[5, (1, 1, 3, 5, 3, 1, 1, 10)]$ ; з)  $[2, (1, 1, 1, 1, 1, 1, 6)]$ .

**308.** а) 4, 11; б) 8, 13; в) 154, 373, 526; г) 38, 149, 154, 186, 191, 290, 302, 327, 339, 438, 443, 475, 480, 591, 628.

**310.** Решение можно найти в книге [13].

**311.** а) 561, 1105, 1729, 2465, 2621, 6601, 8911.

**313.** а) да; б) нет:  $101 \cdot 127$ ; в) нет:  $517 \cdot 89$ ; г) да; д) нет:  $17 \cdot 41 \cdot 233$ ; е) нет:  $41 \cdot 61 \cdot 101$ ; ж) да; з) да; и) нет:  $2767 \cdot 2957 \cdot 4211$ ; к) да.

**317.** а) нет; б) нет; в) да.

**318.** а) нет; б) да; в) нет; г) да; д) да; е) нет.

**320.**  $n = 2$ :  $x^2 + x + 1$ ;  $n = 3$ :  $x^3 + x + 1, x^3 + x^2 + 1$ ;  $n = 4$ :  $x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$ ;  $n = 5$ :  $x^5 + x^2 + 1, x^5 + x^3 + 1, x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x + 1, x^5 + x^4 + x^3 + x^2 + 1$ .

**323.**  $\varphi(p^n - 1)$ .

**330. Указание.** Воспользуйтесь задачей 321 и определите, какие слагаемые возможны в рассматриваемой сумме и сколько раз каждое из них встречается.

**331. Указание.** Используя задачу 282, покажите, что в правой части равенства нечётное число раз встречаются только слагаемые вида  $a_{1\pi}^{2^{m-1}} a_{2\pi}^{2^{m-2}} \dots a_{m\pi}^{2^0}$ , где  $\pi \in S_m$ .

## Криптосистемы с открытым ключом

**332. Указание.** Проведите непосредственную проверку.

**333.**  $d_M = 9$ ,  $d_D = 18$ ,  $d_C = 2$ ;  $K_{MD} = 3$ ,  $K_{MC} = 9$ ,  $K_{DC} = 18$ .

**334. а) РЮКЗАК.**

**335. Указание.** Проведите непосредственную проверку.

**336. а)  $c_A = 7$ ,  $d_A = 17$ ; б)  $m = 10$ .**

**337.  $m = 8$ .**

**338. ФИАЛКА.**

**339.** Секрет сохранить не удастся. Ева перехватит следующие сообщения:  $C' = x \oplus k_B$ ,  $C'' = C \oplus k_A$ ,  $C''' = C \oplus k_B$ , из которых несложно определить ключи Алисы и Боба и само сообщение:  $k_A = C' \oplus C''$ ,  $k_B = C'' \oplus C'''$ ,  $x = C' \oplus C'' \oplus C'''$ .

**340. Указание.** Воспользуйтесь теоремой Эйлера (см. задачу 287).

**341.** Открытый ключ Боба  $\{143, 7\}$ , секретный ключ —  $\{11, 13, 103\}$ . Передано секретное сообщение  $m = 21$ .

**342. Вы познали РША.**

**343. «Риджентс-парк, скамейка у пруда, в ПОЛНОЧЬ».**

**344. ФМШ.**

**345. а) открытый ключ  $\{187, 13\}$ , секретный ключ —  $\{11, 17, 37\}$ ; б) секретный номер дома 15; в) обратитесь к одной из книг по асимметричной криптографии.**

**346. Указание.** Проведите непосредственную проверку.

**347.** а) да б) нет в) нет г) да.

**348.** Передано сообщение (01101). При зашифровании Боб использовал случайные числа 31, 17, 9, 4, 22.

**349.** Передано сообщение (10100). При зашифровании Боб использовал случайные числа 2, 5, 17, 2, 3.

**350.** Бит 1 можно зашифровать двумя способами — значениями 1 и 4. Число способов зашифрования бита 0 также равно двум (независимо от значения  $y$ ), а вот конкретные значения, которые будут сопоставляться биту 0, будут зависеть от выбора  $y$ .

**351.** Несложно заметить, что это число равно  $\varphi(n) = (p - 1)(q - 1)$ .

**352.** Нет.

**353. Указание.** Проведите непосредственную проверку.

**354.** Открытый ключ:  $d = 21$ ; переданные сообщения:  $r = 17$ ,  $e = 12$ .

**355.** Передано сообщение  $m = 5$ . При этом Боб выбрал случайное число  $s = 12$ .

**356.** а) открытый ключ  $\{101, 3, d_A = 22\}$ , секретный ключ  $\{c_A = 6\}$ ; б) при расшифровании всех сообщений получаем числа 25, 50, 50. В Центр следует отправить значение из первого сообщения (66, 82), так как другие два сообщения (66, 63), (97, 73) легко мог сгенерировать злоумышленник путём модификации первого сообщения (объясните сами, каким образом); в) обратитесь к одной из книг по асимметричной криптографии.

**357.** Маршрут: 100110101110010001.

## Цифровая подпись

**358. Указание.** Проведите непосредственную проверку.

**359.** Чтобы достичь успеха Еве требуется найти число  $s = y^{d_A} \pmod{n_A}$ . Для этого ей остаётся узнать лишь значение  $d_A$ , которое находится из уравнения  $e_A d_A = 1 \pmod{\varphi(n_A)}$ .

**360.** Автор — Алиса.

**361.** 9 — код топлива MD, 11 — FW.

**362. Указание.** Проведите непосредственную проверку.

**363.** Так как единственным секретом Алисы является число  $c_A$ , то именно его и нужно узнать Еве. Это число можно узнать из уравнения  $d_A = g^{c_A} \pmod{p}$ .

**364.** Автор — Боб.

**365.** Луиджи Копатти.

**366. Указание.** Проведите непосредственную проверку.

**367.** Для успешного подделывания подписи Еве требуется знать  $c_{A_i}$ . Для этого нужно решить уравнения  $d_{A_i} = (c_{A_i}^{-1})^2 \pmod{n}$ ,  $i = 1, \dots, m$ .

**368.** Нет.

## Криптография на эллиптических кривых

**370.** а) замена  $x = x'$ ,  $y = y' - \frac{a_1}{2}x' - \frac{a_3}{2}$ ; б) сначала привести к виду а) той же заменой, что и в а); затем  $x = x' - \frac{a_2}{3}$ ,  $y = y'$ ; в) если  $a_1 = 0$ , то  $x = x' + a_2$ ,  $y = y'$ ; если  $a_1 \neq 0$ , то сначала заменой  $x = a_1^2x' + \frac{a_3}{a_1}$ ,  $y = a_1^3y'$  привести к виду  $y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$ , а затем замена  $x = x'$ ,  $y = y' + a_4$ .

**372.** а) нет; б) да; в) нет.

**373.** а) (2,2), (2,3); б) (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3); в) (7,3), (7,8), (8,3), (8,8), (10,4), (10,7); г) (0,3), (0,8), (1,3), (1,8), (2,2), (2,9), (3,0), (4,5), (4,6), (7,2), (7,9), (9,5), (9,6), (10,3), (10,8); д) (1,2), (1,17), (8,3), (8,16), (10,9), (10,10), (14,9), (14,10), (17,7), (17,12), (18,0); е) (0,2), (0,17), (1,8), (1,11), (2,4), (2,15), (4,0), (5,5), (5,14), (6,2), (6,17), (7,0), (8,0), (10,6), (10,13), (13,2), (13,17), (16,3), (16,16), (17,7), (17,12), (18,1), (18,18).

**374.** а)  $(0, \alpha^5)$ ,  $(\alpha^2, 0)$ ,  $(\alpha^2, \alpha^2)$ ,  $(\alpha^3, 1)$ ,  $(\alpha^3, \alpha)$ ; б)  $(0, \alpha^2)$ ,  $(1, \alpha)$ ,  $(1, \alpha^3)$ ,  $(\alpha^2, 1)$ ,  $(\alpha^2, \alpha^6)$ ,  $(\alpha^4, \alpha)$ ,  $(\alpha^4, \alpha^2)$ ,  $(\alpha^5, \alpha^2)$ ,  $(\alpha^5, \alpha^3)$ ; в)  $(0, 1)$ ,  $(\alpha, \alpha^2)$ ,  $(\alpha, \alpha^4)$ ,  $(\alpha^2, 1)$ ,  $(\alpha^2, \alpha^6)$ ,  $(\alpha^3, \alpha^2)$ ,  $(\alpha^3, \alpha^5)$ ,  $(\alpha^4, 0)$ ,  $(\alpha^4, \alpha^4)$ ,  $(\alpha^5, 1)$ ,  $(\alpha^5, \alpha^4)$ ,  $(\alpha^6, \alpha^1)$ ,  $(\alpha^6, \alpha^5)$ .

