ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)**

Кафедра вычислительных машин, комплексов, систем и сетей

А.И. Терентьев

ЗАЩИТА ИНФОРМАЦИИ

ПОСОБИЕ
по выполнению лабораторных работ

*для студентов
III курса направления 230100
и IV курса специальности 230101
дневного обучения*

Москва - 2012

ББК 6Ф7.3
Т69

Рецензент д-р техн. наук, проф. Г.И. Хохлов

Терентьев А.И.

Т69 Защита информации: пособие по выполнению лабораторных работ. - М.: МГТУ ГА, 2012. – 36 с.

Данное пособие издается в соответствии с рабочей программой учебной дисциплины «Защита информации» по Учебному плану для студентов III курса направления 230100 и IV курса специальности 230101 дневного обучения.

Рассмотрено и одобрено на заседаниях кафедры 27.11.12 г. и методического совета 27.11.12 г.

Редактор И.В. Вилкова

Подписано в печать 23.01.13 г.

Печать офсетная	Формат 60x84/16	2,03 уч.-изд. л.
2,10 усл.печ.л.	Заказ № 1558/	Тираж 100 экз.

Московский государственный технический университет ГА
125993 Москва, Кронштадтский бульвар, д. 20
Редакционно-издательский отдел
125493 Москва, ул. Пулковская, д.6а

Введение

С развитием электронных технологий и коммуникаций проблема защиты информационных ресурсов от несанкционированного доступа (НСД), подделки и модификации приобретает особую актуальность и значимость, а изучение современных методов противодействия указанным деструктивным воздействиям является необходимым условием при подготовке квалифицированных специалистов.

В настоящем пособии приведен материал для выполнения двух лабораторных работ, а также рассматриваются некоторые элементы теории, система приемов и способов исследования криптографических методов защиты информации (электронных документов) от НСД, подделки и модификации. Предлагаемые индивидуальные задания для самостоятельной работы позволяют оценить уровень полученных теоретических знаний и качество проведенных исследований, а также способствуют формированию необходимых навыков использования изучаемых методов защиты и противодействия на практике.

ЛАБОРАТОРНАЯ РАБОТА № 1

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

1.1. Цель работы

Изучение принципов построения современных симметричных, асимметричных и гибридных криптографических систем. Исследование и апробирование современных методов блочного криптографического преобразования с секретным ключом: государственного стандарта Российской Федерации на шифрование данных (ГОСТ 28147–89), федеральных стандартов США на шифрование данных DES и AES (Rijndael), а также метода криптографического преобразования с открытым ключом по алгоритму RSA.

1.2. Принципы построения криптографических систем

Одним из эффективных методов защиты информации от несанкционированного доступа является ее специальное преобразование, заключающееся в приведении составляющих ее элементов (слов, букв, цифр) с помощь специальных алгоритмов к виду, не позволяющему воспроизвести исходные данные без знания секрета обратного преобразования (восстановления) или специального ключа. Такое преобразование информации называется зашифрованием или

криптографическим преобразованием и осуществляется с целью ее сокрытия от посторонних лиц, а также обеспечения ее подлинности и целостности. Информацию, подлежащую зашифрованию, называют открытым текстом m. Результат зашифрования открытого текста называют шифрованным текстом c или криптограммой. Применение к шифрованному тексту c обратного преобразования с целью получить открытый текст m называют расшифрованием. Шифратором принято называть специальное техническое устройство, реализующее зашифрование и расшифрование информации. Шифром называют совокупность алгоритмов или однозначных отображений открытого текста m в недоступный для восприятия шифрованный текст c. Ключом k называют некоторый секретный параметр шифра, позволяющий выбрать для шифрования только одно конкретное преобразование E_k из всего множества преобразований, составляющих шифр. Под криптостойкостью понимают потенциальную способность шифра противостоять раскрытию. Для этого стойкий шифр должен удовлетворять требованиям:

1) пространство ключей должно иметь достаточную мощность, чтобы перебор всех возможных преобразований E_k был невозможным;
2) по криптограмме $c = E_k(m)$ очень трудно определить k и/или m.

Для шифрования открытого текста m используется специальный алгоритм, реализуемый вручную или техническим устройством (механическим, электрическим, ЭВМ). Секретность преобразования достигается за счет использования уникального (не известного злоумышленнику) алгоритма или ключа, обеспечивающего каждый раз оригинальное шифрование информации. Однако с развитием криптографии базовым принципом современных систем шифрования стало правило Кирхгофа (Kerckhoff, 1835–1903), согласно которому известность противнику алгоритма преобразования не должна снижать надежность системы шифрования, а ее криптостойкость определяется только секретностью (надлежащим сохранением в тайне от посторонних) и качеством используемых криптографических ключей. Таким образом, без знания секретного ключа расшифрование должно быть практически невыполнимым, даже при известном алгоритме шифрования.

Криптографическая система состоит из следующих компонент:

1) пространства открытых текстов M;
2) пространства ключей K;
3) пространства шифрованных текстов (криптограмм) C;
4) двух функций $E_k : M \to C$ (зашифрования) и $D_k : C \to M$ (расшифрования) для $k \in K$ таких, что

   $E_k(m) = c$ (где c - криптограмма, с $\in C$);

   $D_k(c) = m$ (где m - открытый текст, $m \in M$);

   $D_k(E_k(m)) = m$ (для любого открытого текста $m \in M$).

Симметричными называются криптосистемы, в которых для зашифрования и расшифрования информации используется один и тот же ключ, называе-

мый секретным, что обусловливает другие наименования таких систем: одноключевые или криптосистемы с секретным ключом. Обобщенная схема симметричной криптосистемы приведена на рис. 1.1.

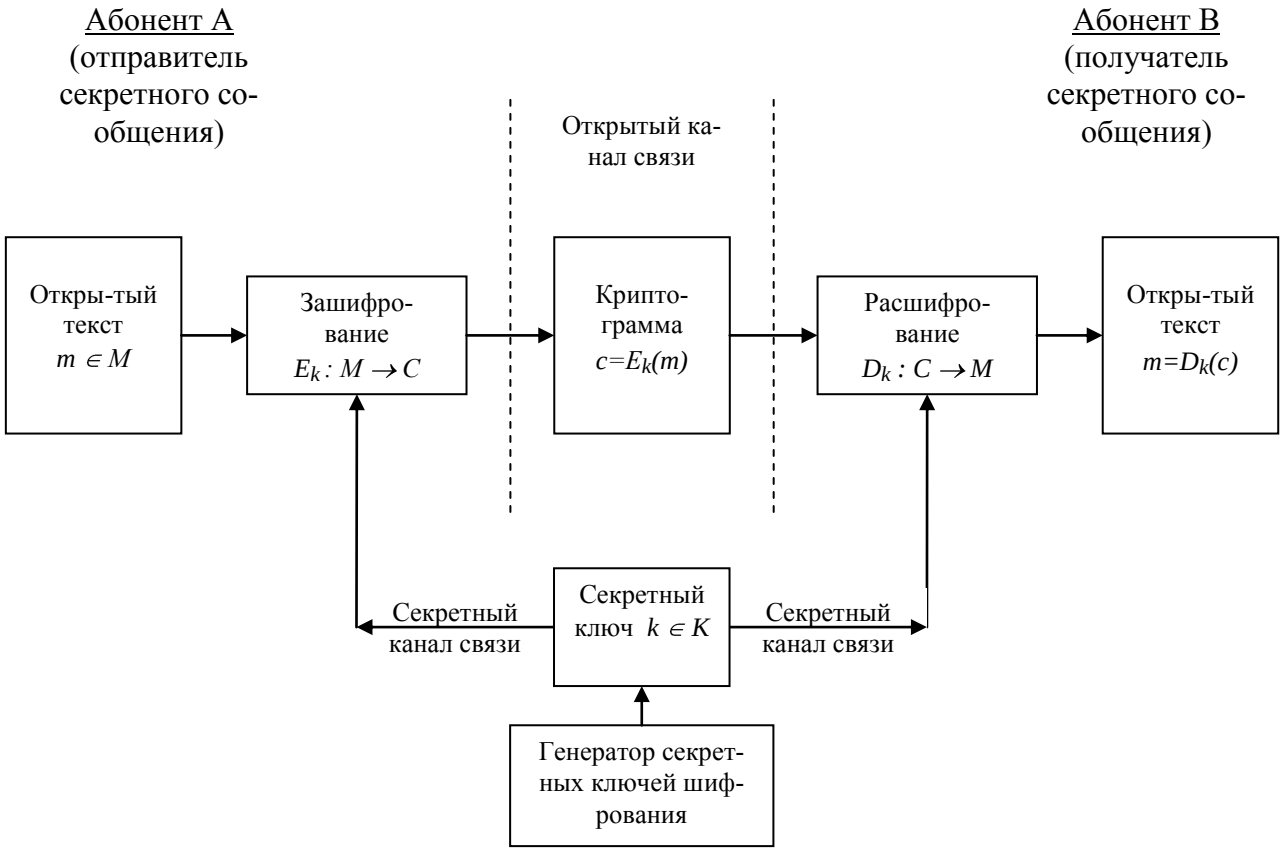


Рис. 1.1. Схема симметричной криптографической системы

Симметричные криптосистемы могут реализовываться на различных алгоритмах (стандартах) шифрования с секретным ключом, которые можно разделить на блочные и поточные.

При блочном шифровании открытый текст предварительно разбивается на равные по длине блоки. Блочные шифры выполняют предусмотренные своим алгоритмом криптографические преобразования над одним блоком данных (блоком открытого текста или некоторой гаммированной последовательностью) фиксированной длины, в результате которых получается блок шифрованного текста такой же длины. После этого аналогичному преобразованию подвергается следующий блок данных.

Поточные шифры преобразуют открытый текст в шифрованный текст по одному элементу за операцию (потоком − элемент за элементом). Например, биты открытого текста складываются по модулю 2 с битами некоторой псевдослучайной последовательности.

