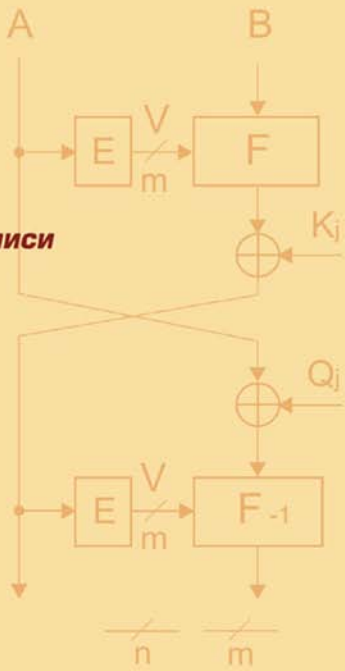
Н. А. Молдовян
А. А. Молдовян

ВВЕДЕНИЕ В КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

- *Проблематика криптографии*
- *Элементы теории чисел*
- *Двухключевые криптосистемы*
- *Системы электронной цифровой подписи с составным модулем*
- *Открытое распределение ключей и открытое шифрование*
- *Управление ключами и протоколы*



УЧЕБНОЕ ПОСОБИЕ

bhv

Н. А. Молдовян, А. А. Молдовян

Введение в криптосистемы с открытым ключом

Санкт-Петербург
«БХВ-Петербург»
2005

Содержание

Введение **7**

Глоссарий **9**

Глава 1. Проблематика криптографии и симметричные шифры **15**

1.1. Проблемы защиты информации в компьютерных системах 15
1.2. Задачи криптографии 17
1.2.1. Обеспечение секретности 17
1.2.2. Современные приложения 24
1.3. Элементы симметричного шифрования 31
1.3.1. Условная и безусловная секретность 31
1.3.2. Общие вопросы разработки шифров 35
1.3.3. Композиционные и итеративные блочные шифры 37
1.3.4. Управляемые операции как криптографический примитив 43
1.4. Особенности проектирования блочных шифров на основе управляемых операций 45
1.4.1. Управляемые операции и отображения 45
1.4.2. Расписание использования ключа 47
1.4.3. Варианты криптосхем 50
1.4.4. Криптосистемы с гибким алгоритмом и требования к алгоритму предвычислений 55
1.5. Вероятностные шифры 57
1.5.1. Гомофонические шифры 57
1.5.2. Шифры с простым вероятностным механизмом 58
1.6. Особенности приложений 60
1.6.1. Длина ключа и стойкость 60
1.6.2. Повышение стойкости шифрования при ограничении длины секретного ключа 63
1.6.3. Применение долговременных ключевых элементов при ограничении длины секретного ключа 64
1.6.4. Варианты реализации шифров 66

Глава 2. Элементы теории чисел 71

2.1. Некоторые определения и утверждения 71
2.2. Функция Эйлера 74
2.3. Алгоритм Евклида 76
2.4. Расширенный алгоритм Евклида 78
2.5. Показатели и первообразные корни 79
2.6. Теоремы о числе классов с заданным показателем 83
2.7. Китайская теорема об остатках 86
2.8. Алгоритм возведения в степень по модулю 88
2.9. Нахождение чисел, относящихся к заданному показателю 90
2.10 Теоремы о числе решений степенных сравнений 92

Глава 3. Двухключевые криптосистемы 99

3.1. Понятие электронной цифровой подписи 99
3.2. Сравнительная характеристика одноключевых и двухключевых шифров 102
3.3. От открытого распределения ключей до электронной цифровой подписи 104
3.3.1 Система распределения ключей Диффи–Хеллмана 104
3.3.2 Открытый шифр Эль-Гамаля 106
3.4. Системы ЭЦП на основе задачи дискретного логарифмирования 107
3.4.1. Общие положения 107
3.4.2. Сокращение длины подписи 113
3.4.3. Примеры анализа слабых ЭЦП 117
3.4.4. Цифровая подпись Эль-Гамаля 120
3.4.5. Системы ЭЦП с дополнительными свойствами 122
3.4.6. Стандарты ЭЦП 127
3.5. Проблема бесключевого шифрования 129
3.6. Криптосистема RSA 136
3.6.1. Криптографические преобразования в RSA 136
3.6.2. Вопросы выбора параметров системы RSA 140
3.6.3. Слепая подпись на основе системы RSA 143

Глава 4. Системы ЭЦП с составным модулем 146

4.1. Цифровая подпись Рабина 146
4.2. Цифровая подпись Фиата–Шамира 148
4.3. Обобщение схемы Фиата–Шамира 150
4.4. Уменьшение размера открытого ключа в схеме Фиата–Шамира 151
4.5. Схема ЭЦП Онга–Шнорра–Шамира 153
4.6. Варианты схемы Эль-Гамаля с составным модулем 154

4.7. Схемы на основе сложности извлечения корней по составному модулю 157
4.8. Расширение криптосистемы RSA 158
4.8.1. Модифицированные версии и совместимость с RSA 159
4.8.2. Ограничения на выбор параметров криптосхемы 162
4.9. Переход к схемам ЭЦП с простым модулем 163
4.9.1. Переход к простому модулю в ЭЦП Фиата–Шамира 163
4.9.2. Сокращение размера подписи 165
4.9.3. Цифровая подпись Шнорра 166

Глава 5. Открытое распределение ключей и открытое шифрование 168

5.1. Схема открытого шифрования Рабина 169
5.2. Схемы на основе сложности задачи извлечения корней по модулю 172
5.2.1. Открытое шифрование 172
5.2.2. Схема с сокращенной длиной открытого ключа 174
5.2.3. Открытое распределение ключей 175
5.2.4. Схема на основе сложности извлечения корней второй степени 178
5.3. Открытое распределение общего ключа между тремя и более пользователями 179
5.4. Вероятностные механизмы в двухключевых шифрах 181

Глава 6. Хэш-функции 184

6.1. Защита от модифицирования данных 184
6.2. Криптографические контрольные суммы 187
6.3. Построение хэш-функций на основе блочных преобразований 190
6.4. Нахождение коллизий в общем случае 196
6.5. Атака «встреча посередине» 201

Глава 7. Управление ключами и протоколы 205

7.1. Вопросы управления ключами 205
7.2. Генерация ключей 209
7.3. Схемы распределения ключей 211
7.3.1. Централизованное распределение ключей 213
7.3.2. Открытое распределение ключей 217
7.3.3. Распределение ключей на основе симметричного шифрования 220
7.3.4. Распределение ключей на основе двухключевых шифров 223
7.4. Разделение секрета 224