**375.** а) нет; б) да; в) да; г) нет; д) нет; е) да.

**379.** Решение можно найти в книге: *Кнэпп Э. Эллиптические кривые*. М.: Факториал Пресс, 2004.

**380.** а)  $2P = (4, 2)$ ;  $2P = (2, 4)$ ;  $2P = (0, 4)$ ; б)  $2P = (3, 0)$ ;  $2P = (1, 8)$ ;  $2P = (7, 2)$ ; в)  $2P = (5, 14)$ ;  $2P = (13, 17)$ ;  $2P = (13, 17)$ .

**381.** а)  $(0, 4)$ ;  $(0, 4)$ ;  $(0, 1)$ ;  $(0, 4)$ ; б)  $(2, 9)$ ;  $(1, 8)$ ;  $(2, 2)$ ;  $\mathcal{O}$ ; в)  $(17, 2)$ ;  $(7, 3)$ ;  $\mathcal{O}$ ;  $(17, 7)$ .

**382.** а)  $2P = \mathcal{O}$ ,  $2P = (1, \alpha^2)$ ,  $2P = (1, \alpha)$ ; б)  $2P = (\alpha^3, 1)$ ,  $2P = (\alpha^6, \alpha^3)$ ,  $2P = (\alpha^3, 1)$ ; в)  $2P = (\alpha^9, \alpha^3)$ ,  $2P = (\alpha^{11}, \alpha^{10})$ ,  $2P = (\alpha^7, \alpha^3)$ .

**383.** а)  $(\alpha, 1)$ ,  $\mathcal{O}$ ,  $(\alpha^2, 1)$ ,  $(1, \alpha)$ ; б)  $(\alpha^3, 1)$ ,  $(\alpha^4, \alpha^5)$ ,  $(\alpha^6, \alpha^4)$ ,  $(\alpha^4, 1)$ ; в)  $(\alpha^7, \alpha^4)$ ,  $(\alpha^{11}, \alpha^{10})$ ,  $\mathcal{O}$ ,  $(\alpha^2, \alpha^{10})$ .

**385.**  $N = 5$ .

**386.** а) 11; б)  $Q_A = (\alpha^6, \alpha^4)$ ; в)  $K_{AC} = (\alpha^3, \alpha^{10})$  и  $K_{A3} = (\alpha^9, \alpha^4)$ .

**387.** а) сообщение: АВТОДРОМ, ключ  $x_k = (11101)$ ; б)  $k_\Gamma = 11$  и  $k_C = 5$ .

**389.** а)  $C_1 = (0, 1)$  и  $C_2 = (\alpha^5, \alpha^2)$ ; б)  $Q_A = (\alpha, 0)$ ; в)  $M = (\alpha^5, \alpha^3)$ .

**390.** а) открытый ключ: кривая  $E$ , точка  $P = (11, 11)$ , точка  $Q_{By} = (14, 14)$ ; секретный ключ:  $k_{By} = 14$ ; б)  $N = 13$ .

**391.** а)  $Q_{KB} = (2, 26)$ ; б)  $M^1 = (0, 2)$ ,  $M^2 = (4, 24)$ ,  $M^3 = (22, 11)$ ,  $M^4 = (40, 32)$ .

## Криптоанализ асимметричных систем

**392.** а)  $2^3 \cdot 11 \cdot 17$ ; б) простое; в)  $2 \cdot 3 \cdot 7 \cdot 13 \cdot 19$ ; г)  $2^2 \cdot 5 \cdot 7 \cdot 13 \cdot 23$ ; д)  $3^3 \cdot 17^2 \cdot 53$ ; е)  $2^2 \cdot 73^2 \cdot 109$ .

**395.** а)  $13 \cdot 19$ ; б)  $29 \cdot 61$ ; в)  $7 \cdot 31 \cdot 47$ ; г)  $3 \cdot 7^2 \cdot 13^2$ ; д) к чётному числу метод не применим; е)  $1009 \cdot 1013$ .

**396.** а)  $p = 17, q = 19$ ; б)  $p = 227, q = 277$ ; в)  $p = 1117, q = 1171$ ; г)  $p = 3301, q = 3391$ .

**397.** а) 28; б) 170; в) 513; г) 530.

**399. Указание.** Используйте теорему Ферма, см. задачу 286.

**400.** а)  $n = 311 \cdot 13$ ; б)  $n = 433 \cdot 19$  в)  $n = 1009 \cdot 29$  г)  $n = 421 \cdot 1283$ ; г)  $n = 997 \cdot 1123$ ; е)  $n = 1237 \cdot 2237$ ;

**401.** а)  $p = 15\ 401, q = 46\ 691, b = 11$ ; б)  $p = 135\ 979, q = 115\ 979, b = 180$ .

**404.** а)  $x = 7$ ; б)  $x = 14$ ; в)  $x = 43$ ; г)  $x = 23$ ; д)  $x = 31$ ; е)  $x = 11$ .

**405.** а)  $x = 21$ ; б)  $x = 43$ ; в)  $x = 61$ ; г)  $x = 100$ ; д)  $x = 53$ ; е)  $x = 11$ .

**406.** а)  $n = 23 \cdot 31$  б)  $n = 107 \cdot 109$  в)  $n = 2447 \cdot 3449$  г)  $n = 198491317 \cdot 373587883$ .

**407.** а)  $n = 23 \cdot 167$  б)  $n = 19 \cdot 211$  в)  $n = 197 \cdot 107$  г)  $n = 601 \cdot 877$ .

**408.** а)  $m = 30$ ; б)  $m = 111$ ; в)  $m = 17$ ; г)  $m = 1900$ .

**409.** а)  $m = 64$ ; б)  $m = 192$ ; в)  $m = 1234$ ; г)  $m = 1000$ .

**410.** а)  $d = 5, p = 137, q = 599$  б)  $d = 569, p = 1234577, q = 7654337$ .

**411.** а)  $d = 3$  б)  $d = 37$  в)  $d = 769$ .

## Теория секре́тности Шеннона

**412.** Доказательство вытекает из того, что  $D(\cdot, \cdot)$  — функция.

**413.** Переформулировка задачи 412.

**415.**  $p(x|y) = p(y|x) = 1/5$ , если  $(x, y) \in \{(0, 2), (1, 0), (2, 1)\}$ ; иначе  $p(x|y) = p(y|x) = 2/5$ .

**419.** При  $n = m$ .

**421.** При ненулевых  $a, b$ , таких что  $b$  и  $n$  взаимно просты.

**422.** а) да; б) нет; в) да; г) да; д) нет.

**429.** Поскольку  $H(Y) \leq \log_2 |Y|$  и  $H(Z|Y) = H(X) + H(Z) - H(Y)$ , то  $H(Z|Y) = H(X) + H(Z) - H(Y) = H(Z) + \log_2 |X| - D_X - H(Y) \geq H(Z) - D_X$ , откуда получаем требуемое.

**430.** Нет, неверно.

**431.** Нет, неверно.

**432.** При  $p(x) = 1/2$  и  $p(z) \neq 1/2$  система строго идеальна, но не совершенно секретна. При  $p(x) \neq 1/2$  и  $p(z) = 1/2$  система совершенно секретна, но не строго идеальна.

**438.** Решение можно найти в книге [1].

**439.** Вытекает из задачи 438 при подстановке  $s(\ell) = 0$ .

**440.** а) 26; б) 2 для английского и русского языков; в)  $\lceil 4n/3 \rceil$ ; г)  $\infty$ .

## Анализ псевдослучайных последовательностей

**448.** 12.

**449.** Да.

**452. Указание.** Воспользуйтесь тем, что каждый элемент последовательности зависит только от значений предыдущих  $\ell_u$  элементов.