Современные симметричные криптосистемы представлены такими широко известными стандартами, как ГОСТ 28147–89 (Россия), DES и Rijndael

(США), которые являются блочными шифрами. Эти и большинство других шифров с секретным ключом основаны на принципе итерации.

Принцип итерации (повторения) заключается в многократном, состоящем из одинаковых циклов (раундов), преобразовании одного блока открытого текста. Как правило, на каждом раунде преобразование данных осуществляется при помощи нового вспомогательного ключа, полученного из исходного секретного ключа по специальному алгоритму.

Стандарты ГОСТ 28147−89 (Россия), DES (США) и многие другие известные шифры с секретным ключом основаны на использовании конструкции (структуры, сети, петли) Хорста Фейстеля (H. Feistel). Конструкция Фейстеля заключается в том, что блок открытого текста с четным числом элементов (например, бит) разбивается на две равные части – левую L и правую R. На каждом раунде одна из частей подвергается преобразованию при помощи функции шифрования f и раундового (вспомогательного) ключа k_i. Результат этой операции суммируется по модулю 2 (обозначается на схеме как $\oplus$) с другой частью. Затем левая L и правая R части меняются местами и процесс преобразования повторяется. Обобщенная схема конструкции Фейстеля представлена на рис. 1.2.

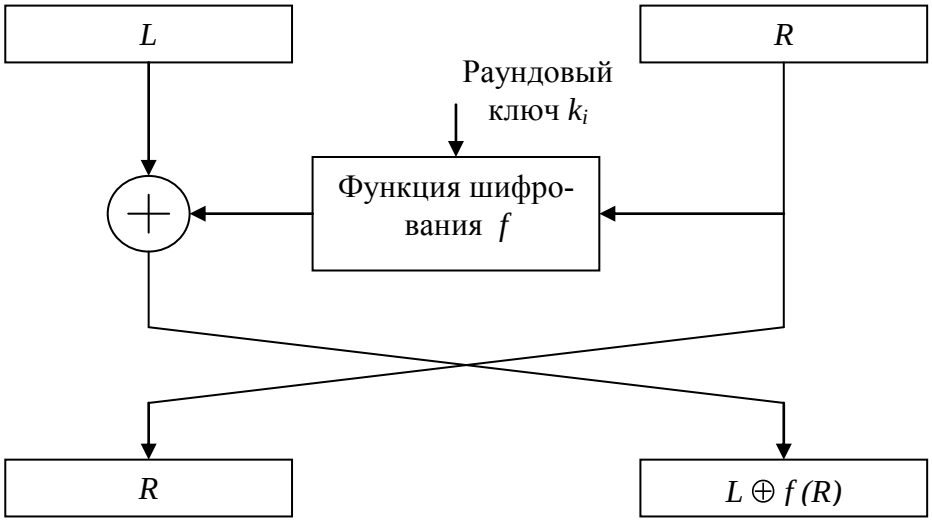


Рис. 1.2. Схема конструкции Фейстеля

Достоинством конструкции Фейстеля является то, что прямое и обратное криптографическое преобразование имеют одинаковую структуру. Только при расшифровании раундовые ключи используются в обратном порядке. Недостатком является то, что при каждом раунде преобразуется только половина блока открытого текста. Это приводит к необходимости увеличивать число раундов для достижения требуемой криптостойкости шифра.

Существенным недостатком симметричных криптосистем является сложность обеспечения безопасной доставки (распределения) и использования секретных ключей шифрования. Этот недостаток исключен в асимметричных криптосистемах (другое наименование: двуключевые или криптосистемы с открытым ключом), в которых для зашифрования информации используется один ключ, называемый открытым, а для последующего расшифрования – другой ключ, называемый закрытым (секретным). Обобщенная схема асимметричной криптосистемы приведена на рис. 1.3.

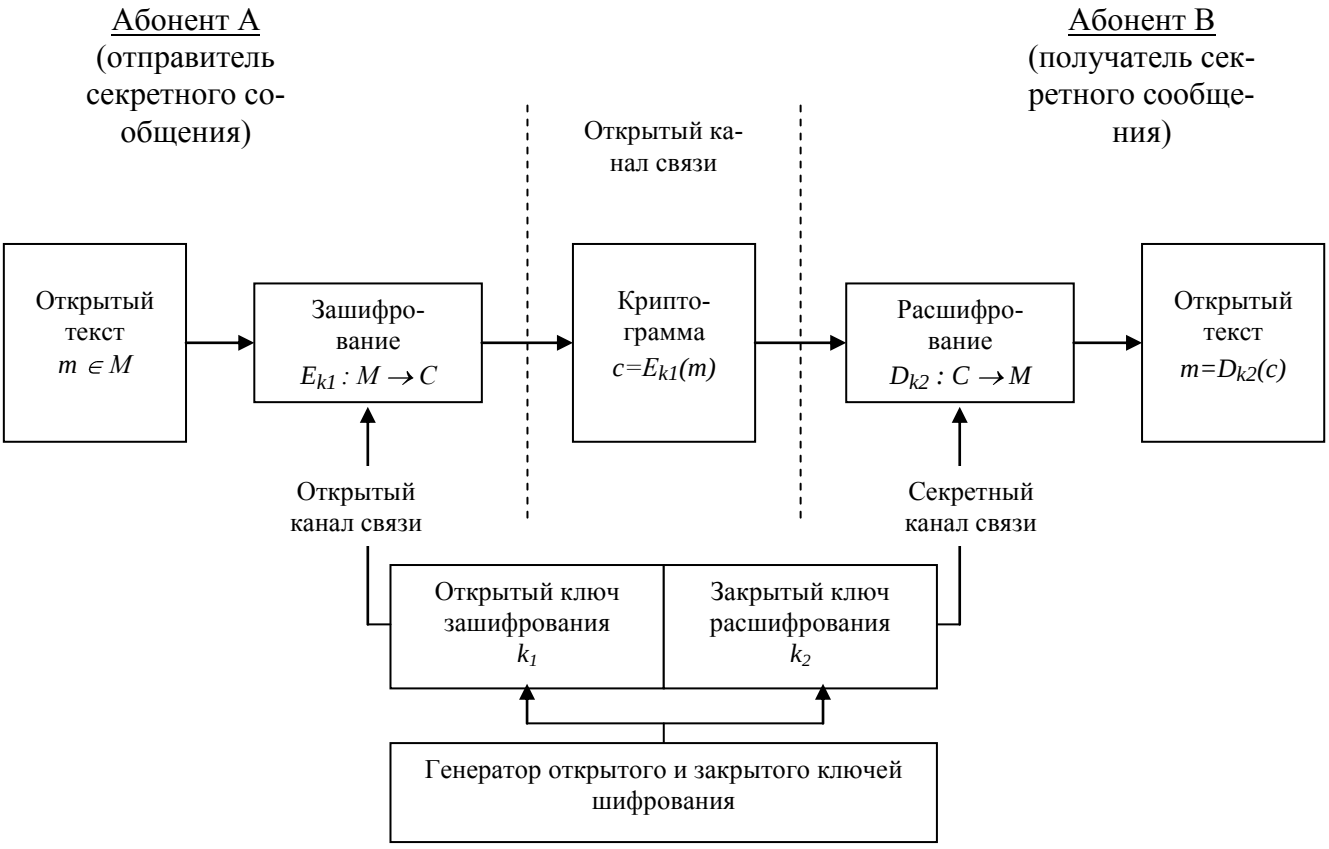


Рис. 1.3. Схема асимметричной криптографической системы

В асимметричных криптосистемах проблемы с доставкой открытого ключа не существует, поскольку он никакого секрета не представляет и может быть известен всем желающим зашифровывать информацию. Метод шифрования с открытым ключом, вместе с открытым распределением ключей, был предложен в 1976 году Уитфилдом Диффи и Мартиным Хеллманом, а его первая практическая реализация осуществлена Рональдом Ривестом, Эди Шамиром и Леонардом Эдлеманом (алгоритм RSA).

Существенным недостатком методов шифрования с открытым ключом является низкое быстродействие: они на 2−3 порядка медленнее методов шифрования с секретным ключом. В свою очередь, основной (достаточно сложной и требующей значительных затрат) проблемой при симметричном шифровании

является обеспечение безопасного распределения (доставки абонентам) секретных криптографических ключей. Поэтому на практике эффективно используются гибридные криптосистемы [от лат. hibrida − помесь], совмещающие в себе элементы симметричных и асимметричных криптосистем и сочетающие соответственно присущие им достоинства: для симметричных методов шифрования − высокую скорость и короткие криптографические ключи, для асимметричных − возможность открытого и безопасного распределения ключей шифрования.

В гибридной криптосистеме методы шифрования с открытым ключом применяются для шифрования, передачи и последующего расшифрования только секретного ключа симметричного шифрования, который непосредственно применяется для шифрования передаваемых сообщений (открытого текста). Таким образом, асимметричная криптосистема гармонично дополняет симметричную криптосистему, обеспечивая простое и безопасное распределение (передачу) секретных ключей шифрования. Обобщенная схема гибридной криптосистемы приведена на рис. 1.4.