7.4.1. Схемы на основе китайской теоремы об остатках 225
7.4.2. Пороговые схемы на основе многочленов 227
7.4.3. Неоднородное ключевое пространство 229
7.5. Криптографические протоколы 230
7.5.1. Понятие криптографического протокола 230
7.5.2. Временной замок 233
7.5.3. Защита материальных объектов от подделки 235
7.5.4. Электронная жеребьевка 235
7.5.5. Игра в покер по телефону (электронное казино) 237
7.6. Понятие слепой подписи 239
7.7. Протоколы с нулевым разглашением 242
7.7.1. Протокол Фиата–Шамира 242
7.7.2. Протоколы на основе системы RSA 244
7.7.3. Протокол с одним раундом проверки 245
7.7.4. Протоколы на основе сложности разложения на множители 247
7.7.5. Протоколы на основе сложности дискретного логарифмирования 249
7.8. Инфраструктура открытых ключей (PKI) 250

Глава 8. Криптографический практикум. 256

8.1. Задания для практических занятий. 256
8.1.1. Открытое распределение ключей 257
8.1.2. Открытое шифрование 259
8.1.3. Схемы ЭЦП 261
8.1.4. Генерация простых чисел 268
8.2. Задачник 275
8.2.1. Арифметические задачи 275
8.2.2. Схемы цифровой подписи 277
8.2.3. Хэш-функции 280

Заключение 282

Список литературы 283

Памяти нашего отца
посвящается

Введение

Криптографические методы нашли широкое применение в практической информатике для решения многочисленных проблем информационной безопасности. В проблематике современной криптографии можно выделить следующие три типа основных задач:

- обеспечение конфиденциальности (секретности);
- обеспечение анонимности (неотслеживаемости);
- обеспечение аутентификации информации и источника сообщений.

Первый тип задач относится к защите информации от несанкционированного доступа с использованием шифрования по секретному ключу. Доступ к информации имеют только обладатели секретного ключа. Такие задачи решаются с помощью одноключевых криптосистем, которые применяются человечеством уже несколько тысячелетий. Второй и третий типы задач обязаны своей постановкой массовому применению электрических способов обработки и передачи информации. Решение задач обеспечения анонимности (при обращении электронных денег или при тайном электронном голосовании) и аутентификации информации связано с открытием двухключевой криптографии, сделанным около 30 лет назад. С того момента проблематика двухключевой криптографии является наиболее интенсивно развивающимся направлением современной криптографии. Появившееся новое направление криптографии востребовало широкого применения теории чисел, комбинаторики, теории сложности, дискретной математики и других ее разделов. Предоставленная двухключевой криптографией возможность эффективного решения новых типов задач привела к возникновению и широкому практическому использованию новых информационных технологий, дающих существенную экономическую отдачу. В последнее время широко обсуждается проблема электронного правительства, под которым понимается максимальное использование компьютерной техники и электронного документооборота по реализации управленческих функций правительства. Основой придания юридической значимости электронной информации, циркулирующей в информацион-

ных системах в банковской сфере, управленческой деятельности правительства и других государственных органов, включая вооруженные силы и спецслужбы, является двухключевая криптография, обеспечивающая эффективные решения по обеспечению аутентификации и неотслеживаемости. Использование криптографии в современных информационных системах позволяет достигнуть не только максимальной оперативности в финансовой, деловой и управленческой деятельности, но и создать практически непреодолимые преграды для многих противоправных и антиобщественных действий преступных элементов, включая решение проблемы фальсификации денег и ценных бумаг.

В настоящее время имеется достаточно обширная русскоязычная литература по всем разделам криптографии, однако сохраняется потребность в учебных пособиях, в которых детально рассматриваются механизмы построения систем электронной цифровой подписи (ЭЦП) и вопросы обоснования выбора параметров ЭЦП в их взаимосвязи с рассмотренными математическими результатами и методическим материалом для выполнения практических заданий.

Предлагаемая вниманию читателей книга рассматривает в основном вопросы построения шифров с открытым ключом, включая системы ЭЦП и слепой подписи. Симметричные криптосистемы характеризуются достаточно кратко, а именно в плане изложения основных сведений. Дается математический минимум для освоения и полного понимания основных систем ЭЦП и идей, лежащих в их основе. Раскрываются криптографические и организационные основы придания юридической силы электронным документам. Книга ориентирована на использование при преподавании дисциплин «Криптографические методы защиты информации», «Теоретические основы криптографии», «Теоретические основы компьютерной безопасности» и «Криптография» в рамках подготовки специалистов по следующим вузовским специальностям: «Компьютерная безопасность», «Организация и технология защиты информации», «Комплексное обеспечение информационной безопасности автоматизированных систем», «Автоматизированные системы обработки информации и управления», «Прикладная математика».

Глоссарий

Алгоритм защитного контрольного суммирования — алгоритм вычисления некоторого двоичного вектора сравнительно малого размера, зависящего от каждого бита сообщения произвольной длины. Важнейшим типом алгоритмов защитного контрольного суммирования являются хэш-функции.

Аппаратный шифр — шифр, ориентированный на реализацию в виде электронного устройства.

Аутентификация — процедура установления подлинности пользователя (абонента сети, отправителя сообщения), программы, устройства или данных (информации, получаемого сообщения, ключа). Частным вариантом аутентификации является установление принадлежности сообщения конкретному автору.

Блочный шифр — шифр, входными текстами для которого являются блоки фиксированного размера.

Вероятностное шифрование — процесс шифрования с использованием случайных параметров.

Гибкий шифр — шифр, описываемый как набор криптоалгоритмов, выбираемых в зависимости от секретного ключа.

Гибридная криптосистема — криптосистема, в которой распределение ключей осуществляется с помощью двухключевых криптоалгоритмов, а процесс шифрования информации — с помощью одноключевых. Гибридные криптосистемы сочетают в себе удобство распределения секретных ключей и высокую скорость шифрования.

Двухключевая криптография — направление исследований в области криптографии и разработки криптосистем, основанных на использовании двух ключей — открытого и закрытого. Открытый (публичный, общедоступный) ключ предполагается известным всем пользователям криптосистемы и потенциальному противнику. Закрытый ключ предполагается известным только одному пользователю. Существенным является то, что для реализации различных протоколов в двухключевых криптосистемах не требуется, чтобы секретный ключ был известен более чем одному поль-

зователю. Это позволяет реализовать криптографические протоколы, предусматривающие взаимодействие сторон в условиях недоверия друг другу. Двухключевые криптосистемы лежат в основе современных систем электронной цифровой подписи.

Зашифрование — процесс преобразования информации с целью предотвращения несанкционированного доступа. Зашифрование преобразует исходный открытый текст в шифртекст (или криптограмму). Шифртекст называют иногда шифрованным текстом. Зашифрование есть процесс преобразования данных, обеспечивающий защиту информации путем сокрытия ее смысла. Стойкость зашифрования (или уровень защищенности) определяется тем, что при зашифровании используется один или несколько секретных параметров, которые предполагаются известными только законным (легальным) пользователям.