**460.** а)  $x^{n+1} + 1$ ; б)  $x^2 + 1$ ; в)  $x^4 + x + 1$ ; г)  $x^4 + x + 1$ .

**461.** а)  $x^8 + x^7 + x^6 + x^4 + 1$ ; б)  $x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$ ; в)  $x^8 + x^6 + x^5 + x^4 + 1$ ; г)  $x^8 + x^6 + x^5 + x^3 + x^2$ ; д)  $x^7 + x^6 + x^3 + 1$ .

**462.**  $x^2 \oplus x \oplus 1$ . Детали решения:

| $n$ | $u_n$ | $m$ | $a$ | $b$ | $G_n$  | $\deg G_n$ |
|-----|-------|-----|-----|-----|--|------------|
| 0   | 0     | —   | —   | —   | 1  | 0          |
| 1   | 1     | —   | —   | —   | $x^2 \oplus 1$                                     | 2          |
| 2   | 1     | 1   | 1   | 0   | $x^2 \oplus 1 \oplus x(1) = x^2 \oplus x \oplus 1$ | 2          |
| 3   | 0     | —   | —   | —   | $x^2 \oplus x \oplus 1$                            | 2          |
| 4   | 1     | —   | —   | —   | $x^2 \oplus x \oplus 1$                            | 2          |
| 5   | 1     | —   | —   | —   | $x^2 \oplus x \oplus 1$                            | 2          |

**463.**  $x^4 \oplus 1$ . Детали решения:

| $n$ | $u_n$ | $m$ | $a$ | $b$ | $G_n$  | $\deg G_n$ |
|-----|-------|-----|-----|-----|--|------------|
| -1  | -     | -   | -   | -   | 1  | 0          |
| 0   | 1     | -   | -   | -   | $x \oplus 1$   | 1          |
| 1   | 0     | 0   | 0   | 0   | $x \oplus 1 \oplus 1 = x$  | 1          |
| 2   | 1     | 0   | 0   | 1   | $x(x) \oplus 1 = x^2 \oplus 1$   | 2          |
| 3   | 1     | 2   | 1   | 1   | $x^2 \oplus 1 \oplus 1(x) = x^2 \oplus x \oplus 1$                       | 2          |
| 4   | 1     | 2   | 1   | 2   | $x(x^2 \oplus x \oplus 1) \oplus x = x^3 \oplus x^2$                     | 3          |
| 5   | 0     | 4   | 2   | 2   | $x^3 \oplus x^2 \oplus 1(x^2 \oplus x \oplus 1) = x^3 \oplus x \oplus 1$ | 3          |
| 6   | 1     | 4   | 2   | 3   | $x(x^3 \oplus x \oplus 1) \oplus x^2 \oplus x \oplus 1 = x^4 \oplus 1$   | 4          |
| 7   | 1     | -   | -   | -   | $x^4 \oplus 1$   | 4          |

464. а)  $x^3 + x^2 + x$ ; б)  $x^5 + x$ ; в)  $x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3$ ;  
г)  $x^{12} + x^3$ .

465. Во всех пунктах ответ:  $x^7 + x^5 + 1$ .

## Булевы функции

471.  $2^n$ .

472.  $C_n^k$ .

473.  $n2^{n-1}$ ;  $C_n^k 2^{n-1}$ .

474.  $C_{n/2}^k C_{n/2}^\ell$ .

475. две единицы:  $\sum_{k=0}^{\lceil n/2 \rceil} C_{n-k+1}^k$  или рекурсивная формула  $C_{n+1} = C_n + C_{n-1}$ , при  $C_0 = 1, C_1 = 2$ ;

три единицы:  $\sum_{k=0}^{\lfloor 2/3 \rfloor + (n \bmod 3)} \sum_{i=0}^k (C_{n-k+1}^i + C_{n-k+1-i}^{(k-i)/2})$  или рекурсивная формула  $A_{n+1} = A_n + A_{n-1} + A_{n-2}$ , при  $A_0 = 1, A_1 = 2, A_2 = 4$ .

476.  $C_n^r; \sum_{i=0}^r C_n^i$ .

477. а)  $2^m$ ; б)  $C_m^{\frac{k+m-r}{2}} C_{n-m}^{\frac{k-m+r}{2}}$ ; в)  $\sum_{i=0}^k C_m^{\frac{i+m-r}{2}} C_{n-m}^{\frac{i-m+r}{2}}$ ;

г)  $\sum_{i=0}^k \sum_{j=r}^n C_m^{\frac{i+m-j}{2}} C_{n-m}^{\frac{i-m+j}{2}}$ .

Считаем в ответах б), в), г), что при  $a$  нецелом  $C_n^a$  равно нулю.

478. Если  $x = 0$ , то  $2^n$  и 0 соответственно; если  $x \neq 0$ , то  $2^{n-1}$  и  $2^{n-1}$ .

479.  $2^k$ .

480.  $2^{n-k}$ .

481.  $C_n^k 2^{n-k}; 3^n$ .

482.  $C_n^k; C_{n-\ell}^{n-k}$ .

486. 168;  $\prod_{i=0}^{k-1} (2^k - 2^i)$ .

487.  $\frac{\prod_{i=0}^{k-1} (2^{n-i}-1)}{\prod_{i=1}^k (2^i - 1)}$

**490.**  $2^{2^n}$ .

**495.** а)  $1 \oplus x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_2x_3$ ; б)  $1 \oplus x_2$ ; в)  $1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3$ .

**496.** а)  $x_1 \oplus x_2 \oplus 1$ ; б)  $x_1x_2 \oplus 1$ ; в)  $x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$ ; г)  $x_1 \oplus x_2 \oplus x_3$ ; д)  $x_1x_2x_3$ ; е)  $x_1x_2x_3 \oplus x_1x_3 \oplus 1$ .

**499.** а) 0; б)  $2^n$ ; в)  $2^{n-1}$ ; г)  $2^{n-1}$ ; д)  $2^{n-2}$ ; е)  $2^{n-2}$ ; ж)  $2^{n-k}$ ; з)  $2^n - w$ .

**500.** 0,  $2^{n-1}$ ,  $2^n$ .

**501.** Да.

**503.** 2; 3; 0; 4.

**504.**  $2^n$  (линейных);  $2^{n+1}$  (аффинных);  $2^s$ , где  $s = \sum_{i=0}^k C_n^i$  (функций, степень которых не превосходит  $k$ ).

**509.** а) 1; б) 0; в)  $x_2 \oplus 1$ .

**510.** Нет.

**512.**  $\sum_{i=0}^n (-1)^i \cdot C_n^i \cdot 2^{2^{n-i}}$ ; 1.

**514.** а)  $(2, 2, 2, -2)$ ; б)  $(2, -6, -2, -2, -2, -2, 2, 2)$ ; в)  $W_f(a) = (-1)^{a_0} 2^n$ , остальные коэффициенты равны 0.

**516.**  $2^{n/2}$ .

**519.** а) да; б) нет; в) нет; г) да; д) нет; е) нет.

**521. Указание.** Воспользуйтесь формулой для вычисления преобразования Мёбиуса для  $f$  и равенством из задачи 520, рассмотрев в качестве  $S$  множество векторов  $\{y \mid y \preceq a\}$ .

**522. Указание.** Воспользуйтесь результатом задачи 521.

**523.** а)  $x_1x_2 \oplus x_1$ ; б) Не существует; в)  $x_1, x_2 \oplus x_1 \oplus x_2 \oplus 1$ .

**527.** Следует из определений.

**528.** Следует из определений. Нет, неверно.

**530.** Следует из определений. Нет, неверно.

**531.** Следует из определений.

**533.** Следует из определений. Нет, неверно.

**534.**  $n!; 2^n; n! \cdot 2^n$ .

**538.** а) да, перестановка: (134) — в циклическом представлении; б) да, перестановка: (24); в) нет; г) нет; д) нет.

**539.**  $2^{n+1}$ . Поясковая функция определяется произвольным двоичным вектором  $(b_0, b_1, \dots, b_n)$  как  $f(x) = b_k$ , если  $wt(x) = k$ .