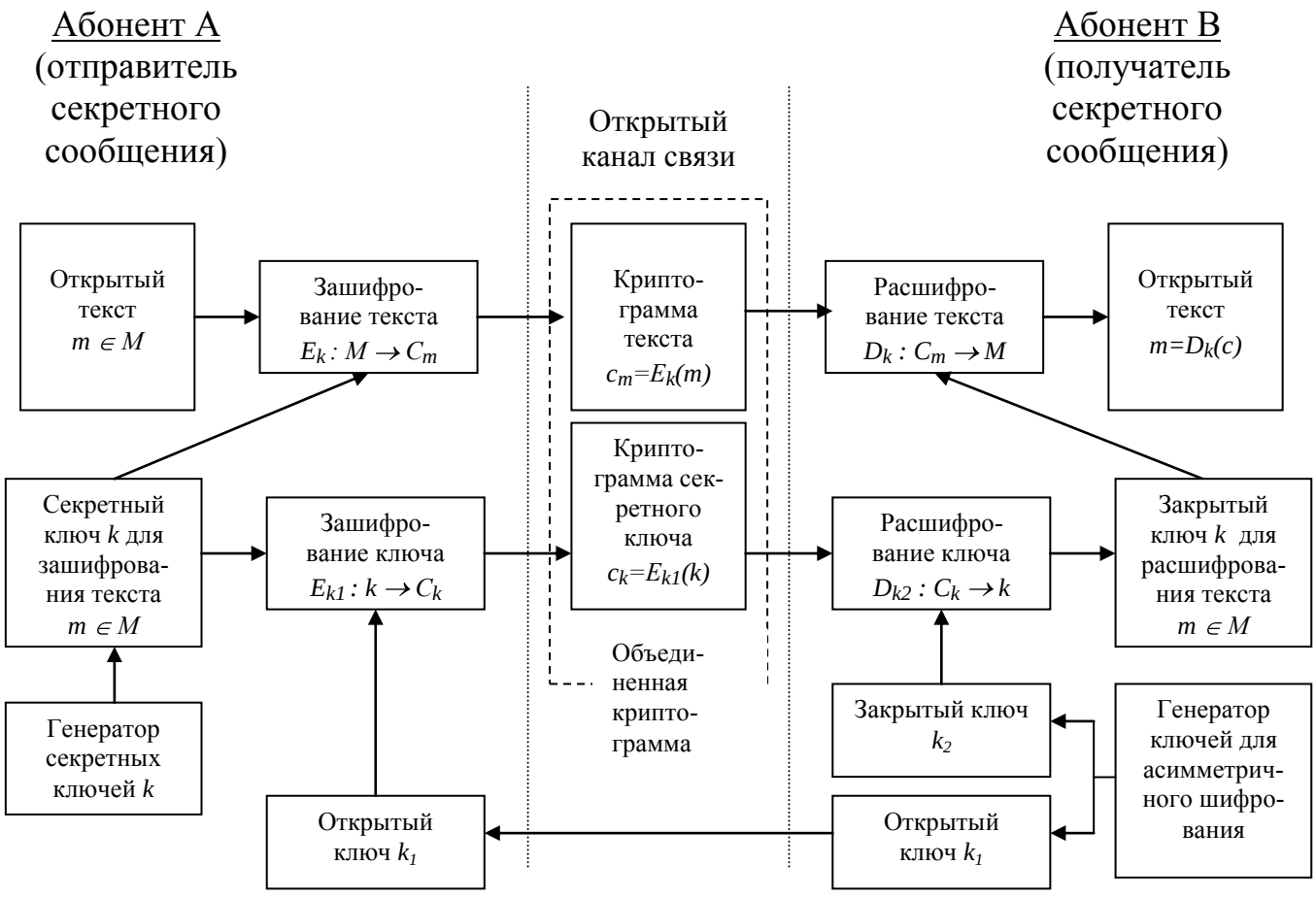


Рис. 1.4. Схема гибридной криптографической системы

Протокол сеанса секретной связи (передачи секретного сообщения) между абонентом А (отправителем) и абонентом В (получателем) может быть следующим:

1. Абонент В генерирует открытый (k_1) и закрытый (k_2) ключи для асимметричного шифрования, и передает открытый ключ k_1 по открытому (доступному, незащищенному) каналу связи абоненту А.

2. Абонент А генерирует сеансовый секретный криптографический ключ k для симметричного шифрования и зашифровывает на нем подлежащее передаче секретное сообщение (открытый текст) m.

3. Абонент А зашифровывает сеансовый секретный криптографический ключ k на открытом ключе k_1.

4. Абонент А передает по открытому каналу связи в адрес абонента В криптограмму исходного открытого текста (зашифрованное сообщение m) вместе с криптограммой сеансового секретного криптографического ключа k, использованного для зашифрования этого сообщения.

5. Абонент В расшифровывает на закрытом ключе k_2 сеансовый секретный криптографический ключ k, с помощью которого расшифровывает криптограмму сообщения m.

Для повышения криптостойкости в гибридной криптографической системе для каждого сеанса секретной связи (шифрования нового сообщения) генерируется свой секретный ключ для симметричного шифрования, называемый соответственно сеансовым.

Выбор размера криптографических ключей для симметричного и асимметричного шифрования осуществляется таким образом, чтобы их потенциальная криптостойкость к атаке по методу полного перебора возможных вариантов была сопоставимой.

В случае, если открытый и закрытый ключи асимметричного шифрования используются неоднократно (долговременно), то их криптостойкость должна быть существенно выше, чем у сеансового секретного ключа симметричного шифрования, поскольку при их раскрытии (дискредитации), противник получит возможность расшифровывать передаваемые сеансовые секретные ключи и соответственно зашифрованные на них сообщения.

В табл. 1 приведены длины ключей симметричных криптосистем, имеющих трудность раскрытия по методу полного перебора, сопоставимую с трудностью факторизации соответствующих модулей асимметричных криптосистем.

Таблица 1

Длина ключа симметричной криптосистемы, бит	Модуль асимметричной криптосистемы, бит
56	384
64	512
80	768
112	1792
128	2304
192	5184
256	9216

1.3. Подготовка к выполнению работы

1. По основной [1, с. 49–77] и дополнительной [1–11] литературе, а также настоящему пособию изучить:

базовые методы шифрования (перестановки, замены, аддитивные), используемые в современных производных (комбинированных) шифрах;

принципы построения и характерные особенности симметричных, асимметричных и гибридных криптографических систем;

современные стандарты криптографического преобразования с секретным ключом (DES, ГОСТ 28147-89, AES (Rijndael)) и алгоритм шифрования с открытым ключом RSA.

2. Изучить порядок выполнения лабораторной работы. Получить у преподавателя и ознакомиться с руководством пользователя и интерфейсом обучающих программ, предназначенных для использования в лабораторной работе.

3. По настоящему пособию определить вариант индивидуального задания для:

а) моделирования (построения) гибридной криптографической системы;

б) вычисления числовой криптограммы (шифрования) сообщения по алгоритму RSA.

4. Используя учебную литературу и полученную у преподавателя обучающую программу "Математические основы криптографии", повторить элементы теории чисел и модулярной арифметики, а также основные математические операции, применяемые при реализации современных криптографических систем.

1.4. Порядок выполнения работы

1.4.1. Исследование стандартов шифрования с секретным ключом

1.4.1.1. Исследование стандарта шифрования DES (Data Encryption Standard)

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея блок-схемы: алгоритма DES, функции шифрования, алгоритма генерации раундовых 48-битовых криптографических ключей, а также используемые таблицы перестановки, замены, расширения и преобразования. Выделить в алгоритме конструкцию Фейстеля.

3. Используя обучающую программу, апробировать процесс зашифрования и расшифрования различных вариантов открытого текста (сообщений) на

различных криптографических ключах по алгоритму DES в режиме "Электронной кодовой книги" (ECB − Electronic Code Book):

а) ввести в режиме ручного ввода открытый текст для шифрования длиной не более 240 символов или выбрать его из имеющихся в обучающей программе вариантов;

б) ввести в режиме ручного ввода 64-битовый криптографический ключ для шифрования или выбрать его из имеющихся в обучающей программе вариантов;

в) выполнить процесс формирования раундовых 48-битовых криптографических ключей, вывести на экран дисплея исходный 64-битовый криптографический ключ и полученные раундовые 48-битовые криптографические ключи;

г) выполнить процесс зашифрования и расшифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

д) убедиться в корректности работы программы, правильности проведенных перестановок, замен, расширений и преобразований, сравнить первичный открытый текст с результатом расшифрования его криптограммы;

е) повторить пункты а−д для открытых текстов различной длины и новых криптографических ключей;

ж) выполнить пункты а−д для оригинальных открытого текста длиной не более 8 символов (64 бит) и 64-битового криптографического ключа, отличных от вариантов, имеющихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования.

4. Исследовать влияние исходных 64-битовых криптографических ключей на качество шифрования. Ввести "слабые" криптографические ключи. Рассмотреть, как это отражается на генерации 16 раундовых 48-битовых ключей и криптостойкости шифрования в целом. Рассмотреть назначение, расположение и влияние на процесс шифрования служебных битов исходного 64-битового криптографического ключа.

5. Исследовать результаты расшифрования при искажении элементов (битов) криптограммы (в условиях воздействия помех). Отразить полученные результаты в отчете по лабораторной работе.

1.4.1.2. Исследование стандарта шифрования ГОСТ 28147−89

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея блок-схемы: алгоритма ГОСТ 28147−89,

функции шифрования и таблицы выбора 32 раундовых 32-битовых криптографических ключей. Выделить в алгоритме конструкцию Фейстеля.

3. Используя обучающую программу, апробировать процесс зашифрования и расшифрования различных вариантов текста на различных криптографических ключах по алгоритму ГОСТ 28147−89 в режиме простой замены:

а) ввести в режиме ручного ввода текст для шифрования длиной не более 240 символов или выбрать его из имеющихся в обучающей программе вариантов;

б) ввести в режиме ручного ввода 256-битовый криптографический ключ для шифрования или выбрать его из имеющихся в обучающей программе вариантов;

в) выполнить выборку из исходного 256-битового ключа 32-раундовых 32-битовых криптографических ключей, вывести их на экран дисплея;

г) выбрать и вывести на экран дисплея таблицу подстановки, используемую в функции шифрования;

д) выполнить процесс зашифрования и расшифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

е) убедиться в корректности работы программы и правильности проведенных преобразований, сравнить первичный открытый текст с результатом расшифрования его криптограммы;

ж) повторить пункты а−е для открытых текстов различной длины и новых криптографических ключей;

з) выполнить пункты а−е для оригинальных открытого текста длиной не более 8 символов (64 бит) и 256-битового криптографического ключа, отличных от вариантов, имеющихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования.