Ключ — секретный параметр, управляющий ходом шифрования. Ключ определяет выбор конкретного варианта преобразования для зашифрования и расшифрования из множества преобразований, составляющих шифр. Синонимами являются секретный ключ, ключ шифрования.

Криптоанализ — процесс (алгоритм) получения исходного текста по шифрованному без знания ключа или процесс вычисления ключа по исходному и шифрованному тексту. Криптоанализ выполняется противником с целью получения возможности осуществления несанкционированного доступа или разработчиком с целью получения оценки стойкости шифра.

Криптографическое преобразование — процедура специального преобразования информации для решения одной из следующих криптографических задач: шифрования данных, формирования электронной цифровой подписи, вычисления специальных криптографических контрольных сумм и имитовставки.

Криптографический примитив — в широком смысле это операция или процедура, используемая в качестве элемента шифра, в узком — это операции и процедуры, которые определяют требуемые свойства криптосистемы (стойкость, возможность зашифрования и расшифрования с использованием различных ключей и т. п.).

Криптографический протокол — протокол, предусматривающий взаимодействие двух и более сторон с использованием криптографических алгоритмов.

Криптосистема — система обеспечения безопасности защищенной сети, использующая криптографические средства. В качестве подсистем может включать системы шифрования, идентификации, цифровой подписи и др., а также систему распределения ключей.

Криптосистема с закрытым (секретным) ключом — традиционная криптосистема, использующая секретный ключ, известный более чем одному пользователю.

Криптостойкость (*стойкость шифра*) — способность криптосистемы противостоять атакам противника, направленным на получение ключа, открытого сообщения или навязывание ложного сообщения. Количественно выражается числом операций некоторого типа, которые необходимо выполнить для решения задачи криптоанализа. При этом указывается тип атаки на криптосистему, т. е. исходные данные для криптоанализа. Если исходные данные не указываются, то подразумевается стойкость к лучшему известному алгоритму криптоанализа (для атаки на основе специально подобранных текстов).

Лобовое нападение (силовая атака) — криптоанализ путем исчерпывающего перебора всех возможных ключей, т. е. методом подбора ключа. Для криптосистем с конечным ключом этот метод является универсальным, т. е. он применим к любому шифру такого типа. Однако вероятность раскрытия ключа с помощью метода опробования всех возможных ключей является весьма низкой. Для задания низкой вероятности успеха такой атаки для симметричных криптосистем требуется использовать ключи размером не менее 80 бит. В настоящее время считается, что гарантированную стойкость к лобовому нападению обеспечивают равновероятно генерируемые случайные ключи размером 128 бит.

Перестановочная сеть — управляемая перестановочная сеть, состоящая из некоторого числа активных каскадов (активных слоев), между которыми расположены узлы фиксированной коммутации (фиксированные перестановки), причем каждый активный каскад состоит из совокупности управляемых элементарных переключателей, управляемых некоторым управляющим битом и выполняющих тождественное преобразование или перестановку двух битов в зависимости от значения управляющего бита.

Подстановочно-перестановочная сеть — узел преобразования, состоящий из некоторого числа каскадов (слоев), между которыми расположены узлы фиксированной коммутации (перестановки), причем каждый каскад состоит из совокупности блоков подстановки (обычно одного размера).

Поточный шифр — шифр, последовательно преобразующий отдельные биты или знаки исходного текста.

Противник — субъект (специальная программа, оснащенная группа специалистов или физическое лицо), пытающийся преобразовать шифртекст в открытый текст без знания ключа или вычислить ключ по известным исходным и шифрованным текстам. Синонимами являются термины атакующий, нападающий, криптоаналитик, криптоаналитик противника.

Предвычисления — процедуры преобразований или вычисления, выполняемые предварительно и используемые в дальнейшем при многократном выполнении некоторого алгоритма.

Программный шифр — шифр, ориентированный на реализацию в виде программы.

Простое расписание использования ключа — расписание использования ключа, при котором подключи, входящие в шифрующие преобразования, представляют собой битовые цепочки, являющиеся частью секретного ключа. Представляет собой вариант отказа от сложных процедур преобразования секретного ключа. Применяется с целью уменьшения сложности схемотехнической реализации шифров и увеличения производительности криптосистем.

Протокол рукопожатия — протокол, позволяющий двум удаленным сторонам, владеющим некоторым общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета.

Разделение секрета — распределение некоторых долей секретного ключа между несколькими хранителями секрета таким образом, что любой из них или коалиция из малого их числа не могут восстановить секретный ключ. При этом восстановление ключа становится возможным, если численность коалиции хранителей секрета будет равна или превысит некоторое пороговое значение.

Расшифрование — процесс восстановления открытого текста по шифрованному тексту и известному ключу. (Отметим, что вместо термина «расшифрование» иногда используется термин «дешифрование». В российской специальной литературе под термином «дешифрование» обычно понимают процесс восстановления открытого текста без знания ключа или вычисление ключа по открытым текстам и шифртекстам.)

Раскрытие шифра (криптосистемы, криптоалгоритма) — нахождение способа решения задачи криптоанализа за разумное время при использовании современных вычислительных средств. В качестве синонима используется термин «взлом шифра».

Режим шифрования — вариант осуществления криптографического преобразования информации (зашифрование и расшифрование) или вариант использования шифра. Например, блочные шифры могут быть использованы в режиме электронной кодовой книги, режиме сцепления блоков шифра, режиме выработки ключевой гаммы.

Симметричная криптосистема — криптосистема с закрытым ключом. Симметричность означает, что ключи, задающие пару взаимно обратных

криптографических преобразований, могут быть получены один из другого с небольшой трудоемкостью.

Система тайного электронного голосования — криптографический протокол, обеспечивающий тайну голосования и возможность проверки каждым голосующим, как учтен его голос («за» или «против»). При этом никто, включая избирательный комитет, не сможет установить, как проголосовал избиратель.

Слепая подпись — протокол формирования электронной цифровой подписи, позволяющий сформировать правильную ЭЦП, соответствующую некоторому цифровому сообщению, которое подписывающая сторона получает в зашифрованном (т. е. недоступном для нее) виде. Принципиальным требованием к системам слепой подписи является *анонимность* правильной подписи. Подписывающий не должен иметь возможности однозначно установить связь между правильной подписью и какой-либо информацией, которую он получал в процессе подписывания «вслепую», если он подписал таким способом два или более сообщения.