**540.** а) нет; б) нет; в) нет; г) эквивалентно относительно  $GL_3$ .

**541.** Да.

**542.** Два класса. Представители: 0,  $x_1x_2$ .

**543.** Решение можно найти в книгах [17], [19]. Оно опирается на теорему Диксона.

**544.** Несложно следует из задачи 543.

**545.** а) верно, кроме случая аффинной эквивалентности; б) верно; в) верно только для  $S_n$  и  $GL_n(2)$ ; г) верно.

**546.**  $n = 3$ :  $C(0) = \{0\}$ ,  $C(1) = \{1, 2, 4\}$ ,  $C(3) = \{3, 6, 5\}$ ;  $n = 4$ :  $C(0) = \{0\}$ ,  $C(1) = \{1, 2, 4, 8\}$ ,  $C(3) = \{3, 6, 12, 9\}$ ,  $C(5) = \{5, 10\}$ ,  $C(7) = \{7, 14, 13, 11\}$ ;  $n = 5$ :  $C(0) = \{0\}$ ,  $C(1) = \{1, 2, 4, 8, 16\}$ ,  $C(3) = \{3, 6, 12, 24\}$ ,  $C(5) = \{5, 10, 20, 9, 18\}$ ,  $C(7) = \{7, 14, 28, 25, 19\}$ ,  $C(11) = \{11, 22, 13, 26, 21\}$ ,  $C(15) = \{15, 30, 29, 27, 23\}$ .

**547. Указание.** а) Используйте задачу 262; б) Воспользуйтесь свойством следа, см. задачу 326.

**548. Указание.** Используйте свойство б) задачи 547. Подробное решение приводится в пособии [33].

**549.** Нет. Рассмотрите, к примеру, тождественно равную константе функцию.

**550. Указание.** Воспользуйтесь свойством линейности следа, см. задачу 325.

**551.** Решение можно найти в книге [42].

**554.** а) 0; б)  $x_2 \oplus x_3$  в)  $1 \oplus x_1 \oplus x_2$ ; г)  $x_2 \oplus x_1x_2$ ; д)  $1 \oplus x_1 \oplus x_3 \oplus x_2x_3$ .

**555.** а)  $tr(\alpha)$ ; б)  $tr(\alpha^4c)$ ; в)  $tr(\alpha) + tr(\alpha^4c) + tr(c^3)$ ; г)  $tr(\alpha^3c) + tr(\alpha^2c^3) + tr(\alpha c^7)$ ; д)  $tr(c^7)$ . Отметим, что во всех пунктах приведённый ответ может быть не единственным в силу задачи 549.

## Криптографические свойства булевых функций

**556.** При  $n = 1$  по две функции. При  $n = 2$  имеется 6 сбалансированных, 10 несбалансированных.

**557.**  $C_{2^n}^{2^{n-1}}$ .

**562.** а) да; б) нет; в) да; г) нет; д) да; е) нет.

**563.** б) порядок 0 имеют  $f(x) = x$ ,  $f(x) = x \oplus 1$ ; порядок 1 имеют  $f(x) = 0$ ,  $f(x) = 1$ .

**564.** Функции  $f_7, f_{10}$  имеют порядок устойчивости 1, остальные — 0. Справедливо  $CI(f_1) = CI(f_{16}) = 2$ ,  $CI(f_7) = CI(f_{10}) = 1$ , остальные имеют порядок 0. АНФ:  $f_1(x_1, x_2) = 0$ ,  $f_7(x_1, x_2) = x_1 \oplus x_2$ ,  $f_{10}(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ ,  $f_{16}(x_1, x_2) = 1$ .

**565.** Совпадают.

**568. Указание.** Используйте тождество Саркара, см. задачу 526.

**Решение. Необходимость.** Обозначим  $S_y = \sum_{x \in \mathbb{Z}_2^n, x \leq y} W_f(x)$ , где  $y$  — некоторый вектор. Для  $S_y$  справедливо тождество Саркара:

$$S_y = \sum_{x \in \mathbb{Z}_2^n, x \leq y} W_f(x) = 2^n - 2^{wt(y)+1} wt(f^y),$$

где  $f^y$  — подфункция  $f$ , полученная фиксацией значения 0 для всех переменных, которые в векторе  $y$  равны 1.

Пусть  $f$  — корреляционно-иммунная порядка  $r$  и  $1 \leq wt(y) \leq r$ . Индукцией по  $wt(y)$  покажем, что  $W_f(y) = 0$ .

База. Если  $wt(y) = 1$ , то  $S_y = W_f(0) + W_f(y)$ . С другой стороны, по тождеству Саркара  $S_y = 2^n - 2^{1+1}wt(f^y) = 2^n - 2^2wt(f)/2^1 = 2^n - 2wt(f) = W_f(0)$ . Из полученных двух равенств заключаем, что  $W_f(y) = 0$ .

Шаг. Пусть  $wt(y) = k$ ,  $1 < k \leq r$ . По предположению  $W_f(z) = 0$  для всех  $z$ ,  $1 \leq wt(z) < k$ . Тогда для  $S_y$  выполнено:  $S_y = W_f(0) + W_f(y)$ . С другой стороны, вновь воспользуемся тождеством Саркара:

$$S_y = 2^n - 2^{k+1}wt(f^y) = 2^n - 2^{k+1}wt(f)/2^k = 2^n - 2wt(f) = W_f(0).$$

Таким образом,  $W_f(y) = 0$ , т. е. доказали необходимость.

**Достаточность.** Для любых чисел  $k$  и  $\ell$ ,  $0 \leq \ell \leq k \leq r$ , обозначим через  $F_{k,\ell}$  множество всех подфункций, которые получаются из  $f$  подстановкой вместо  $k$  переменных констант, среди которых  $\ell$  единиц и  $k - \ell$  нулей.

Пусть для всех  $y$ ,  $1 \leq wt(y) \leq r$ , верно, что  $W_f(y) = 0$ . Тогда для любого  $z$ ,  $wt(z) \leq r$ , выполнено:  $S_z = W_f(0) = 2^n - 2wt(f)$ . Тогда из тождества Саркара получаем, что  $wt(f^z) = wt(f)/2^{wt(z)}$ .

Поскольку  $F_{k,0} = \{f^z \mid z \in \mathbb{Z}_2^n, wt(z) = k\}$ , то тем самым доказано, что  $wt(f') = wt(f)/2^k$  для всех  $k = 0, 1, \dots, r$  и любой  $f' \in F_{k,0}$ .

Далее, проведем индукцию по  $\ell$ . Для  $\ell = 0$  доказано. Шаг. Предположим, что  $wt(f') = wt(f)/2^{r-1}$  и  $wt(f'_1) = wt(f)/2^r$  для любых  $f' \in F_{r-1,\ell}$  и  $f'_1 \in F_{r,\ell}$  и некоторого  $\ell$ ,  $0 \leq \ell < r$ . Покажем, что  $wt(f'') = wt(f)/2^r$  для любой функции  $f'' \in F_{r,\ell+1}$ . Для любой  $f'' \in F_{r,\ell+1}$  найдутся  $f' \in F_{r-1,\ell}$ ,  $f'_1 \in F_{r,\ell}$  и переменная  $x_i$  такие, что  $f' = x_i f'' \oplus (x_i \oplus 1) f'_1$ . По предположению индукции  $wt(f') = wt(f)/2^{r-1}$  и

$wt(f'_1) = wt(f)/2^r$ . Нетрудно убедиться, что  $wt(f') = wt(f'') + wt(f'_1)$ . Следовательно,

$$wt(f'') = wt(f)/2^{r-1} - wt(f)/2^r = wt(f)/2^r.$$

Таким образом, доказали, что вес любой  $f' \in F_{r,\ell}$  равен  $wt(f)/2^\ell$  для всех  $\ell \leq r$ . Следовательно, рассмотрев все подфункции  $f'$  функции  $f$ , полученные любой фиксацией  $r$  произвольных переменных, доказали, что  $f$  — корреляционно-иммунная порядка  $r$ .

**570.** Решение можно найти в книге [1].

**571.** Решение можно найти в книге [1].

**572.** Решение можно найти в работе: *Fon-Der-Flaass D. G. A bound on correlation immunity // Siberian Elektron. Mat. Izv. 2007, № 4. P. 133–135.*

**575.** а) любая булева функция от  $n$  переменных; б)  $f(x_1, \dots, x_n) = 0$ ; в) 0,  $x_1 \oplus 1$ ,  $x_1x_2 \oplus x_2$ ,  $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ ; г) 0,  $x_1 \oplus 1$ ,  $x_2 \oplus 1$ ,  $x_1 \oplus x_2$ ,  $x_1x_2 \oplus 1$ ,  $x_1x_2 \oplus x_1$ ,  $x_1x_2 \oplus x_2$ ,  $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ .

**576.** а) 256; б) 128; в) 128; г) 64; д) 16; е) 4; ж) 2; з) 1.

**578.**  $2^{2^n - wt(f)}$ .

**579.** 1, аннулятор —  $\ell_{a,a_0}$ .

**580.** д) решение можно найти в пособии [24].

**581.** а) 1; б) 2; в) 0; г) 0; д) 1; е) если  $n = 2$ , то  $AI(f) = 1$ , иначе  $AI(f) = 2$ .

**582. Указание.** Рассмотрите множество  $A = \{1, x_1, x_2, \dots, x_1x_2, \dots\}$  всех мономов с числом переменных не более  $n/2$  и мультимножество  $B = \{f(x), f(x) \cdot x_1, f(x) \cdot x_2, \dots, f(x) \cdot x_1x_2, \dots\}$ , полученное домножением  $f$  на мономы из  $A$ . Далее докажите, что существует нетрииальный линейное соотношение между элементами из  $A \cup B$ .

**586.** а) 0; б) 1; в) 2; г) 1.

**589. Указание.** Используйте задачи 516 и 588.

**590.** а) да; б) да; в) нет.

**596. Указание.** Воспользуйтесь результатом задачи 521 и определением дуальной функции к бент-функции (см. задачу 597).

**598. Указание.** Воспользуйтесь результатом задачи 521 и определением дуальной функции к бент-функции (см. задачу 597).

**602.** В каждом случае — нет.

**604.** Решение можно найти в книге [1].

**606.** Следствие задач 573 и 604.

**605.** Решение можно найти в книге [1].

**607.** Решение можно найти в работе: *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискрет. матем., 2006, Т. 18, № 3, С. 152–159.

## Векторные булевые функции

**608.** Типа  $3 \rightarrow 2$  больше.

**609.**  $2^{m \cdot 2^n}$ .

**610.** существуют только при  $n = m$ ; количество —  $2^n!$ .

**611.** а)  $(100) \oplus (011)x_1$ ; б)  $(0000) \oplus (0011)x_1 \oplus (1111)x_2 \oplus (1000)x_1x_2$ ;  
в)  $(010) \oplus (110)x_1 \oplus (001)x_3$ ; г)  $(111) \oplus (100)x_1 \oplus (111)x_2 \oplus (011)x_3 \oplus (010)x_1x_2 \oplus (101)x_1x_3 \oplus (001)x_2x_3$ .

**615. Указание.** Используйте равенство из задачи 614.

**616. Решение.** Проведем цепочку преобразований:

$$\begin{aligned} & \sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m} (W_F(u, v))^4 = \\ & \sum_{x, y, z, t \in \mathbb{Z}_2^n} \left( \sum_{v \in \mathbb{Z}_2^m} (-1)^{\langle v, F(x) \oplus F(y) \oplus F(z) \oplus F(t) \rangle} \right) \left( \sum_{u \in \mathbb{Z}_2^n} (-1)^{\langle u, x \oplus y \oplus z \oplus t \rangle} \right) = \\ & 2^{n+m} |\{(x, y, z, t) : \begin{cases} x \oplus y \oplus z \oplus t = 0 \\ F(x) \oplus F(y) \oplus F(z) \oplus F(t) = 0 \end{cases}\}| = \\ & 2^{n+m} |\{(x, y, z) : F(x) \oplus F(y) \oplus F(z) \oplus F(x+y+z) = 0\}| \geqslant \\ & 2^{n+m} |\{(x, y, z) : x = y \text{ или } x = z \text{ или } y = z\}|. \end{aligned}$$

Подсчитаем количество элементов последнего множества:

$$|\{(x, y, z) : x = y \text{ или } x = z \text{ или } y = z\}| =$$

$$3 \cdot |\{(x, x, y) : x, y \in \mathbb{Z}_2^n\}| - 2 \cdot |\{(x, x, x) : x \in \mathbb{Z}_2^n\}| = 3 \cdot 2^{2n} - 2 \cdot 2^n.$$

**618. а) 2; б) 1.**

**620.**  $2^{n-1} - 2^{n/2-1}$ , все компонентные функции — бент-функции.

**622. Указание.** Используйте равенство из задачи 614 и дуальные функции к компонентным булевым функциям.

**623. Решение.** Так как нелинейность функции вычисляется по формуле

$$N_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} |W_F(u, v)|,$$

то нужно найти оценку на коэффициенты Уолша — Адамара.

Очевидно, что

$$\max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^2 \geq \frac{\sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^4}{\sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^2}$$

Оценим значение числителя дроби. Используя задачу 616 и исключив случай  $v = 0$ , получаем оценку:

$$\sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^4 \geq 2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n) - 2^{4n}.$$

Оценим теперь значение знаменателя:

$$\sum_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^2 = \sum_{v \in \mathbb{Z}_2^m, v \neq 0} 2^{2n} = 2^{2n}(2^m - 1).$$

Первый переход осуществили, используя равенство Парсеваля.

Получаем итоговую оценку:

$$\begin{aligned} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2^m, v \neq 0} (W_F(u, v))^2 &\geq \frac{2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n) - 2^{4n}}{(2^m - 1)2^{2n}} = \\ &= 3 \cdot 2^n - 2 - 2 \frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}. \end{aligned}$$

Извлекаем квадратный корень и подставляем минимальное значение максимума модуля коэффициентов Уолша — Адамара в выражение для нелинейности и получаем итоговую оценку:

$$N_F \leq 2^{n-1} - \frac{1}{2} \sqrt{3 \cdot 2^n - 2 - 2 \frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}}.$$

**625.** а) каждая — АВ-функция; б) нет, АВ-функции существуют только при нечётном  $n$ ; в) да; г) нет; д) да.

**626. Указание.** Воспользуйтесь результатом задачи 522.

**627.** а) нет; б) да; в) да; г) нет.

**628.** а) 4; б) 2; в) 2; г) 6; д) 4.

**632.** а) каждая — APN-функция; б) да; в) нет; г) да; д) да.

**633. Решение.** Напомним, что АНФ векторной функции  $F$  это представление в виде:

$$F(x_1, \dots, x_n) = \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \dots x_{i_k} \oplus a_0,$$

где  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$  и  $a_{i_1, \dots, i_k}, a_0 \in \mathbb{Z}_2^m$ .

Сопоставим набору  $\{i_1, \dots, i_k\}$  вектор  $I$ , у которого единицы стоят только на местах с номерами  $i_1, \dots, i_k$ . Соответствующий вектор  $a_{i_1, \dots, i_k}$  обозначим через  $a_I$ . Нетрудно убедиться, что справедлива следующая формула вычисления коэффициента  $a_I$  по значениям функции  $F$ :

$$a_I = \bigoplus_{x \in \mathbb{Z}_2^n, x \leq I} F(x).$$

Мы хотим определить коэффициенты  $a_I$ , где  $wt(I) = 2$ . Без ограничения общности считаем, что  $I = (1, 1, 0, \dots, 0)$ , т. е. мы ищем коэффициент при слагаемом  $x_1 x_2$ . Распишем его:

$$\begin{aligned} a_I &= \bigoplus_{x \in \mathbb{Z}_2^n, x \leq I} F(x) = F(0, 0, 0, \dots, 0) \oplus F(0, 1, 0, \dots, 0) \oplus \\ &\quad F(1, 0, 0, \dots, 0) \oplus F(1, 1, 0, \dots, 0). \end{aligned}$$

По определению, APN-функцией является функция, для которой уравнение  $F(x) \oplus F(x \oplus a) = b$  имеет не более двух решений для любых  $a \neq 0, b$ . Это означает, что для всех  $a \neq 0$  и для всех  $x$  и  $y$  таких, что  $x \neq y, x \neq y \oplus a$ , выполнено  $F(x \oplus a) \oplus F(x) \oplus F(y \oplus a) \oplus F(y) \neq 0$ .

Следовательно, если в полученном выражении для  $a_I$  положим  $a = (0, 1, 0, \dots, 0)$ ,  $x = (0, 0, 0, \dots, 0)$ ,  $y = (1, 0, 0, \dots, 0)$ , тогда так как  $F$  по условию APN-функция, то  $a_I \neq 0$ . Аналогично доказывается для всех остальных векторов  $I$  веса 2.