4. Исследовать результаты расшифрования при искажении элементов (битов) криптограммы (в условиях воздействия помех). Отразить полученные результаты в отчете по лабораторной работе.

1.4.1.3. Исследование стандарта шифрования AES (Rijndael)

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея блок-схему алгоритма AES (Rijndael), описание основных процедур и преобразований, правила формирования прямоугольных матриц блока данных и ключа шифрования, алгоритм получения раундовых криптографических ключей.

3. Используя обучающую программу, апробировать процесс зашифрования и расшифрования различных вариантов текста на различных криптографических ключах по алгоритму AES (Rijndael) в режиме "Электронной кодовой книги" (ECB − Electronic Code Book):

а) ввести в режиме ручного ввода текст для шифрования длиной не более 240 символов или выбрать его из имеющихся в обучающей программе вариантов;

б) ввести в режиме ручного ввода 128, 192 или 256-битовый криптографический ключ для шифрования или выбрать его из имеющихся в обучающей программе вариантов;

в) установить длину блока данных и определить количество циклов (раундов) шифрования;

г) выполнить процедуры формирования и вывести на экран дисплея полученные раундовые криптографические ключи;

д) выполнить процесс зашифрования и расшифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

е) убедиться в корректности работы программы, правильности выполненных процедур и преобразований, сравнить первичный открытый текст с результатом расшифрования его криптограммы;

ж) повторить пункты а−е для новых открытых текстов и криптографических ключей различной длины;

з) выполнить пункты а–е для оригинальных открытого текста и криптографического ключа, отличных от вариантов, содержащихся в обучающей программе и имеющих длину в соответствии с индивидуальным заданием, указанным в табл. 2. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования.

4. Исследовать результаты расшифрования при искажении элементов (битов) криптограммы (в условиях воздействия помех). Отразить полученные результаты в отчете по лабораторной работе.

Таблица 2

Последняя цифра номера зачетной книжки	Длина блока данных, бит	Длина криптографического ключа, бит
0 или 1	128	128
2	128	192
3	128	256
4	192	128
5	192	192
6	192	256
7	256	128
8	256	192
9	256	256

1.4.2. Исследование алгоритма шифрования с открытым ключом RSA

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея описание и блок-схему алгоритма RSA, правила вычисления открытого (закрытого) криптографического ключа, прямого и обратного криптографических преобразований.

3. Используя обучающую программу, апробировать процесс зашифрования и расшифрования различных вариантов текста на различных криптографических ключах по алгоритму RSA:

а) ввести в режиме ручного ввода текст для шифрования длиной не более 240 символов или выбрать его из имеющихся в обучающей программе вариантов;

б) выполнить процедуру вычисления и вывести на экран дисплея открытый и закрытый (секретный) криптографические ключи для шифрования или ввести их в режиме ручного ввода (или выбрать их из имеющихся в обучающей программе вариантов);

в) представить введенный открытый текст как последовательность чисел в соответствии с выбранным модулем криптографического преобразования;

г) выполнить процесс зашифрования и расшифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

д) убедиться в корректности работы программы, правильности выполненных вычислений, сравнить первичный открытый текст с результатом расшифрования его криптограммы;

е) повторить пункты а–д для новых открытых текстов и криптографических ключей различной длины;

ж) выполнить пункты а–д для оригинальных открытого текста и криптографических ключей, отличных от вариантов, имеющихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования.

4. При помощи калькулятора (не используя обучающую программу) выполнить самостоятельное вычисление числовых значений криптограммы по простейшей реализации алгоритма RSA.

Текст для шифрования и исходные значения простых чисел P и G для вычисления открытого (E) и закрытого (D) криптографических ключей приведены в табл. 3 и табл. 4. Вариант текста для шифрования определяется по предпоследней цифре (i) номера зачетной книжки (табл. 3). Вариант значений P и G определяется по последней (j) цифре номера зачетной книжки (табл. 4). Полученные ключи E и D должны удовлетворять условию: $E > 7$ и $E \neq D$.

Таблица 3

i	Текст для шифрования
0	ВЗЛОМ
1	ВИРУС
2	ДАТЧИК
3	ДОСТУП
4	МЕТОД
5	ОБЪЕКТ
6	ПАРОЛЬ
7	ПЭМИН
8	РЕЖИМ
9	СЕКРЕТ

Таблица 4

j	Значение P	Значение G
0	3	17
1	3	19
2	3	23
3	3	29
4	5	11
5	5	17
6	7	17
7	7	19
8	13	17
9	19	29

Числовые представления (эквиваленты) букв русского алфавита представлены в табл. 5.

Таблица 5

Буква	Число	Буква	Число	Буква	Число
А	1	К	12	Х	23
Б	2	Л	13	Ц	24
В	3	М	14	Ч	25
Г	4	Н	15	Ш	26
Д	5	О	16	Щ	27
Е	6	П	17	Ъ	28
Ё	7	Р	18	Ы	29
Ж	8	С	19	Ь	30
З	9	Т	20	Э	31
И	10	У	21	Ю	32
Й	11	Ф	22	Я	33

Простые числа до 2239 представлены в табл. 6.

Таблица 6

2	163	379	613	859	1109	1409	1657	1951
3	167	383	617	863	1117	1423	1663	1973
5	173	389	619	877	1123	1427	1667	1979
7	179	397	631	881	1129	1429	1669	1987
11	181	401	641	883	1151	1433	1693	1993
13	191	409	643	887	1153	1439	1697	1997
17	193	419	647	907	1163	1447	1699	1999
19	197	421	653	911	1171	1451	1709	2003
23	199	431	659	919	1181	1453	1721	2011
29	211	433	661	929	1187	1459	1723	2017
31	223	439	673	937	1193	1471	1733	2027
37	227	443	677	941	1201	1481	1741	2029
41	229	449	683	947	1213	1483	1747	2039
43	239	457	691	953	1217	1487	1753	2053
47	233	461	701	967	1223	1489	1759	2063
53	241	463	709	971	1229	1493	1777	2069
59	251	467	719	977	1231	1499	1783	2081
61	257	479	727	983	1237	1511	1787	2083
67	263	487	733	991	1249	1523	1789	2087
71	269	491	739	997	1259	1531	1801	2089
73	271	499	743	1009	1277	1543	1811	2099
79	277	503	751	1013	1279	1549	1823	2111
83	281	509	757	1019	1283	1553	1831	2113
89	283	521	761	1021	1289	1559	1847	2129
97	293	523	769	1031	1291	1567	1861	2131
101	307	541	773	1033	1297	1571	1867	2137
103	311	547	787	1039	1301	1579	1871	2141
107	313	557	797	1049	1303	1583	1873	2143
109	317	563	809	1051	1307	1597	1877	2153
113	331	569	811	1061	1319	1601	1879	2161
127	337	571	821	1063	1321	1607	1889	2179
131	347	577	823	1069	1327	1609	1901	2203
137	349	587	827	1087	1361	1613	1907	2207
139	353	593	829	1091	1367	1619	1913	2213
149	359	599	839	1093	1373	1621	1931	2221
151	367	601	853	1097	1381	1627	1933	2237
157	373	607	857	1103	1399	1637	1949	2239

1.4.3. Моделирование гибридной криптосистемы

1. Выполнить моделирование (построение) гибридной криптосистемы. Необходимые для моделирования параметры определяются по последней цифре номера зачетной книжки в соответствии с табл. 7.

Таблица 7

Последняя цифра номера зачетной книжки	Метод шифрования с секретным ключом		Метод шифрования с открытым ключом
	стандарт	длина ключа (бит)	
1, 6	ГОСТ 28147-89	стандартная	RSA
2, 7	AES (Rijndael)	128	RSA
3, 8	AES (Rijndael)	192	RSA
4, 9	AES (Rijndael)	256	RSA
5, 0	DES	стандартная	RSA

2. Для выбранного варианта определить длину используемых криптографических ключей, исходя из предположения, что открытый и закрытый ключи асимметричного шифрования являются долговременными.

3. Отобразить в отчете по лабораторной работе полученные параметры гибридной криптосистемы (длину ключей и блоков) на ее обобщенной схеме.

4. Провести сеанс секретной связи (передачу секретного сообщения), имитируя использование смоделированной гибридной криптосистемы по следующему протоколу:

а) студент В – получатель секретного сообщения, самостоятельно генерирует открытый и закрытый ключи для асимметричного шифрования;

б) студент В передает по открытому каналу связи (публично объявляет, записывает в тетрадь, передает по локальной сети, копирует на дискету) открытый ключ студенту А. Закрытый ключ сохраняется в тайне от остальных студентов, выполняющих лабораторную работу;

в) студент А – отправитель секретного сообщения, генерирует сеансовый секретный криптографический ключ;

г) студент А составляет короткое сообщение $m \in M$ и зашифровывает его на полученном сеансовом секретном ключе;

д) студент А зашифровывает использованный сеансовый секретный ключ на открытом ключе студента В;

е) студент А передает по открытому каналу связи (по локальной сети, копирует на дискету) в адрес студента В зашифрованное сообщение вместе с зашифрованным сеансовым секретным криптографическим ключом;

ж) студент В расшифровывает на своем закрытом ключе сеансовый секретный криптографический ключ, с помощью которого расшифровывает сообщение *m*, составленное студентом А.

з) студенты А и В сравнивают результат расшифрования криптограммы с исходным сообщением (открытым текстом), составленным студентом А.