Удостоверяющий центр — организация, осуществляющая регистрацию, хранение и распространение открытых ключей в двухключевых криптосистемах. Основным назначением удостоверяющего центра является аутентификация открытых ключей пользователей. Для распространения открытых ключей используются 1) электронные справочники открытых ключей и 2) цифровые сертификаты. Справочники и сертификаты подписываются удостоверяющим центром.

Управление ключами — совокупность мероприятий и процедур, обеспечивающих защищенную генерацию, распределение, хранение и уничтожение ключей.

Уравнение вычисления подписи — уравнение, задающее определенное соотношение между секретным ключом, значением хэш-функции от документа и цифровой подписью. Служит для формирования электронной цифровой подписи, подлинность которой может быть проверена с использованием открытого ключа.

Уравнение проверки подписи — уравнение, задающее определенное соотношение между открытым ключом, хэш-функцией документа и цифровой подписью. Служит для проверки подлинности подписи.

Хэширование — процесс вычисления значения хэш-функции.

Хэш-функция — криптографическая функция (процедура, алгоритм), аргументом которой являются произвольные сообщения (тексты, документы), представленные в виде последовательности битов, и значения которой лежат в области от 0 до $2^m - 1$, где m — размер хэш-кода (выходного зна-

чения хэш-функции). Хэш-функции представляют собой специальный класс криптографических контрольных сумм, обычно вычисляемых без использования секретных параметров и обеспечивающих сложную зависимость выходного значения от каждого бита входного сообщения.

Целостность информации — характеристика соответствия информации ее эталонному состоянию. Нарушение целостности информации есть ее несанкционированное модифицирование (умышленное или неумышленное).

Цифровой сертификат — электронный документ, содержащий информацию о владельце сертификата (ФИО, должность, организация, адрес, срок действия, открытый ключ и др.) и подписанный доверительным центром.

Цифровая подпись — электронная цифровая подпись.

Шифр с открытым ключом (двухключевой шифр) — двухключевая криптосистема. Синонимами являются термины «шифр (криптосистема) с публичным (открытым) ключом», «асимметричная криптосистема».

Шифр (криптосистема) — совокупность алгоритмов, используемых при зашифровании и расшифровании.

Шифрование — процесс преобразования информации с использованием некоторой дополнительной информации, управляющей этим процессом и называемой ключом. Реализуется в виде процедуры расшифрования или зашифрования. Часто под шифрованием понимается зашифрование.

Шифратор — электронное устройство или программа, реализующая алгоритмы шифрования.

Электронная цифровая подпись — некоторая дополнительная информация, соответствующая данному электронному документу (сообщению), которая могла быть сформирована только владельцем некоторого секрета — закрытого ключа и которая позволяет с использованием специального алгоритма установить факт соответствия подписи закрытому ключу подписывающего. Под электронной цифровой подписью (ЭЦП) понимается также криптографическая система (совокупность алгоритмов и правил), позволяющая подписывать цифровые сообщения и проверять правильность формируемых цифровых подписей.

ГЛАВА 1

Проблематика криптографии и симметричные шифры

1.1. Проблемы защиты информации в компьютерных системах

Криптография, история которой охватывает несколько тысячелетий, зародилась из потребности передачи секретной информации. Длительное время она была связана только с разработкой специальных методов преобразования информации с целью ее представления в форме, недоступной для потенциального злоумышленника. С началом применения электронных способов передачи и обработки информации задачи криптографии начали расширяться. В настоящее время, когда компьютерные информационные технологии нашли массовое применение, проблематика криптографии включает многочисленные задачи, которые не связаны непосредственно с засекречиванием информации. Современные проблемы криптографии включают разработку систем электронной цифровой подписи и тайного электронного голосования, протоколов электронной жеребьевки и аутентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и т. п.

Многие задачи практической информатики эффективно решаются с использованием криптографических методов. В криптографии рассматривается некий злоумышленник (оппонент, криптоаналитик противника, нарушитель, нелегальный пользователь), который осведомлен об используемых криптографических алгоритмах, протоколах, методах и пытается вскрыть их. Вскрытие криптосистемы может заключаться, например, в несанкционированном чтении информации, формировании чужой подписи, изменении результатов голосования, нарушении тайны голосования, модифицировании данных, которое не будет обнаружено законным получателем. Разнообразные действия оппонента в общем случае называются криптографической атакой (нападением). Специфика криптографии состоит в том, что она направлена на разработку методов, обеспечивающих стойкость к любым действиям зло-

умышленника, хотя на момент разработки криптосистемы невозможно предусмотреть все возможные способы атаки, которые могут быть изобретены в будущем на основе новых идей, достижений теории и технологического прогресса. Центральным является вопрос, насколько надежно решается та или иная криптографическая проблема. Ответ на этот вопрос непосредственно связан с оценкой трудоемкости каждой конкретной атаки на криптосистему. Решение такой задачи, как правило, чрезвычайно сложно и составляет самостоятельный предмет исследований, называемый *криптоанализом*. *Криптография и криптоанализ* образуют единую область науки — *криптологию*, которая в настоящее время является разделом математики, имеющим важные приложения в современных информационных технологиях.

Широкое применение компьютерных технологий в системах обработки данных и управления привело к обострению проблемы защиты информации от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жестко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Это создает большое число угроз информации, которые могут быть реализованы как со стороны внешних, так и внутренних нарушителей.

Радикальное решение проблем защиты информации, циркулирующей в высокопроизводительных автоматизированных системах, может быть получено на базе использования криптографических методов. При этом важным является применение скоростных алгоритмов шифрования, которые не приводят к снижению производительности компьютерных и телекоммуникационных систем. Криптографические преобразования данных являются гибким и эффективным средством обеспечения их конфиденциальности, целостности и подлинности. Использование методов криптографии в совокупности с необходимыми техническими и организационными мероприятиями может обеспечить защиту от широкого спектра потенциальных угроз.

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронных данных, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся этой информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи. Теоретическая база для решения этой проблемы появилась после открытия *двухключевой криптографии* американскими исследователями Диффи и Хеллманом в середине 1970-х гг. [22], которое составило блестящее достижение многовекового эволюционного развития криптографии. Революционные идеи двухключевой криптографии привели к резкому росту числа открытых исследований в этой области, показали новые пути развития криптографии, ее

далеко не исчерпанные возможности и уникальное значение в современных условиях бурного развития электронных информационных технологий.

1.2. Задачи криптографии

1.2.1. Обеспечение секретности

Слово «криптография» в переводе с греческого языка означает «тайнопись», что вполне отражает ее первоначальное предназначение. Примитивные с позиций сегодняшнего дня криптографические методы известны с древнейших времен и длительное время рассматривались скорее как некоторые ухищрения, чем как строгая научная дисциплина. Классической задачей криптографии является обеспечение обратимости преобразования некоторого *исходного текста (открытого текста)* в кажущуюся случайной последовательность знаков, называемую *шифртекстом (закрытым текстом)*, или *криптограммой*. При этом шифртекст может содержать как новые знаки, так и уже имеющиеся в исходном сообщении. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является возможность однозначного восстановления исходного текста в полном объеме, используя лишь некоторые логические действия с символами шифртекста. В далекие времена надежность сохранения информации в тайне определялась секретностью самого метода преобразования.