**634. Указание.** Сравните задачи 627 и 640.

**635.** Детали классификации можно найти в работе: *M. Brinkmann, G. Leander On the classification of APN functions to dimension five // Des. Codes Cryptogr. (2008) 49, P. 273–288.*

**636.** Данная функция была представлена в презентации: *Dillon J. F. APN polynomials: an update // Fq9, The 9th International Conference on Finite Fields and Appl. Dublin, Ireland, 2009.*

**641.** Следует из определения.

**642.** а) да; б) да.

**644.** Могут быть разными.

**645. Указание.** Используйте задачи 638(а) и 641.

**646.** Следует из решения задачи 645.

**647. Указание.** Используйте задачи 600 и 639.

**648.** а) аналогично задаче 645; б) рассмотрите нелинейности аффинно эквивалентных функций и функций  $F$  и  $F^{-1}$ .

**649. Указание.** Рассмотрите решение более сложной задачи 650.

**650. Решение.** Разобъём доказательство на три пункта.

*Представимость.* Можем представить функцию  $F$  в виде полинома:

$$F(x, y) = \sum_{a \in GF(2^n)} \sum_{b \in GF(2^n)} F(a, b)(1 + (x + a)^{2^n - 1})(1 + (y + b)^{2^n - 1}).$$

Действительно, возьмем  $x = a, y = b$ , тогда

$$F(a, b)(1 + (x + a)^{2^n - 1})(1 + (y + b)^{2^n - 1}) = F(a, b).$$

В остальных случаях (если  $x \neq a$  и/или  $y \neq b$ ) это слагаемое равно нулю.

*Степень.* Пусть  $\{\alpha_1, \dots, \alpha_n\}$  — базис  $GF(2^n)$  как векторного пространства над  $GF(2)$ . Тогда любой элемент  $x \in GF(2^n)$  можем представить в виде:  $x = \sum_{i=1}^n x_i \alpha_i$ , где  $x_i \in \{0, 1\}$ . Так как любое число  $j \in \{0, \dots, 2^n - 1\}$  можно представить в двоичной системе счисления:  $j = \sum_{s=0}^{n-1} j_s 2^s$ , где  $j_s \in \{0, 1\}$ , то функция  $F$  будет выглядеть следующим образом:

$$\begin{aligned} F(x, y) &= \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \delta_{ij} \left( \sum_{i=1}^n x_i \alpha_i \right)^{\sum_{v=0}^{n-1} i_v 2^v} \left( \sum_{i=1}^n y_i \alpha_i \right)^{\sum_{s=0}^{n-1} j_s 2^s} = \\ &= \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \delta_{ij} \prod_{v=0: i_v \neq 0}^{n-1} \left( \sum_{i=1}^n x_i \alpha_i^{2^v} \right) \prod_{s=0: i_s \neq 0}^{n-1} \left( \sum_{i=1}^n y_i \alpha_i^{2^s} \right). \end{aligned}$$

Последнее равенство получается из задачи 321.

Отсюда  $\deg(F) \leq \max_{i,j: \delta_{ij} \neq 0} \{wt(i) + wt(j)\}$ . В действительности, степень всегда равна этой приведённой верхней границе, так как число  $2^{\sum_{i=0}^d \binom{n}{i}}$  всех функций степени, не превышающей  $d$ , совпадает с числом полиномов  $\sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \delta_{ij} x^i y^j$  таких, что  $\max_{i,j=0,\dots,2^n-1: \delta_{ij} \neq 0} \{wt(i) + wt(j)\} \leq d$  для любых  $d$ .

*Однозначность.* В предыдущем пункте показано, что число полиномов и число функций совпадает. Поскольку каждой функции соответствует полином, заключаем, что представление однозначное.

**651.**  $L(x) = \sum_{k=0}^{n-1} a_k x^{2^k}$ ;  $A(x) = a + L(x)$ , где  $a, a_0, \dots, a_{n-1} \in GF(2^n)$ .

**653.** а) – 4); б) – 8); в) – 6); г) – 1); д) – 7); е) – 2); ж) – 10); з) – 5); и) – 3); к) – 9).

## Криптоанализ симметричных шифров

**654.** А ответа здесь нет! В качестве **указания** рекомендуем обратиться к рассказам А. П. Чехова 1894–1897 гг.

**655.** Ниже приведена заполненная расширенная таблица. Обратите внимание на совпадающие открытые тексты и шифртексты.

|    | Открытый текст   | Шифртекст        | Ключ             |
|----|------------------|------------------|------------------|
| 1  | 0123456789abcde7 | c95744256a5ed31d | 0123456789abcdef |
| 2  | eff0e8e2e5f2ece8 | a688301a8a4b5655 | 68656c6c6f776f72 |
| 3  | a688301a8a4b5655 | ed70bc5f05110e50 | 68656c6c6f776f72 |
| 4  | 1bd58d519dab10e9 | f3f0eee1eef0eef1 | fefefefefefefefe |
| 5  | f3f0eee1eef0eef1 | 1bd58d519dab10e9 | fefefefefefefefe |
| 6  | f3f0eee1eef0eef1 | fcc4264e6971562d | 1f1f1f1f0e0e0e0e |
| 7  | fcc4264e6971562d | f3f0eee1eef0eef1 | 1f1f1f1f0e0e0e0e |
| 8  | f3f0eee1eef0eef1 | 1b4acf1c0ee11f84 | e0e0e0e0f1f1f1f1 |
| 9  | 1b4acf1c0ee11f84 | f3f0eee1eef0eef1 | e0e0e0e0f1f1f1f1 |
| 10 | f3f0eee1eef0eef1 | 571bb1e06a86b944 | 0101010101010101 |
| 11 | 571bb1e06a86b944 | f3f0eee1eef0eef1 | 0101010101010101 |
| 12 | f3f0eee1eef0eef1 | 3596522dbc5b1ae9 | f3f0eee1eef0eef1 |

|    | Открытый текст    | Шифртекст        | Ключ                   |
|----|-------------------|------------------|------------------------|
| 13 | 3596522dbc5b1ae9  | d8efedb6d0d4423d | f3f0eee1eef0eef1       |
| 14 | e7ece5fff1e5e1ff  | 47deb08e5e15741f | f3f0eee1eef0eef1       |
| 15 | eaebbe0e2e8e0f2f3 | 0ba3dd24c394072a | ec ee ed e8 f2 eef0 e0 |

**660.** Вероятность линейного приближения первого S-блока имеет наибольшее отклонение от 1/2. Лучшие приближения S-блоков:

| S-блок | Приближение             | Преобладание |
|--------|-------------------------|--------------|
| $S_1$  | $b \cdot x = 3 \cdot y$ | +7           |
| $S_2$  | $b \cdot x = 1 \cdot y$ | -6           |
| $S_3$  | $e \cdot x = 1 \cdot y$ | -5           |
|        | $f \cdot x = 3 \cdot y$ | +5           |

**680.** а) (0000 0000); б) (1111 1111); в) (1101 0001); г) (1000 0000); д) (0101 0101); е) (0011 1000); ж) (1000 0001); з) (1111 0000).

**681.** а) несовместна; б) совместна, решения (000), (101); в) несовместна; г) совместна, решения (0001), (0110), (1111); д) совместна, решение (1000); е) совместна, решения (1010 1010), (0101 0101); ж) несовместна.

**682.** а) (1011); б) (0110), (1011), (1101); в) (01100101); г) (0000), (0100), (0010), (0001); (0110), (0011); д) (0011), (1000), (1001).

**683.**  $K = (011)$ .

**684.** а)  $K = (101101)$ ; б)  $K = (100010)$  и  $K = (101000)$ ; в)  $K = (001000)$  и  $K = (001101)$ .

**685.** а) можно,  $K = (0011)$ ; б) информацию извлечь нельзя; в) можно,  $K = (0011)$ ; г) можно сказать, что ключ имеет один из следующих видов  $K = (*01*)$ ,  $K = (01 * 1)$ ,  $K = (11 * 0)$ .

**686.** а)  $K = (100)$  и  $P = (101\ 001\ 111)$ ;  $K = (110)$  и  $P = (111\ 011\ 101)$ ; б)  $K = (100)$  и  $P = (101\ 001\ 111)$ ;  $K = (011)$  и  $P = (010\ 110\ 000)$ ; в)  $K = (101)$  и  $P = (100\ 000\ 110)$ ; г)  $K = (010)$  и  $P = (011\ 111\ 001)$ ; д)  $K = (110)$  и  $P = (111\ 011\ 101)$ ; е)  $K = (001)$  и  $P = (000\ 100\ 010)$ .