1.5. Контрольные вопросы

1. В чем заключаются традиционные методы шифрования, являющиеся базовыми для современных производных шифров с секретным ключом.
2. В чем заключается правило Кирхгоффа.
3. Что называется криптостойкостью шифра. Какой шифр считается стойким.
4. В чем заключаются принципы блочного шифрования.
5. В чем заключаются принципы поточного шифрования.
6. Какие основные преимущества и недостатки блочного и поточного шифрования.
7. В чем заключается принцип итерации.
8. Как реализуется конструкция Фейстеля, в каких стандартах шифрования она используется.
9. Какие основные параметры у стандартов шифрования ГОСТ 28147−89, DES, Rijndael (длина ключа, длина шифруемого блока, количество раундов (циклов) шифрования).
10. Какие отличительные особенности имеет стандарт AES (Rijndael) по сравнению с алгоритмами ГОСТ 28147−89 и DES.
11. В каких режимах работы могут использоваться стандарты шифрования ГОСТ 28147-89, DES и AES (Rijndael).
12. Какие особенности структуры у криптографических ключей, используемых в стандартах ГОСТ 28147−89, DES и Rijndael.
13. Как реализуется режим "Электронной кодовой книги" в стандарте DES и простой замены в ГОСТ 28147−89.
14. Как вырабатывается и для чего служит иммитовставка.
15. На каких математических принципах и задачах (проблемах) основаны асимметричные криптосистемы.
16. Что называется простым числом, взаимно простыми числами, вычетом числа по некоторому модулю. В чем заключается основная теорема арифметики, алгоритм Евклида, малая теорема Ферма.
17. Какие основные преимущества и недостатки симметричных и асимметричных криптосистем.
18. Как строится (реализуется) гибридная криптосистема. В чем ее преимущество по сравнению с другими типами криптосистем.
19. От чего зависит крипстойкость шифра на основе алгоритма RSA. Какие длины ключей рекомендованы для использования на практике при реализации криптосистем RSA.
20. Какие шифры называются комбинированными (производными) и какие базовые методы шифрования используются при их реализации.

1.6. Содержание отчета

Отчет по выполненной лабораторной работе должен содержать:

1. Тему и цель работы.

2. Структурную схему гибридной криптосистемы с параметрами, соответствующими варианту индивидуального задания.

3. Схемы алгоритмов шифрования, которые использовались при построении гибридной криптосистемы.

4. Результаты, полученные при апробировании процесса симметричного шифрования с использованием обучающих программ.

5. Результаты самостоятельного шифрования по алгоритму RSA в соответствии с вариантом индивидуального задания.

6. Анализ полученных результатов и выводы по лабораторной работе.

7. Возможные предложения по использованию рассмотренных методов шифрования на практике и/или совершенствованию обучающих программ.

Литература

Основная

1. Терентьев А.И. Введение в информационную безопасность: учеб. пособие. – М.: МГТУ ГА, 2001.

Дополнительная

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие. – М.: Гелиос АРВ, 2001.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2002.
3. Введение в криптографию/ под общ. ред. В.В.Ященко. – М.: МЦНМО, "ЧеРо", 1998.
4. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001.
5. Фороузан Б.А. Криптография и безопасность сетей: учеб. пособие/ пер. с англ. под ред. А.Н.Берлина. – М.: Интернет-Университет информационных технологий: БИНОМ. Лаборатория знаний, 2010.
6. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография: учебник для вузов. – СПб.: Издательство "Лань", 2001.
7. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): учеб. пособие для университетов и педагогических вузов/ под ред. В.А.Садовничего. – М.: Высш. школа, 1999.
8. Панасенко С.П. Алгоритмы шифрования: специальный справочник. – СПб.: БХВ-Петербург, 2009.
9. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000.
10. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ под ред. В.Ф.Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.
11. Чмора А.Л. Современная прикладная криптография. - 2-е изд. стереотип. – М.: Гелиос АРВ, 2002.

ЛАБОРАТОРНАЯ РАБОТА № 2

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ПОДЛИННОСТИ И ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

2.1. Цель работы

Изучение современных принципов обеспечения подлинности и целостности электронных документов с использованием методов криптографического преобразования информации. Построение функций хэширования на основе блочных шифраторов с секретным ключом. Исследование и апробирование функции хэширования по ГОСТ Р 34.11–94 и алгоритмов электронной цифровой подписи EGSA (Эль-Гамаля), ГОСТ Р 34.10–94 и ГОСТ Р 34.10–01.

2.2. Функции хэширования и алгоритмы электронной цифровой подписи

Функцией хэширования или хэш-функцией (Hash-function) называется алгоритм сжатия (преобразования) текста $m \in M$ (где M – пространство текстов) произвольной длины L до некоторого числового значения $z = h(m)$ фиксированной длины, называемого хэш-значением или дайджестом этого текста (Message Digest). При этом значение z хэш-функции сложным образом зависит от исходного текста m и непременно изменяется при любой его модификации. Таким образом не существует двух разных текстов $m_1 \neq m_2$, имеющих одинаковое хэш-значение z, т.е. всегда справедливо $h(m_1) \neq h(m_2)$. Кроме того, по отношению к злоумышленнику (противнику), хэш-функция является однонаправленной, т.е. восстановить по ее хэш-значению z исходный текст m не представляется возможным.

На практике качественные функции хэширования эффективно реализуются на основе блока хэширования, преобразующего две входные последовательности элементов (например, бит) одинаковой длины в одну выходную последовательность (хэш-значение) такой же длины. Входными последовательностями могут являться i-й блок текста m_i (предварительно весь текст m, подлежащий хэшированию, разбивается на блоки $m = (m_1, \ldots, m_i, \ldots, m_n)$ фиксированной длины) и хэш-значение z_{i-1}, полученное для предыдущего блока m_{i-1} текста m. В результате формируется хэш-значение z_i для текущего блока m_i

$$z_i = h(m_i, z_{i-1}).$$

Хэш-значение, полученное для последнего блока m_n, является результирующим хэш-значением всего текста (сообщения) m. Таким образом формируется хэш-значение фиксированной длины, независимо от длины входного текста m. Схема описанной конструкции изображена на рис. 2.1.

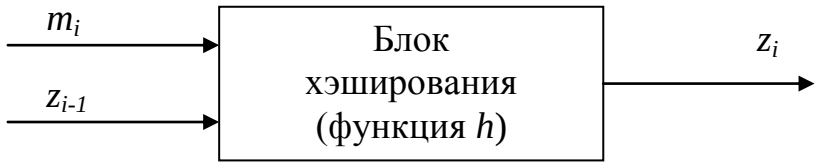
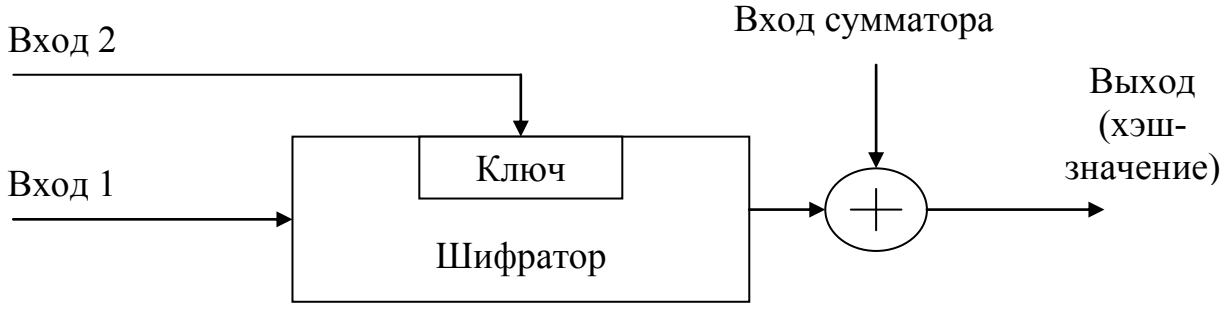


Рис. 2.1. Схема функции хэширования

На практике рассмотренную функцию хэширования можно реализовать на основе алгоритмов симметричного блочного шифрования, используя в качестве блока однонаправленного хэширования блочный шифратор с секретным ключом (имеющий, в простейшем случае, одинаковую длину блока данных и ключа шифрования). В этом случае в качестве одного входа функции хэширования служит вход шифратора для блока данных, а второго – ключа шифрования.

Для обеспечения взаимной зависимости (сцепления, обратной связи) блоков текста, результат криптографического преобразования (последовательность на выходе шифратора), суммируется по модулю 2 с текущим блоком данных m_i, предыдущим хэш-значением z_{i-1} или некоторой гаммированной последовательностью. Полученная на выходе сумматора последовательность будет являться текущим хэш-значением z_i. Качество (стойкость, безопасность) такой функции хэширования определяется криптостойкостью используемого алгоритма симметричного блочного шифрования. Обобщенная схема функции хэширования, у которой хэш-значение, входной блок данных и ключ шифрования имеют одинаковую длину, показана на рис. 2.2.



$\oplus$ – операция побитового сложения по *mod* 2
последовательностей одинаковой длины

Рис. 2.2. Схема реализации функции хэширования на основе блочного шифратора с секретным ключом

На основе рассмотренного метода реализован отечественный стандарт функции хэширования ГОСТ Р 34.11-94, который преобразует двоичную последовательность произвольной длины в 256-битовое хэш-значение. В нем использован в режиме простой замены алгоритм симметричного блочного шифрования по ГОСТ 28147−89, имеющий 256-битовый ключ и обрабатывающий блоки данных длиной 64 бита. Функция хэширования по ГОСТ Р 34.11-94 предназначена для использования при формировании электронной цифровой подписи по ГОСТ Р 34.10-94. Подробное описание указанных алгоритмов можно найти в дополнительной литературе [1, 3, 4, 6–9, 11].

В настоящее время под электронной цифровой подписью (ЭЦП) документа понимается некоторое числовое значение (дополнительное количество информации), вычисленное по специальному алгоритму для этого электронного документа и зашифрованное с помощью секретного ключа подписанта. ЭЦП передается вместе с подписанным документом и проверяется посредством общеизвестной процедуры с помощью соответствующего открытого ключа.