Однако секретность алгоритма принципиально не может обеспечить его *безусловную стойкость*, т. е. невозможность чтения криптограммы противником, обладающим бесконечными вычислительными ресурсами. Поскольку секретные алгоритмы недоступны для проведения широкомасштабных криптоаналитических исследований, то по сравнению с открытыми алгоритмами имеется значительно более высокая вероятность того, что впоследствии будут найдены уязвимые места и эффективные способы их взлома. В связи с этими обстоятельствами в настоящее время наиболее широко используются открытые алгоритмы, прошедшие длительное тестирование и обсуждение в открытой криптографической литературе.

Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации сравнительно малого размера, называемой *секретным ключом*. Ключ используется для управления процессом криптографического преобразования (шифрования) и является легко сменяемым элементом криптосистемы. Ключ может быть заменен пользователями в произвольный момент времени, тогда как сам алгоритм шифрования является долговременным элементом криптосистемы и связан с длительным этапом разработки и тестирования.

При прочих равных условиях отсутствие полных данных об алгоритме шифрования существенно (при адекватной его реализации) затрудняет проведение криптоаналитической атаки. Поэтому были предложены современные шифры, в которых непосредственно действующий алгоритм шифрования является легко сменяемым элементом и выбирается случайно. При этом общая структура криптосистемы открыта для детального обсуждения, что позволяет оценить ее стойкость в целом. Такие шифры реализуются как гибкие криптосистемы, в которых алгоритм, действующий в сеансе шифрования, формируется по специальному *алгоритму инициализации (предвычислений)*. Этот алгоритм является открытым, а сам действующий алгоритм шифрования — неизвестным и зависимым от секретного ключа пользователя.

В течение многих веков криптография была предметом избранных — жрецов, правителей, крупных военачальников и дипломатов. Несмотря на малую распространенность, использование криптографических методов вскрытия шифров противника оказывало существенное воздействие на исход важных исторических событий. Известен не один пример, когда переоценка используемых средств шифрования приводила к военным и дипломатическим поражениям. Несмотря на применение криптографических методов в важных областях, эпизодическое использование криптографии не могло даже близко подвести ее к той роли, которую она имеет в современном обществе. Своим превращением в научную дисциплину криптография обязана потребностям практики и развитию электронных информационных технологий.

Пробуждение значительного интереса к криптографии и ее развитие началось с XIX в., что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относиться к этой дисциплине как к обязательному инструменту своей деятельности.

Говоря об исторических аспектах научных исследований в области криптографии, необходимо отметить тот факт, что весь период с древних времен до 1949 г. можно назвать донаучным периодом, когда средства закрытия письменной информации не имели строгого математического обоснования. Поворотным моментом, придавшим криптографии научность и выделившим ее в отдельное направление математики, явилась публикация в 1949 г. статьи К. Э. Шеннона «Теория связи в секретных системах» [38]. Указанная работа послужила основой для развития *одноключевых симметричных криптосистем*, в которых предполагается обмен секретными ключами между корреспондентами. Впоследствии в силу особенностей построения симметричные шифры были разделены на две криптосистемы: *поточные* и *блочные шифры*. Отличительная особенность первых состоит в преобразовании каждого символа в потоке исходных данных, тогда как вторые осуществляют последовательное преобразование целых блоков данных.

Фундаментальным выводом из работы Шеннона стало определение зависимости надежности алгоритма от размера и качества секретного ключа, а также от *информационной избыточности* исходного текста. Шеннон ввел формальное определение информации и функции ненадежности ключа как его неопределенности при заданном количестве известных битов закрытого текста. Кроме того, им было введено важное понятие *расстояния единственности* как минимального размера текста, на котором еще возможно однозначное раскрытие исходного текста. Было показано, что расстояние единственности прямо пропорционально длине ключа и обратно пропорционально избыточности исходного текста. Следствием работы Шеннона стало доказательство наличия теоретически стойких шифров, как например шифр Вернама.

Наиболее мощным толчком развития криптографии явилась публикация в 1976 г. фундаментальной статьи У. Диффи и М. Е. Хеллмана «Новые направления в криптографии» [22]. В этой работе впервые было показано, что секретность передачи информации может обеспечиваться без обмена секретными ключами. Тем самым была открыта эпоха *двухключевых (асимметричных) криптосистем*, разновидностью которых являются системы электронной цифровой подписи. Данный вид криптосистем называется также шифрами с открытым ключом. Они используются в системах тайного электронного голосования, защиты от навязывания ложных сообщений, электронной жеребьевки, идентификации и аутентификации удаленных пользователей и ряде других систем.

В последние годы на базе совершенствования электронных технологий появились новые теоретические разработки в области *квантовой криптографии* [2], основанной на принципах неопределенности Гейзенберга.

Наряду с развитием криптографических систем совершенствовались и методы, позволяющие восстанавливать исходное сообщение, исходя из шифртекста и другой известной информации, получившие название *криптоанализа*. Успехи криптоанализа приводили к ужесточению требований к криптографическим алгоритмам. Принципиально важным вопросом криптографии всегда была надежность криптосистем. Эта проблема допускала различное трактование на протяжении всей истории криптографии.

Голландский криптограф Керкхофф (1835–1903) впервые сформулировал *правило оценки стойкости шифра*, в соответствии с которым:

1. Весь механизм преобразований считается известным злоумышленнику.
2. Надежность алгоритма должна определяться только неизвестным значением секретного ключа.

Второе требование можно интерпретировать как направленность на разработку таких алгоритмов, для которых оппонент не сможет разработать методы, позволяющие снять защиту или определить истинный ключ за время существенно меньшее, чем время *полного* (*тотального*) *перебора* всего множества возможных секретных ключей.

Принятие оценки стойкости шифра, по Керкхоффу, отражает осознание необходимости испытания криптосхем в условиях, более благоприятных для атаки, по сравнению с условиями, в которых, как правило, может действовать потенциальный нарушитель. Правило Керкхоффа стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нем содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. В настоящее время это правило интерпретируется более широко: *все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику*. В последнюю формулировку криптосистемы входят как частный случай систем защиты. В расширенном понимании правила Керкхоффа предполагается, что все элементы криптосистем защиты подразделяются на две категории — долговременные и легко сменяемые элементы. К *долговременным* относятся те элементы, которые связаны со структурой криптосистем защиты и заменяются только специалистами. К *легко сменяемым* относятся элементы криптосистемы, которые предназначены для частого модифицирования в соответствии с заданным порядком. Легко сменяемыми элементам шифра являются, например, секретный ключ, пароль, идентификатор и т. п. Правило Керкхоффа отражает тот факт, что надлежащий уровень секретности зашифрованной информации должен быть обеспечен только за счет неизвестных легко сменяемых элементов шифра. Действительно, долговременные элементы системы защиты трудно сохранить в тайне, поэтому система должна быть стойкой в случае, когда они являются известными атакующему.