**687.** а) (001111); б) (111011).

## Трудные и нерешённые математические задачи

**696.**  $n/2$ .

**702.** Рекомендуем найти решение в [41].

**706.** Решение приводится в статье: Токарева Н. Н. Группа автоморфизмов множества бент-функций // Дискретная математика. 2010. Т. 22. № 4. С. 34–42.

**707.** Решение приводится в статье, указанной в ответе к задаче 706.

**710. Решение.** Воспользуйтесь тем, что граф  $G_f$  регулярный. Поскольку вес произвольной бент-функции равен  $2^{n-1} \pm 2^{\frac{n}{2}-1}$ , значение  $k = |\text{supp}(f)|$  сразу определяется.

Для доказательства сильной регулярности и равенства  $\lambda = \mu$  можно проделать следующее. Пусть  $x, y$  — произвольные различные вершины графа. Тогда число общих смежных им вершин  $z$  равно  $|\text{supp}(f_x) \cap \text{supp}(f_y)|$ , где  $f_x$  обозначает функцию, заданную равенством  $f_x(z) = f(x + z)$ . Пусть  $M = \text{supp}(f)$ . Заметим, что  $\text{supp}(f_x) = M + x$ . Из этого равенства несложно следует, что

$$|\text{supp}(f_x) \cap \text{supp}(f_y)| = |(M + x) \cap (M + y)| = |M \cap (M + x + y)|.$$

Обозначим  $u = x + y$  и определим значение  $|\text{supp}(f) \cap \text{supp}(f_u)|$ .

Из формулы для мощности симметрической разности двух множеств несложно получить равенство  $|\text{supp}(f + f_u)| = 2|\text{supp}(f)| - 2|\text{supp}(f) \cap \text{supp}(f_u)|$ . Воспользуемся теперь тем, что  $|\text{supp}(f)| = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ , а также тем, что производная  $D_u f$  бент-функции  $f$  по любому ненулевому направлению  $u$  уравновешена, т. е.  $|\text{supp}(f + f_u)| = 2^{n-1}$ . Тогда получаем  $|\text{supp}(f) \cap \text{supp}(f_u)| = 2^{n-2} \pm 2^{\frac{n}{2}-1}$ .

Таким образом, величина  $|\text{supp}(f) \cap \text{supp}(f_u)|$  не зависит от выбора вектора  $u$ , ее точное значение найдено. Напомним, что эта величина равна числу общих смежных вершин для  $x$  и  $y$ .

**711. Решение.** Уравновешенность функции  $D_u f$  для любого ненулевого вектора  $u$  следует из равенств  $|\text{supp}(f + f_u)| = 2|\text{supp}(f)| - 2|\text{supp}(f) \cap \text{supp}(f_u)| = 2k - 2\lambda = 2^{n-1}$ .

**712. Решение.** Известно (см. например, статью Cameron P. Strongly regular graphs. University of London. Preprint. 2001. 23 p.), что для любого сильно регулярного графа с параметрами  $(v, k, \lambda, \mu)$  выполняются условия:

$$k(k - \lambda - 1) = (v - k - 1)\mu; \quad (16.1)$$

$$\text{числа } \frac{1}{2} \left( v - 1 \pm \frac{(v - 1)(\mu - \lambda) - 2k}{\sqrt{(\mu - \lambda)^2 + 4(k - \mu)}} \right) \text{ целые.} \quad (16.2)$$

Подставим  $v = 2^n$ ,  $\lambda = \mu$  в уравнение (16.1). Тогда оно примет вид

$$k(k-1) = \lambda(2^n - 1), \quad (16.3)$$

а условие (16.2) будет означать, что числа  $\frac{1}{2}(2^n - 1 \pm \frac{k}{\sqrt{k-\lambda}})$  целые. Тогда  $k - \lambda = a^2$  для некоторого целого  $a$ ,  $a > 0$ . Подставляя это выражение в (16.3), приходим к уравнению

$$k^2 - 2^n k + a^2(2^n - 1) = 0. \quad (16.4)$$

При решении его относительно  $k$  возникает дискриминант  $D = 2^{2n} - 4a^2(2^n - 1)$ , который, как нетрудно заметить, должен быть квадратом некоторого четного положительного числа, скажем, числа  $2b$ . Найдем все возможные решения уравнения

$$b^2 + a^2(2^n - 1) = 2^{2n-2} \quad (16.5)$$

в целых числах  $a > 0, b > 0$ . Заметим, что из (16.5) вытекает неравенство

$$\max\{a, b\} < 2^{n-1}. \quad (16.6)$$

Рассматривая (16.5) по модулю  $2^n$ , получаем, что  $(b-a)(b+a) = 0 \pmod{2^n}$ . Возможны три случая.

Случай 1. Пусть  $(b+a) = 0 \pmod{2^n}$ . Заметим, что  $b+a \neq 0$ , так как  $a, b$  положительные. Тогда  $b+a \geq 2^n$ , что противоречит неравенству (16.6). Следовательно, в этом случае целых решений (16.5) нет.

Случай 2. Пусть  $(b-a) = 0 \pmod{2^n}$ . Заметим, что если  $b-a = q \cdot 2^n$  при некотором целом  $q \neq 0$ , то  $\max\{a, b\} > 2^n$ , что вновь противоречит неравенству (16.6). Следовательно,  $a = b$ . Согласно (16.5) имеем  $a^2 \cdot 2^n = 2^{2n-2}$ . Таким образом,  $a = b = 2^{(n/2)-1}$ . Решая уравнение (16.4), находим  $k = 2^{n-1} \pm 2^{(n/2)-1}$ ,  $\lambda = 2^{n-2} \pm 2^{(n/2)-1}$ , что соответствует искомым параметрам из утверждения 1.

Случай 3. Пусть  $b+a = s \cdot 2^\ell$ ,  $b-a = t \cdot 2^r$ , где  $s, t$  — нечетные,  $s \geq 1$ ,  $t \neq 0$ ; целые числа  $\ell, r$  такие, что  $0 < \ell < n$ ,  $0 < r < n$ , а также  $\ell+r \geq n$ . Подставляя выражения для  $b^2 - a^2$  и  $a^2$  в (16.5), получаем:  $st \cdot 2^{\ell+r} = 2^{2n-2} - 2^n(s^2 \cdot 2^{2\ell-2} + t^2 \cdot 2^{2r-2} - st \cdot 2^{\ell+r-1})$ , откуда следует

$$st = 2^{2n-\ell-r-2} - s^2 \cdot 2^{n+\ell-r-2} - t^2 \cdot 2^{n-\ell+r-2} + st \cdot 2^{n-1}. \quad (16.7)$$

Поскольку в левой части равенства стоит нечетное число, равенство возможно только, если в правой части хотя бы один показатель при степени двойки равен нулю. Рассмотрим эти возможности.

Подслучай 3.1. Если  $\frac{2n - \ell - r - 2}{2} = 0$ , то  $\ell = r = n - 1$ . Подставляя эти значения в (16.7), получаем  $st = 1 - 2^{n-2}(s^2 + t^2) + st \cdot 2^{n-1}$ . Так как  $s^2 + t^2$  — четное число, то  $st = 1 \pmod{2^{n-1}}$ . Другими словами,  $st = 1 + q \cdot 2^{n-1}$  при некотором целом  $q$ . Тогда  $b^2 - a^2 = (1 + q \cdot 2^{n-1})2^{2n-2}$  и подставляя это выражение в (16.5), имеем  $a^2 + q \cdot 2^{2n-3} = 0$ . Заметим, что при  $q \geq 0$  это равенство противоречит тому, что  $a > 0$ . Но при  $q < 0$  получаем противоречие с неравенством  $a^2 < 2^n$ , которое несложно следует из (16.5). Следовательно, данный подслучай не реализуется.

Подслучай 3.2. Если  $n + \ell - r - 2 = 0$ , то, как нетрудно заметить,  $\ell = 1, r = n - 1$ . Тогда  $b - a = t \cdot 2^{n-1}$  и следовательно,  $\max\{a, b\} > 2^{n-1}$ , что противоречит (16.6).