Специальное числовое значение z (двоичное, десятичное или другое), которое неразрывно связано с документом и характеризует его в целом, является значением функции хэширования $h(m)$ подписываемого текста m. Число z, зашифрованное секретным ключом подписанта, по сути и является электронной цифровой подписью этого документа.

При проверке подлинности и целостности электронного документа получатель самостоятельно вычисляет (естественно, используя одинаковую с подписантом функцию хэширования) его хэш-значение $z' = h(m')$. В случае, если расшифрованное с помощью имеющегося у него открытого ключа полученное хэш-значение z совпадет с самостоятельно вычисленным хэш-значением z' (т.е. $z = z'$), то ЭЦП признается подлинной и целостность документа не вызывает сомнений.

Для формирования ЭЦП можно успешно применять практически все известные методы открытого (асимметричного) шифрования, что в сочетании с открытым распределением ключей позволяет организовать электронный документооборот с приданием электронным документам юридической значимости. Обобщенная схема ЭЦП на основе методов асимметричного шифрования приведена на рис. 2.3.

Кроме того, для этих целей могут так же использоваться методы симметричного шифрования (системы с секретным ключом). Однако их реализация предусматривает наличие специальных центров распределения ключей.

Среди современных алгоритмов ЭЦП широкую известность получил алгоритм Эль-Гамаля (EGSA − El Gamal Signature Algorithm), являющийся более надежным по сравнению с алгоритмом RSA, поскольку он основан на задаче дискретного логарифмирования, которая считается вычислительно более сложной, чем разложение большого числа на простые множители. Рассмотрим основные этапы алгоритма Эль-Гамаля.

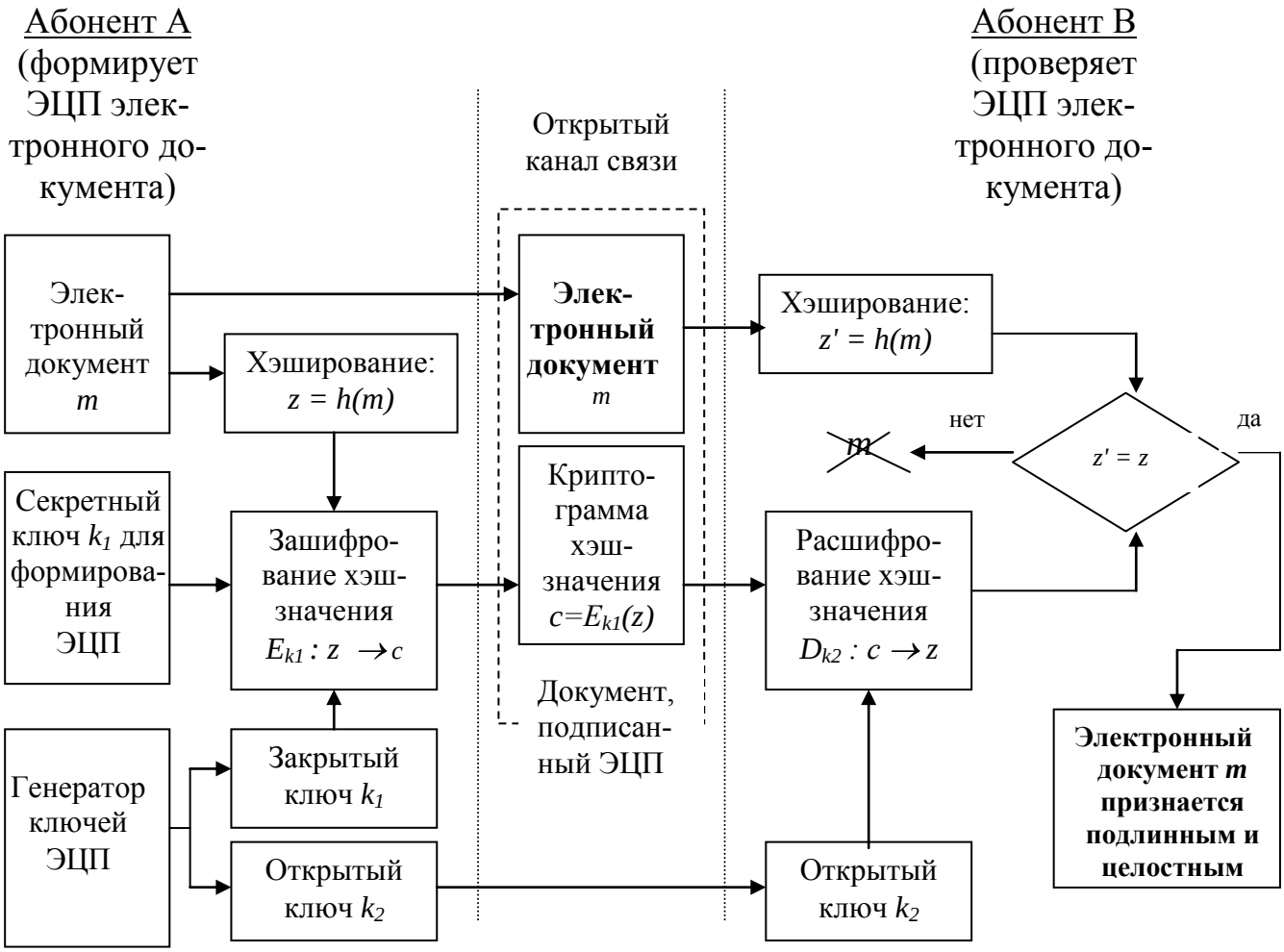


Рис. 2.3. Схема ЭЦП на основе методов асимметричного шифрования

1. Вычисляются открытый и закрытый ключи, для чего выбираются некоторое большое простое число P и большое целое число G (причем $P > G$), которые известны подписанту и получателю и не являются секретом. На практике используются очень большие числа $P \sim 10^{308}$ (2^{1024}) и $G \sim 10^{154}$ (2^{512}). Затем подписант выбирает случайное целое число X такое, что $1 < X \le (P\text{-}1)$, и вычисляет число

$$Y = G^X \bmod P,$$

которое является открытым ключом, используемым для проверки подлинности подписи отправителя, и открыто передается всем получателям электронных документов. Число X является секретным ключом отправителя для формирования ЭЦП и должно храниться в секрете.

2. Исходный электронный документ m представляется подписантом в виде целого числа z, причем $1 < z < (P\text{-}1)$, с помощью любой известной сторонам функции хэширования.

3. Выбирается случайное целое число K, причем $1 < K < (P\text{-}1)$, такое, что K и P являются взаимно простыми, т.е. $НОД\ (K,\ P\text{-}1) = 1$. Затем отправитель вычисляет целое число

$$a = G^K \ mod\ P$$

и, применяя расширенный алгоритм Евклида, вычисляет, используя числа X и K, целое число b из уравнения

$$z = X \cdot a + K \cdot b\ (mod\ (P\text{-}1)).$$

Пара чисел $(a,\ b)$ образуют ЭЦП, принадлежащую электронному документу m и передаваемую вместе с ним получателю. При этом пара чисел $(X,\ K)$ держится в строгом секрете (как правило, число K уничтожается после формирования ЭЦП).

Проверка подлинности ЭЦП полученного электронного документа заключается в проверке справедливости соотношения

$$Y^a \cdot a^b\ (mod\ P) = G^{z'}\ (mod\ P),$$

где числа $Y,\ a,\ b,\ P,\ G$ известны получателю, а число z' вычисляется им для документа m с использованием известной обеим сторонам функции хэширования. Если это соотношение выполняется, то полученный электронный документ m признается подлинным и целостным, поскольку можно математически доказать, что равенство будет истинным только в том случае, если подпись $S = (a,\ b)$ сформирована для документа m с использованием секретного ключа X, из которого был получен открытый ключ Y. Тем самым, подтверждается факт того, что отправителем электронного документа m может являться только обладатель секретного ключа X.

Следует отметить, что выполнение новой ЭЦП по методу EGSA требует выбора каждый раз нового случайного значения K, поскольку, если злоумышленник узнает какое-либо значение K, повторно используемое подписантом, то он сможет раскрыть его секретный ключ.

2.3. Подготовка к выполнению работы

1. По основной [1, с. 57–82] и дополнительной [1–11] литературе, а также настоящему пособию изучить:

- принципы построения функции хэширования электронных документов;
- современные стандарты криптографического преобразования с секретным ключом (DES, ГОСТ 28147-89, AES (Rijndael)) и алгоритмы шифрования с открытым ключом RSA и EGSA;

- принципы и методы обеспечения подлинности и целостности электронных документов посредством формирования ЭЦП;
- современные стандарты функций хэширования (ГОСТ Р 34.11-94) и электронной цифровой подписи (EGSA, ГОСТ Р 34.10-94, ГОСТ Р 34.10-01);
- положения Федерального закона "Об электронной цифровой подписи".

2. Изучить порядок выполнения лабораторной работы. Получить у преподавателя и ознакомиться с руководством пользователя и интерфейсом обучающих программ, предназначенных для использования в лабораторной работе.

3. По настоящему пособию определить вариант индивидуального задания для:

- моделирования (построения) функции хэширования на основе алгоритма симметричного блочного шифрования;
- вычисления электронной цифровой подписи по алгоритму EGSA для простого буквенного сообщения.

4. Используя учебную литературу и полученную у преподавателя обучающую программу "Математические основы криптографии", повторить элементы теории чисел и модулярной арифметики, а также основные математические операции, применяемые при реализации современных криптографических систем и функций хэширования.

2.4. Порядок выполнения работы

2.4.1. Моделирование функции хэширования на основе алгоритма симметричного блочного шифрования

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить необходимые обучающие и вспомогательные программы, активировать их информационно-справочные системы.