Согласно современным требованиям криптосистемы с секретным ключом, включая шифры с ключом ограниченного размера (128–256 бит), должны быть стойкими к криптоанализу на основе известного алгоритма, большого объема известного открытого текста и соответствующего ему шифртекста. Несмотря на эти общие требования, шифры, используемые специальными службами, сохраняются, как правило, в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности защиты секретной информации, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточно сложную проблему. Чтобы избежать возможных слабостей, алгоритм шифрования может быть построен на основе хорошо изученных и проверенных на практике принципов и способов преобразования. Ни один серь-

езный современный пользователь не будет полагаться только на надежность сохранения в секрете своего алгоритма, поскольку крайне сложно гарантировать то, что информация об алгоритме не станет известной злоумышленнику до окончания срока его использования.

Обоснование надежности используемых систем осуществляется как теоретически, так и экспериментально при моделировании криптоаналитических атак с привлечением группы опытных специалистов, которым предоставляются значительно более благоприятные условия по сравнению с условиями, возникающими на практике в предполагаемых областях применения криптоалгоритма. Например, кроме шифртекста и алгоритма преобразований криптоаналитикам предоставляется исходный текст, шифртексты, полученные из данного открытого текста с помощью различных ключей, и т. п. Оценивается стойкость испытываемой криптосистемы ко всем известным методам криптоанализа и, по возможности, разрабатываются новые подходы к ее вскрытию. Если в этих условиях криптосистема оказывается стойкой, то она рекомендуется для того или иного конкретного применения.

В современном криптоанализе рассматриваются атаки на засекречивающие системы на основе следующих известных данных:

- шифртекста;
- открытого текста и соответствующего ему шифртекста;
- выбранного открытого текста;
- выбранного шифртекста;
- адаптированного открытого текста;
- адаптированного шифртекста.

Кроме того, рассматриваются следующие методы инженерного (технического) криптоанализа, дополнительно использующие:

- преднамеренно генерируемые аппаратные ошибки;
- замеры потребляемой мощности;
- замеры времени вычислений;
- некоторую информацию, перехватываемую по каналу побочных электромагнитных излучений.

Мы детально перечислили типы атак на криптосистемы, предназначенные для шифрования данных с целью защиты от несанкционированного чтения. По отношению к иным видам криптосистем существует ряд других атак, которые будут рассмотрены ниже. А сейчас рассмотрим перечисленные типы атак подробнее.

- В случае *криптоанализа на основе известного шифртекста* считается, что противник знает механизм шифрования и ему доступен только шифртекст. Это соответствует модели внешнего нарушителя, который имеет физический доступ к линии связи, но не имеет доступа к аппаратуре зашифрования и расшифрования.
- При *криптоанализе на основе известного открытого текста* предполагается, что криптоаналитику известен шифртекст и некоторая часть исходного текста, а в частных случаях и соответствие между шифртекстом и исходным текстом. Возможность проведения такой атаки складывается при зашифровании документов, подготовленных с использованием стандартных форм, в условиях, когда определенные блоки данных известны и повторяются. В ряде современных средств защиты компьютерной информации используется режим глобального шифрования, в котором вся информация на встроенном магнитном носителе записывается в виде шифртекста, включая главную корневую запись, загрузочный сектор, системные программы и пр. При хищении такого носителя (или компьютера) легко установить, какая часть криптограммы соответствует стандартной системной информации, и получить большой объем известного исходного текста для выполнения криптоанализа.
- В *нападениях на основе выбранного открытого текста* предполагается, что криптоаналитик противника может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа. Это соответствует модели внутреннего нарушителя. На практике такая ситуация может возникнуть, когда в атаку на шифр вовлекаются лица, которые не знают секретного ключа, но в соответствии со своими служебными полномочиями имеют возможность использовать шифратор для закрытия передаваемых сообщений. Для осуществления такой атаки могут быть использованы также технические работники, готовящие формы документов, электронные бланки и др.
- *Криптоанализ на основе выбранного шифртекста* предполагает, что противник (оппонент) имеет возможность использовать для расшифрования сформированные им самим шифртексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог вычислить секретный ключ шифрования с минимальной трудоемкостью.
- *Атака на основе адаптированных текстов* соответствует случаю, когда атакующий многократно подставляет тексты для зашифрования (или расшифрования), причем каждую новую порцию данных выби-

рает в зависимости от полученного ранее результата преобразования. Этот вид атаки является наиболее благоприятным для нападающего.

В настоящее время к наиболее мощным типам криптоаналитических атак на основе выбранных или адаптированных текстов относится *дифференциальный* (*разностный*) *криптоанализ* [12, 31] и *линейный криптоанализ* [31], а также производные от них методы.

При тестировании новых криптосистем особый интерес представляют нападения на основе известного *секретного* ключа или *расширенного (рабочего)* ключа шифрования. Имеется различие между секретным ключом и расширенным ключом, поскольку секретный ключ не всегда непосредственно используется в преобразованиях шифруемого текста, а часто служит только для выработки расширенного ключа, который и используется в процессе шифрования. Существуют шифры (например блочный шифр ГОСТ 28147–89), в которых секретный ключ непосредственно используется при шифровании данных, т. е. секретный ключ служит и рабочим ключом шифрования. Очевидно, что расширенный ключ является секретным элементом шифра. При проведении криптоанализа на основе известных элементов ключа (секретного или расширенного) предполагается, что криптоаналитик имеет информацию о некоторой части ключа. Чем больше известная доля ключа, при которой шифр оказывается стойким, тем меньше опасений будет вызывать шифр в реальных условиях атаки, когда ключ атакующему неизвестен, но осуществляется попытка восстановить его элементы. При сравнении двух шифров предпочтение можно отдать тому шифру, который имеет лучшие показатели по указанному критерию.

Одним из направлений построения скоростных программных шифров является использование зависимости алгоритма шифрования от секретного ключа. В таких криптосистемах конкретная модификация алгоритма шифрования сменяется одновременно с заменой секретного ключа и атакующему неизвестна. Они называются *недетерминированными* или *гибкими шифрами*. При тестировании гибких шифров представляется разумным проводить анализ их стойкости с использованием атаки на основе *выбранной модификации алгоритма* шифрования. В этом варианте криптоаналитику предоставляется возможность анализировать самую слабую, по его мнению, модификацию из числа потенциально реализуемых вариантов криптоалгоритма. Затем для выбранной модификации проводится криптоанализ на основе специально подобранных текстов, в том числе может рассматриваться и вариант *атаки с частично известным ключом* шифрования. Если не удается найти слабую модификацию криптоалгоритма, то анализируемый гибкий шифр можно признать криптографически стойким.