Подслучай 3.3. Если  $n - \ell + r - 2 = 0$ , то  $r = 1, \ell = n - 1$ . Из неравенства (16.6) вытекает, что  $a + b < 2^n$ , и так как  $a + b = s \cdot 2^{n-1}$  при нечетном  $s$ , то  $s = 1$ . Подставляя известные параметры в (16.7), приходим к уравнению  $t^2 - (2^{n-1} - 1)t + (2^{2n-4} - 2^{n-2}) = 0$ , решая которое находим возможные значения для  $t$ : либо  $t = 2^{n-2}$ , либо  $t = 2^{n-2} - 1$ . Однако значение  $t = 2^{n-2}$  не реализуется, так как тогда  $a$  должно быть равно нулю. Значит,  $t = 2^{n-2} - 1$  и следовательно,  $a = 1, b = 2^{n-1} - 1$ . Решая уравнение (16.4) при таких значениях  $a, b$ , получаем  $k = 2^n - 1$  (что соответствует полному графу, а график  $G$  по условию не такой), либо  $k = 1$  (что соответствует полному паросочетанию на  $2^n$  вершинах, но график  $G$  снова не такой, поскольку  $\lambda > 0$ ). Следовательно, в случае 3 нет подходящих решений (16.5) в целых положительных числах. Таким образом, параметры графа были определены в случае 2 и они имеют искомый вид.



**714. Указание.** Воспользуйтесь определением.

**715. Указание.** Непосредственно следует из задачи 710.

**716. Указание.** Непосредственно следует из задач 710, 712.

## Задачи на программирование

**740.** В задачах главы о криптоанализе симметричных шифров также есть что декодировать. Заполненная таблица приведена ниже.

|    |                              |  |
|----|------------------------------|--|
| 1  | Hello World!                 | 48656c6c6f20576f726c6421                                     |
| 2  | Привет Мир!                  | cff0e8e2e5f220cce8f021                                       |
| 3  | учебное пособие              | f3f7e5e1edeee520effeef1eee1e8e5                              |
| 4  | алгоритмы шифрования         | e0ebe3eef0e8f2ecfb20f8e8f4f0eee2<br>e0ede8ff                 |
| 5  | Симметричная криптография    | d1e8ecece5f2f0e8f7ede0ff20eaf0e8<br>eff2eee3f0e0f4e8ff       |
| 6  | Краткий курс                 | caf0e0f2eae8e920eaf3f0f1                                     |
| 7  | Ну зяц, ну погоди!           | cdf320e7e0fff62c20edf320effee3ee<br>e4e821                   |
| 8  | Сборник задач по             | d1e1eef0ede8ea20e7e0e4e0f720effe                             |
| 9  | криптографии и криптоанализу | eaf0e8eff2eee3f0e0f4e8e820e820ea<br>f0e8eff2eee0ede0ebe8e7f3 |
| 10 | cp1251 синоним windows-1251  | 63703132353120f1e8edeede8ec2077<br>696e646f77732d31323531    |

**741. Указание.** При шифровании используется кодировка cp1251. Каждому символу соответствует один байт (восемь бит), например символу 'п' в кодировке cp1251 соответствует ef.

**742. Указание.** Шифрование происходит как и в задаче 741. Все сообщения осмысленны и состоят преимущественно из букв русского алфавита.

**745. Указание.** При реализации программы вам может помочь задача 653.

## СПИСОК ЛИТЕРАТУРЫ

1. Агibalов Г. П. Избранные теоремы начального курса криптографии: Учебное пособие. Томск: Томский государственный университет, 2005. 116 с.
2. Агibalов Г. П. 50 лет криптографии в Томском государственном университете // Прикл. дискретная математика. 2009. № 2. С. 104–126.
3. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2005. 480 с.
4. Бабаш А. В., Шанкин Г. П. История криптографии. М.: Гелиос АРВ, 2002. Ч. 1. 240 с.
5. Бабаш А. В., Ларин Д. А. История защиты информации в зарубежных странах: Учебное пособие. М.: РИОР; ИНФРА-М, 2013. 283 с.
6. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России: Учебное пособие. М.: КДУ, 2013. 736 с.
7. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. М.: Гелиос АРВ, 2012. 688 с.
8. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.
9. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига/URSS, 2006. 324 с.
10. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига/URSS, 2006. 274 с.

11. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: ФИЗМАТЛИТ, 2005. 416 с.
12. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра: Учебник: В 2 т. М.: Гелиос АРВ, 2003.
13. Глухов М. М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии: Учебное пособие. СПб.: Издательство «Лань», 2011. 400 с.
14. Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008. 288 с.
15. Зубов А. Ю., Зязин А. В., Овчинников В. Н., Рамоданов С. М. Олимпиады по криптографии и математике для школьников. М.: МЦНМО, 2006. 136 с.
16. Kahn D. Взломщики кодов. М.: Центрполиграф, 2000. Перевод книги: Kahn D. The codebreakers, 1967.
17. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
18. Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
19. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 745 с.
20. Mao B. Современная криптография: теория и практика. М.: Издательский дом «Вильямс», 2005. 768 с.
21. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006. 320 с.
22. Нечаев В. И. Элементы криптографии (Основы теории защиты информации) М.: Высш. шк., 1999. 109 с.
23. Панасенко С. П. Алгоритмы шифрования. Специальный спра-  
вочник. СПб.: БХВ-Петербург, 2009. 576 с.

24. Панкратова И. А. Булевы функции в криптографии: Учебное пособие. Томск: Томский гос. ун-т., 2014. 88 с.
25. Пятьдесят лет Институту криптографии, связи и информатики. Исторический очерк / Под ред. Б. А. Погорелова, М., 1999. 272 с.
26. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2010. 232 с.
27. Сачков В. Н. Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004. 424 с.
28. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: АСТ Астрель, 2006. 447 с.
29. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006. 94 с.
30. Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС, 2002. 512 с.
31. Таранников Ю. В. Комбинаторные свойства дискретных структур и приложения в криптологии. М.: МЦНМО, 2011. 152 с.
32. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2011. 170 с.
33. Токарева Н. Н. Симметричная криптография. Краткий курс: Учебное пособие. Новосибирск: НГУ, 2012. 232 с.
34. Фомичёв В. М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
35. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиеевич С. В. Математические и компьютерные основы криптологии: Учебное пособие. Минск: Новое знание, 2003. 382 с.
36. Черёмушкин А. В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.

37. Черёмушкин А. В. Информационная безопасность. Глоссарий / Под ред. С. Пазизина, М.: АВАНГАРД ЦЕНТР, 2013. 322 с. URL: <http://www.glossary.ib-bank.ru/>
38. Ян С. Й. Криптоанализ RSA. М.; Ижевск: Ижевский ин-т компьютерных исследований, 2011. 312 с.
39. Ященко В. В. Введение в криптографию. М.: МЦНМО, 2012. 348 с.
40. Bard G. Algebraic cryptanalysis. Berlin: Springer, 2009. 360 p.
41. Budaghyan L. Construction and Analysis of Cryptographic Functions: Habilitation Thesis. University of Paris 8. Sept. 2013. 192 p.
42. Carlet C. Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / Eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Chapter 8. P. 257–397. URL: [www.math.univ-paris13.fr/~carlet/](http://www.math.univ-paris13.fr/~carlet/)
43. Carlet C. Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / Eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Chapter 9. P. 398–472. URL: [www.math.univ-paris13.fr/~carlet/](http://www.math.univ-paris13.fr/~carlet/)
44. Cusick T. W., Stănică P. Cryptographic Boolean Functions and Applications. USA: Acad. Press. Elsevier, 2009. 245 p.
45. Hankerson D., Menezes A., Vanstone S. Guide to elliptic curve cryptography. Springer-Verlag, 2004. 311 p.
46. Heys H. M. A Tutorial on Linear and Differential Cryptanalysis // Cryptologia. 2002. V. 26. № 3. P. 189–221.
47. Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93: Proc. Berlin: Springer, 1994. P. 386–397. LNCS V. 765.
48. Matsui M. The First Experimental Cryptanalysis of Data Encryption Standard // Advances in Cryptology — CRYPTO'94. Proc. Berlin: Springer, 1994. P. 1–11. LNCS V. 839.

Учебное издание

**Городилова Анастасия Александровна,  
Токарева Наталья Николаевна,  
Шушуев Георгий Иннокентьевич**

**КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ  
Сборник задач**

Учебное пособие

Редактор *H. A. Борзенкова*

Подписано в печать 11.04.2014 г.  
Формат 70×100 1/16. Уч.-изд. л. 20, 3. Усл. печ. л. 26, 2.  
Тираж 400 экз. Заказ № 97

Редакционно-издательский центр НГУ.  
630090, Новосибирск, ул. Пирогова, 2.