2. В соответствии с вариантом индивидуального задания составить схему функции хэширования на основе алгоритма симметричного блочного шифрования.

3. Используя обучающую программу (шифратор) по выбранному алгоритму симметричного блочного шифрования, апробировать процесс вычисления хэш-значения для текста, определенного вариантом индивидуального задания. Сохранить исходный текст и его двоичное представление, а также полученное хэш-значение в двоичном и шестнадцатеричном виде на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе.

4. Исследовать влияние искажений исходного текста, подлежащего хэшированию, на вид его хэш-значения. Вычислить хэш-значение модифицированного текста и сравнить его с хэш-значением немодифицированного текста.

Сохранить двоичное представление модифицированного текста и полученное для него хэш-значение в двоичном и шестнадцатеричном виде на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе.

Вариант индивидуального задания для построения схемы функции хэширования определяется по предпоследней цифре (i) номера зачетной книжки в соответствии с табл. 8.

Таблица 8

i	Функция хэширования
0	$z_i = E_{zi-1}(m_i) \oplus z_{i-1} \oplus m_i$
1	$z_i = E_{zi-1}(m_i \oplus z_{i-1}) \oplus m_i$
2	$z_i = E_{mi}(z_{i-1}) \oplus z_{i-1}$
3	$z_i = E_{mi}(m_i \oplus z_{i-1}) \oplus m_i \oplus z_{i-1}$
4	$z_i = E_{mi}(z_{i-1}) \oplus m_i \oplus z_{i-1}$
5	$z_i = E_{mi}(m_i \oplus z_{i-1}) \oplus z_{i-1}$
6	$z_i = E_{mi \oplus zi-1}(m_i) \oplus m_i$
7	$z_i = E_{mi \oplus zi-1}(z_{i-1}) \oplus z_{i-1}$
8	$z_i = E_{mi \oplus zi-1}(m_i) \oplus z_{i-1}$
9	$z_i = E_{mi \oplus zi-1}(z_{i-1}) \oplus m_i$

Примеры построения схемы функции хэширования приведены на рис. 2.4 и рис. 2.5.

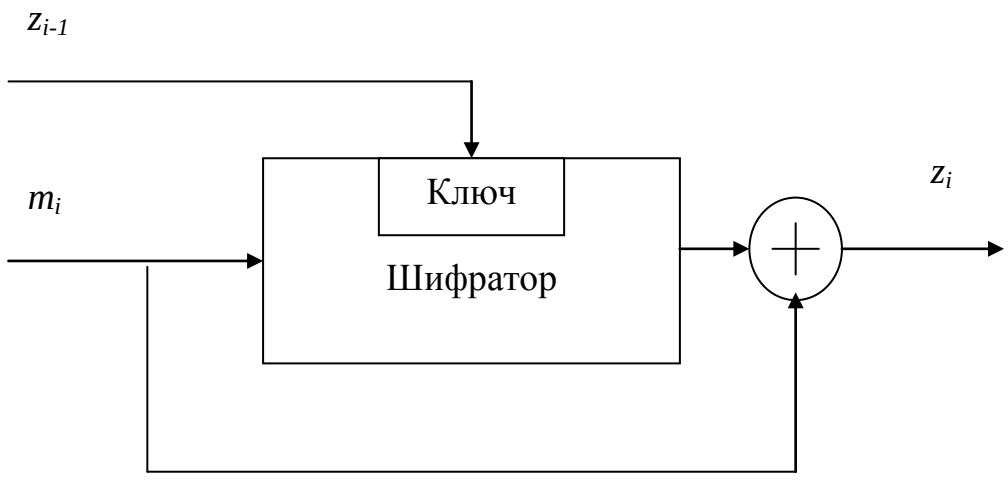


Рис. 2.4. Схема функции хэширования $z_i = E_{zi-1}(m_i) \oplus m_i$

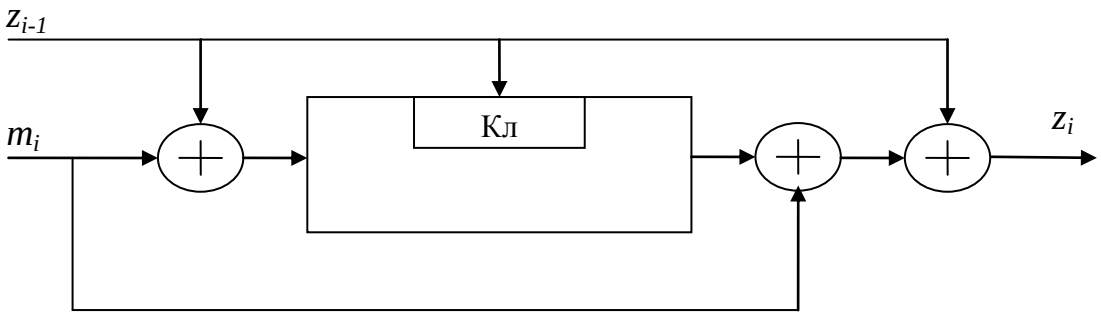


Рис. 2.5. Схема функции хэширования $z_i = E$

Вариант текста, подлежащего хэшированию, определяется по последней (j) цифре номера зачетной книжки в соответствии с табл. 9. Перед хэшированием буквенный текст представляется в виде двоичной последовательности (блока данных) в соответствии с кодом ASCII (КОИ–8).

Таблица 9

j	Текст, подлежащий хэшированию
0	КРИПТОГРАФИЯ
1	ХЭШИРОВАНИЕ
2	ПРЕОБРАЗОВАНИЕ
3	ИМИТОВСТАВКА
4	СЕРТИФИКАЦИЯ
5	ГАММИРОВАНИЕ
6	АУТЕНТИФИКАЦИЯ
7	КРИПТОГРАММА
8	МОДИФИКАЦИЯ
9	БЕЗОПАСНОСТЬ

При вычислении хэш-значения текста следует использовать начальное хэш-значение z_0, соответствующее варианту индивидуального задания, указанному в табл. 10. Номер варианта a вычисляется как

$$a = (i + j) \; mod \; 10,$$

где i – предпоследняя цифра номера зачетной книжки; j – последняя цифра номера зачетной книжки. В целях компактности в табл. 3 начальные хэш-значения z_0 записаны в шестнадцатеричном виде. Перед вычислением хэш-значения текста их следует преобразовать в 64-битовые двоичные последовательности.

Таблица 10

a	Начальное хэш-значение z_0
0	428A2F98D728AE22
1	7137449123EF65CD
2	B5C0FBCFEC4D3D2F
3	*E9B5DBA58189DBBC*
4	3956C25BF348B538
5	59F111F1B605D019
6	923F82A4AF194F9B
7	AB1C5ED5DA6D8118
8	D807AA98A3030242
9	12835B0145706FBE

Алгоритм (стандарт) симметричного блочного шифрования, используемого для практической реализации построенной функции хэширования, определяется по значению *b* в соответствии с табл. 11. Значение *b* вычисляется как

$$b = (i - j) \ mod \ 3,$$

где *i* – предпоследняя цифра номера зачетной книжки;

j – последняя цифра номера зачетной книжки.

Таблица 11

b	Стандарт симметричного шифрования
0	ГОСТ 28147-89
1	DES
2	AES (Rijndael)

В случае необходимости следует адаптировать составленную схему функции хэширования к выбранному стандарту симметричного блочного шифрования, увеличив длину начального хэш-значения z_0 (раундового хэш-значения z_i) и текста, подлежащего хэшированию, посредством дополнения нулями их двоичных представлений (со стороны старших разрядов).

Полученное двоичное хэш-значение всего текста представить в шестнадцатеричном виде.

2.4.2. Исследование функции хэширования по ГОСТ Р 34.11–94

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея описания и блок-схемы основных процедур и преобразований по ГОСТ Р 34.11–94.

3. Используя обучающую программу, апробировать процесс вычисления хэш-значения для различных вариантов текста:

а) ввести в режиме ручного ввода текст для хэширования длиной не менее 64 символов (512 бит) или выбрать его из имеющихся в обучающей программе вариантов, осуществить его разбиение на 256-битовые последовательности m_i;

б) ввести в режиме ручного ввода начальное хэш-значение z_0 (стартовый вектор хэширования) или выбрать его из имеющихся в обучающей программе вариантов;

в) выполнить процедуру генерации 4-х 256-битовых ключей криптографического преобразования, вывести их на экран дисплея;

г) выполнить на полученных ключах криптографическое преобразование 64-битовых блоков хэш-значения z_{i-1} с использованием алгоритма ГОСТ 28147–89 в режиме простой замены, получить и вывести на экран дисплея 256-битовую результирующую последовательность s;

д) выполнить перемешивающее преобразование последовательностей s, z_{i-1} и m_i , вывести полученное значение z_i на экран дисплея;

е) выполнить вычисление хэш-значения для всего исходного текста, вывести его на экран дисплея;

ж) убедиться в изменении полученного хэш-значения при модификации введенного текста, сравнивая хэш-значения, полученные для исходного и модифицированного текстов;

з) повторить пункты а–ж для новых текстов различной длины и стартового вектора хэширования;

и) выполнить пункты а–ж для оригинальных открытого текста длиной не менее 64 символов (512 бит) и стартового вектора хэширования, отличных от вариантов, имеющихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе полученные результаты по всем этапам хэширования.

2.4.3. Исследование электронной цифровой подписи по алгоритму Эль-Гамаля (EGSA)

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея описание и блок-схему алгоритма EGSA, правила вычисления открытых (для проверки) и закрытых (для формирования) ключей электронной цифровой подписи (ЭЦП).