1.2.2. Современные приложения

Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации процессов передачи и обработки информации и интенсификации информационных потоков криптографические методы приобретают уникальное значение. Новые информационные технологии в своей основе имеют двухключевую криптографию, которая позволяет реализовать протоколы, предполагающие, что секретный ключ известен только одному пользователю, т. е. протоколы, ориентированные на взаимное недоверие взаимодействующих сторон. Отметим основные приложения современной криптографии.

- Защита от несанкционированного чтения (или обеспечение конфиденциальности информации).
- Защита от навязывания ложных сообщений (имитозащита).
- Аутентификация законных пользователей.
- Контроль целостности информации.
- Электронная цифровая подпись.
- Разработка систем тайного электронного голосования.
- Обеспечение хождения электронных денег.
- Проведение электронной жеребьевки.
- Создание электронного казино.
- Построение пороговых схем разделения секрета.
- Защита от отказа по факту приема сообщения.
- Одновременное подписание контракта.
- Защита документов и ценных бумаг от подделки.

Первое направление приложений было раскрыто выше. Кратко поясним некоторые из остальных областей применения криптографии.

Имитозащита — это понятие связано с защитой от навязывания ложных сообщений путем формирования в зависимости от секретного ключа специальной дополнительной информации, называемой *имитовставкой*, которая передается вместе с криптограммой. Дело тут в том, что самого по себе шифрования данных недостаточно для защиты от навязывания ложного сообщения, хотя во многих случаях законный получатель, анализируя семантику сообщения, может легко определить, что криптограмма была модифицирована или подменена, например, при передаче по линии связи. Однако при искажении цифровых данных и в некоторых других случаях обнаружить факт изме-

нения данных по семантике крайне сложно. Одним из способов защиты от навязывания ложного сообщения путем целенаправленного или случайного искажения шифртекста является имитозащита. Для вычисления имитовставки используется алгоритм, задающий зависимость имитовставки от каждого бита сообщения. При этом могут быть использованы следующие два варианта:

- вычисление имитовставки по открытому тексту;
- вычисление имитовставки по шифртексту.

Чем больше длина имитовставки, тем меньше вероятность того, что искажение шифртекста не будет обнаружено санкционированным (законным) получателем. Нарушитель может модифицировать шифртекст, но поскольку он не знает секретного ключа, то не может вычислить новое значение имитовставки, соответствующее модифицированному сообщению. Нарушитель либо не меняет имитовставку, либо подменяет ее на случайное значение. Если используется алгоритм вычисления имитовставки с хорошими криптографическими свойствами, то вероятность того, что факт изменений не будет обнаружен законным получателем, составляет $P = 2^{-n}$, где n — длина имитовставки в битах.

Аутентификация законных пользователей заключается в распознавании пользователей, после чего им предоставляются определенные права доступа к ресурсам вычислительных и автоматизированных информационных систем. Аутентификация основана на том, что законные пользователи обладают некоторой информацией, которая является неизвестной для посторонних. Частным вариантом использования процедуры аутентификации является парольная защита входа в компьютерную систему. Например, пользователь формирует некоторую случайную информацию и, сохраняя ее в секрете, использует как пароль. Пароль в явном виде не хранится в памяти ЭВМ или другого устройства, применяемого для выполнения аутентификации. Это требование направлено на то, чтобы потенциальный внутренний нарушитель не имел возможности считать чужой пароль и присвоить себе полномочия другого пользователя. Для того чтобы система защиты могла идентифицировать легальных (санкционированных) пользователей, в памяти ЭВМ хранятся образы их паролей, вычисленные по специальному криптографическому алгоритму, реализующему так называемую одностороннюю функцию $y = F(x)$. Основное требование к односторонней функции состоит в том, чтобы сложность вычисления значения функции по аргументу была низкой, а сложность определения аргумента по значению функции была высокой (например практически неосуществимой за 10 лет при использовании всех вычислительных ресурсов человечества).

Аутентификация пользователя на рабочей станции может быть осуществлена путем выполнения следующей последовательности шагов:

1. Запрос на ввод идентификатора со стороны системы защиты.
2. Ввод пользователем своего идентификатора (имени) NAME.
3. Запрос на ввод пароля со стороны системы защиты.
4. Ввод пользователем пароля P.
5. Вычисление системой защиты значения односторонней функции y, соответствующего значению аргумента $x = P$.
6. Сравнение системой защиты значения $F(P)$ со значением образа (S) пароля, соответствующего пользователю с идентификатором NAME.

Если $F(P) = S$, то система защиты предоставляет пользователю права доступа (полномочия), соответствующие идентификатору NAME. В противном случае в журнале учета работы пользователей регистрируется событие попытки несанкционированного доступа. Для того чтобы выдать себя за санкционированного пользователя, нарушитель должен ввести правильный пароль. Зная образ S, вычислительно невозможно определить пароль P. Если в системе защиты предусмотрены механизмы противодействия перехвату пароля с помощью программных или аппаратных закладок, а также через побочные электромагнитные излучения и наводки или акустический и оптический каналы, то данный способ аутентификации пользователей обеспечивает высокую надежность защиты от захвата чужих полномочий.

Рассмотренный пример относится к аутентификации пользователей на рабочих станциях, т. е. к задаче защиты входа в ЭВМ. Для взаимной аутентификации удаленных рабочих станций принципиальным является предположение, что потенциальный злоумышленник прослушивает канал связи, а следовательно, описанный выше способ аутентификации неприемлем, поскольку недопустима передача пароля по незащищенному каналу. Аутентификация удаленных рабочих станций может быть выполнена по следующей схеме, основанной на использовании алгоритма шифрования E и общего секретного ключа K для удаленных станций A и B.

1. Станция A посылает запрос на соединение со станцией B.
2. Станция B посылает станции A случайное число R.
3. Станция A зашифровывает R по секретному ключу K, получая шифртекст $C_a = E_K(R)$, и направляет станции B значение C_a.
4. Станция B вычисляет $C_b = E_K(R)$ и сравнивает значения C_b и C_a. Если $C_b = C_a$, то принимается решение, что запрос на установление сеанса связи отправлен станцией A, в противном случае связь прерывается.

Правильно зашифровать случайный текст может только тот, кто знает секретный ключ. Если нарушитель будет перехватывать правильные криптограммы от случайных чисел, то при длине числа R не менее 64 бит он за ра-

зумное время не встретит двух одинаковых чисел, а следовательно, не будет иметь возможности подставить ранее перехваченную правильную криптограмму. В этой схеме роль станции В может играть сервер локальной вычислительной сети. Отметим, что данная схема позволяет станции В удостовериться в том, что связь устанавливается со станцией А. Однако для станции А может существовать аналогичная проблема аутентификации станции В. В этом случае дополнительно осуществляется аналогичная процедура аутентификации, а именно — аутентификация станции В станцией А. Такая схема взаимного распознавания удаленных абонентов (станций) называется *протоколом рукопожатия*.

Контроль целостности информации — это обнаружение любых несанкционированных изменений информации, например, данных или программ, хранимых в компьютере. Имитозащита, в сущности, является важным частным случаем контроля целостности информации, передаваемой в виде шифртекста. В практических приложениях часто требуется удостовериться, что некоторые программы, исходные данные, базы данных не были изменены каким-либо несанкционированным способом, хотя сами данные не являются секретными и хранятся в открытом виде. Контроль целостности информации основан на выработке по некоторому криптографическому закону *кода обнаружения модификаций* (КОМ), имеющего значительно меньший объем, чем охраняемая от модифицирования информация. Основным требованием к алгоритму вычисления КОМ является задание зависимости значения КОМ от каждого бита двоичного представления всех символов исходного текста.

Проверка соответствия информации своему эталонному состоянию (контроль целостности информации) выполняется следующим образом. При фиксации эталонного состояния, например, программного модуля File.exe вычисляется значение КОМ, соответствующее этому файлу. Полученное значение КОМ записывается в таблицу, которая будет использоваться при каждой процедуре проверки целостности информации. Пусть программа File.exe управляет сложным и ответственным технологическим процессом, а ее сбои могут привести к простоям, материальным и финансовым потерям. В таком случае перед каждым запуском программы целесообразно удостовериться в ее целостности. С этой целью каждый раз вычисляется КОМ и сравнивается с соответствующим значением, хранимым в таблице кодов. Этот способ эффективен для обнаружения непреднамеренных искажений данных, которые имеют случайный характер.

При преднамеренном модифицировании информации такая схема контроля целостности данных неприемлема, поскольку злоумышленник может обойти ее следующим образом. Он изменит по своему усмотрению данные, вычислит новое значение КОМ, соответствующее измененным данным, и

внесет его в таблицу кодов взамен эталонного значения КОМ (соответствующего эталонному состоянию данных). Чтобы предотвратить такое нападение, можно дополнительно использовать один из следующих механизмов:

- секретный алгоритм вычисления КОМ;
- алгоритм вычисления КОМ с применением секретного ключа, от которого зависит значение КОМ;
- хранение таблицы кодов в защищенной области памяти или хранение таблицы кодов на переносных носителях, доступ к которым контролируется организационными мерами.

В первом случае сложно обеспечить секретность алгоритма, поскольку он является долговременным элементом криптосистемы. Третий случай требует существенных трудозатрат на выполнение дополнительных организационных мер. Наиболее приемлемым является использование второго механизма. Однако во всех трех случаях необходимо предусмотреть защиту от программных закладок.

Методы, используемые для контроля целостности, должны обеспечить чрезвычайно малую вероятность какого-либо умышленного или неумышленного изменения данных, при котором их кодовое представление осталось бы неизменным. В этой области задача криптоанализа заключается в том, чтобы на основе изучения слабых мест алгоритма генерации КОМ осуществить изменение исходной информации таким образом, чтобы значение контрольного кода не изменилось. Алгоритмы вычисления КОМ называются алгоритмами защитного *контрольного суммирования*, а вырабатываемое ими проверочное значение — *контрольной суммой*. Большую роль в современных криптографических протоколах и системах играют *хэш-функции*, которые представляют собой частный случай алгоритмов вычисления защитных контрольных сумм.

Аутентификация информации — это установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком). Соблюдение заранее оговоренного протокола (набора правил и процедур) должно обеспечить максимальную вероятность этого факта. Очевидно, что при этом контролируется и целостность сообщения на возможность подмены или искажения. Принятый протокол должен обеспечить противодействие использованию потенциальным противником ранее переданных сообщений. В симметричных криптосистемах аутентификация осуществляется с применением одного или нескольких секретных ключей и защитных контрольных сумм. В асимметричных криптосистемах аутентификация осуществляется с использованием открытых ключей. Чтобы это было возможным, при распределении открытых ключей

осуществляется их аутентификация с использованием организационно-технических мероприятий.

Проблема аутентификации открытых ключей как одна из фундаментальных проблем криптографии предстала в явном виде с момента открытия *криптографии с открытым ключом* (двухключевой или асимметричной криптографии) в середине 70-х гг. прошлого века. Криптография с открытым ключом дала чрезвычайно удобное решение проблемы распределения секретных ключей, но ее использование требует осуществления процедуры аутентификации открытых ключей. Следует отметить, что проблема аутентификации ключей не является порождением двухключевой криптографии. Она в неявном виде всегда присутствовала в криптографии с секретным ключом. Действительно, при распределении секретных ключей по защищенному каналу одновременно осуществляется и их аутентификация. Например, при получении опечатанного пакета с секретным ключом получатель проверяет целостность пакета и печатей.

Если работа Шеннона «Теория связи в секретных системах» [38] заложила фундамент формирования криптологии как науки, то открытие двухключевой криптографии ознаменовало собой ее переход в качественно новую фазу развития. Это послужило основой для наиболее полного решения проблем аутентификации информации и разработки систем электронной цифровой подписи, которые призваны придать юридическую силу документам и другим сообщениям, переданным в электронном виде.

Электронная цифровая подпись (ЭЦП) основывается на двухключевых криптографических алгоритмах, в которых предусмотрено использование *двух* ключей — *открытого* и *секретного*. Идея использования открытого (т. е. известного всем пользователям криптосистемы и потенциальному злоумышленнику) ключа является фундаментальной, поэтому двухключевые криптосистемы еще называют открытыми шифрами, а выполняемые преобразования — открытым шифрованием. Двухключевые криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными абонентами (пользователями) криптосистемы. Доказательство основано на том, что двухключевые криптосистемы функционируют в условиях, когда пользователю нет необходимости сообщать свой секретный ключ какому-либо второму субъекту. Факт использования секретного ключа при выработке подписи к тому или иному электронному документу проверяется с использованием *открытого* ключа. При этом знание открытого ключа не дает возможности выработать правильную цифровую подпись. Таким образом, ответственность за сохранность *секретного* ключа и соблюдение правил его использования лежит на самом владельце этого ключа. Секретный ключ позволяет составить сообщение со специфической внут-