3. Используя обучающую программу, апробировать процесс формирования ЭЦП для различных вариантов текста на различных криптографических ключах по алгоритму EGSA:

а) ввести в режиме ручного ввода текст, подлежащий защите ЭЦП, длиной не более 240 символов или выбрать его из имеющихся в обучающей программе вариантов;

б) выполнить процедуру вычисления и вывести на экран дисплея открытые и закрытые (секретные) параметры криптографического преобразования или ввести их в режиме ручного ввода (или выбрать их из имеющихся в обучающей программе вариантов);

в) представить введенный текст как последовательность чисел в соответствии с выбранным модулем криптографического преобразования;

г) выполнить процесс вычисления хэш-значения и ЭЦП введенного текста, получить результаты по всем этапам формирования ЭЦП на экране дисплея;

д) выполнить процесс проверки соответствия ЭЦП принятому тексту (подлинности и целостности электронного документа);

е) исследовать механизм обеспечения подлинности и целостности электронного документа на основе ЭЦП посредством внесения различных искажений в текст документа, его хэш-значение и ЭЦП;

ж) убедиться в корректности работы программы, правильности выполненных вычислений, операций и преобразований;

з) повторить пункты а–ж для новых текстов и параметров ЭЦП;

и) выполнить пункты а–ж для оригинальных открытого текста и параметров ЭЦП, отличных от вариантов, содержащихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе открытый текст, ключи ЭЦП и полученные результаты по всем этапам формирования и проверки подлинности ЭЦП.

4. В соответствии с вариантом индивидуального задания при помощи калькулятора (не используя обучающую программу) выполнить самостоятель-

ное вычисление открытого ключа Y и ЭЦП $S = (a, b)$ по простейшей реализации алгоритма EGSA.

Исходные значения чисел P и G, а также хэш-значение z документа m определяются по предпоследней (i) цифре номера зачетной книжки в соответствии с табл. 12. Секретный ключ X для подписывания документа m и целое число k определяются по последней (j) цифре номера зачетной книжки в соответствии с табл. 13.

Таблица 12

i	P	G	z
0	29	28	27
1	31	30	29
2	37	32	33
3	41	34	35
4	43	36	38
5	53	38	40
6	59	40	45
7	61	42	50
8	71	44	52
9	73	46	55

Таблица 13

j	x	k
0	24	23
1	26	19
2	26	17
3	25	23
4	27	19
5	27	17
6	26	23
7	28	19
8	28	17
9	27	23

Для полученных значений Y, $S = (a, b)$ вычислить

$$A = Y^a \cdot a^b \ (mod\ P)$$

и проверить справедливость соотношения

$$Y^a \cdot a^b \ (mod\ P) = G^z \ (mod\ P).$$

2.4.4. Исследование электронной цифровой подписи по ГОСТ Р 34.10-94 (ГОСТ Р 34.10-01)

1. Уточнить у преподавателя состав используемых обучающих (вспомогательных) программ и аппаратных средств. При необходимости, под руководством преподавателя, установить (подключить) их на (к) ПЭВМ. По указанию преподавателя загрузить обучающие и вспомогательные программы.

2. Активировать информационно-справочную систему обучающей программы. Вывести на экран дисплея блок-схему алгоритма ГОСТ Р 34.10–94 (ГОСТ Р 34.10–01), а также правила и описания основных процедур и преобразований.

3. Используя обучающую программу, апробировать процесс формирования ЭЦП для различных вариантов текста:

а) ввести в режиме ручного ввода текст для шифрования длиной не менее 64 символов (512 бит) или выбрать его из имеющихся в обучающей программе вариантов;

б) ввести в режиме ручного ввода исходные числовые значения, необходимые для вычисления закрытого (секретного) и открытого ключей ЭЦП или выбрать их из имеющихся в обучающей программе вариантов;

в) вычислить хэш-значение для введенного текста (используя обучающую программу по ГОСТ Р 34.11–94);

г) выполнить процесс формирования ЭЦП для введенного текста, получить результаты по всем этапам формирования ЭЦП на экране дисплея;

д) выполнить процесс проверки соответствия ЭЦП введенному тексту, получить результаты по всем этапам проверки ЭЦП на экране дисплея;

е) внести изменения в исходный текст, выполнить процесс проверки ЭЦП для модифицированного текста, убедиться в несоответствии ЭЦП модифицированному тексту;

ж) повторить пункты а–е для текстов различной длины и новых исходных числовых значений для формирования ЭЦП;

з) выполнить пункты а–е для оригинальных текста длиной не менее 64 символов (512 бит) и исходных числовых значений для формирования ЭЦП, отличных от вариантов, имеющихся в обучающей программе. Сохранить на гибком магнитном накопителе (дискете) для использования в отчете по лабораторной работе полученные результаты по всем этапам формирования и проверки подлинности ЭЦП.

4. Провести сеанс формирования ЭЦП и проверки ее подлинности по следующему протоколу:

а) студент А – подписант электронного документа, самостоятельно вычисляет ключи для формирования и проверки подлинности ЭЦП;

б) студент А передает по открытому каналу связи (публично объявляет, записывает в тетрадь, передает по локальной сети, копирует на дискету) ключ проверки подлинности ЭЦП студенту В. Секретный ключ для формирования ЭЦП сохраняется им в тайне от других студентов, выполняющих лабораторную работу;

в) студент А составляет электронный документ $m \in M$, вычисляет для него хэш-значение и ЭЦП;

г) студент А передает по открытому каналу связи (по локальной сети, копирует на дискету) в адрес студента В электронный документ с ЭЦП;

д) студент В – получатель электронного документа, защищенного ЭЦП, используя известную функцию хэширования и открытый ключ ЭЦП, проверяет ее подлинность и убеждается в целостности полученного электронного документа;

е) студент С – выполняя роль "злоумышленника", на этапе передачи электронного документа с ЭЦП от студента А к студенту В осуществляет его модификацию и/или подделку ЭЦП посредством подбора секретно-

го ключа для ее вычисления. Полученный электронный документ с ЭЦП передается студенту В;

ж) студент В, осуществляя проверку ЭЦП, убеждается в ее несоответствии полученному электронному документу. Результаты исследования объявляются студентам А и С.

2.5. Контрольные вопросы

1. Для каких целей служит функция хэширования и какими основными свойствами она обладает.
2. В чем заключаются методы реализации функции хэширования, основанные на алгоритмах симметричного блочного шифрования.
3. В чем заключаются методы реализации функции хэширования, основанные на числовых корректирующих кодах.
4. Какие основные параметры у стандартов шифрования ГОСТ 28147–89, DES, Rijndael (длина ключа, длина шифруемого блока, количество раундов (циклов) шифрования).
5. На каких математических принципах и задачах (проблемах) основаны ЭЦП по алгоритму EGSA и ГОСТ Р 34.10–94.
6. На каких математических принципах и задачах (проблемах) основана ЭЦП по ГОСТ Р 34.10–01.
7. Как задается эллиптическая кривая над простым полем. Что называется инвариантом эллиптической кривой. Как определяются коэффициенты эллиптической кривой.
8. Какую длину имеет хэш-значение, полученное по ГОСТ Р 34.10–94 (ГОСТ Р 34.10−01).
9. Что называется простым числом, взаимно простыми числами, вычетом числа по некоторому модулю. В чем заключается основная теорема арифметики, алгоритм Евклида, малая теорема Ферма.
10. Как реализуется функция хэширования по ГОСТ Р 34.11–94. В чем ее преимущество по сравнению с другими типами хэш-функций.
11. От чего зависит криптостойкость ЭЦП на основе алгоритма EGSA.
12. От чего зависит криптостойкость ЭЦП по ГОСТ Р 34.10–01.
13. Какие длины ключей (исходных значений) рекомендованы для использования на практике при формировании ЭЦП по алгоритму EGSA и ГОСТ Р 34.10–94.
14. Каким условиям должны удовлетворять параметры ЭЦП по ГОСТ Р 34.10–01.
15. Какие отличительные особенности, достоинства и недостатки характерны для ЭЦП по ГОСТ Р 34.10–94 и ГОСТ Р 34.10–01.
16. Каким нормативным правовым актом в Российской Федерации определены правовые условия использования ЭЦП в электронных документах.

2.6. Содержание отчета

Отчет по выполненной лабораторной работе должен содержать:

1. Тему и цель работы.
2. Схему функции хэширования с параметрами, соответствующими варианту индивидуального задания.
3. Схемы алгоритмов исследованных функции хэширования и ЭЦП.
4. Результаты, полученные при апробировании процессов хэширования и формирования ЭЦП с использованием обучающих программ.
5. Результаты самостоятельного вычисления ЭЦП по алгоритму EGSA в соответствии с вариантом индивидуального задания.
6. Анализ полученных результатов и выводы по лабораторной работе.
7. Возможные предложения по использованию исследованных методов защиты электронных документов на практике и/или совершенствованию обучающих программ.

Литература

Основная

1. Терентьев А.И. Введение в информационную безопасность: учеб. пособие. – М.: МГТУ ГА, 2001.

Дополнительная

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие. – М.: Гелиос АРВ, 2001.
3. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебный курс. – 2-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2002.
5. Введение в криптографию/ под общ. ред. В.В.Ященко. – М.: МЦНМО, "ЧеРо", 1998.
6. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001.
7. Фороузан Б.А. Криптография и безопасность сетей: учеб. пособие/ пер. с англ. под ред. А.Н.Берлина. – М.: Интернет-Университет информационных технологий: БИНОМ. Лаборатория знаний, 2010.
8. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография: учебники для вузов. – СПб.: Издательство "Лань", 2001.
9. Панасенко С.П. Алгоритмы шифрования: специальный справочник. – СПб.: БХВ-Петербург, 2009.
10. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ под ред. В.Ф.Шаньгина. – 2-е изд., перераб. и

доп. – М.: Радио и связь, 2001.
11. Федеральный закон от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи" (в редакции от 10 июля 2012 года).
12. Чмора А.Л. Современная прикладная криптография. - 2-е изд. стереотип. – М.: Гелиос АРВ, 2002.

Содержание