УДК 004.4+004.056

СИСТЕМА ГИБРИДНОГО ШИФРОВАНИЯ/ДЕШИФРОВАНИЯ ДАННЫХ

Охтиенко М.П., студент гр.881072

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Прянишников Н.А. – начальник ОТИС ИИТ БГУИР

Аннотация. В статье рассматриваются криптографические методы и средства обеспечения информационной безопасности, а также алгоритмы симметричного/ассиметричного шифрования, эффективность которых объединяется в системе гибридного шифрования/дешифрования данных. Описывается архитектура гибридной криптосистемы, основные компоненты, их отношения и как они взаимодействуют друг с другом.

Ключевые слова. Криптография, гибридная криптосистема, шифрование, алгоритм, модульная архитектура; информационная безопасность, информационные технологии.

Введение. Современные методы накопления, обработки информации способствовали появлению угроз, связанных с возможностью потери, раскрытия, модификации данных. Важнейшей характеристикой любой компьютерной системы независимо от ее сложности и назначения становится безопасность циркулирующей в ней информации. Информационная безопасность – это состояние защищенности обрабатываемых, хранимых и передаваемых в ИТС данных от несанкционированного доступа, модификации, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности [1].

Основные задачи защиты информации: целостность; конфиденциальность; достоверность; обеспечение оперативности доступа.

Назначение средств защиты целостности – гарантировать, что принятые данные в точности соответствуют отправленным и не содержат изъятий, дополнений, повторов и изменений в порядке следования фрагментов. Может контролироваться целостность сегментов данных, так и данных в целом, а также потока данных. Дополнительной функцией соответствующих средств может являться и восстановление искаженной информации.

Назначение средств обеспечения конфиденциальности – защитить информацию от атак. Информационная безопасность сталкивается с внешними и внутренними преднамеренными угрозами, направленными на хищение данных.

Эффективными средствами защиты, как от внешних угроз, так и от внутренних, являются: введение системы паролей пользователей, применение для особо важной информации криптографических методов защиты (шифрование), установка систем защиты от утечек информации, защита информации от копирования.

Назначение средств обеспечения доступности – обеспечить своевременный доступ пользователей к необходимой им информации и ресурсам информационной системы. Задача обеспечения доступности – комплексная, для ее решения применяются как методы защиты от НСД, так и специализированные методы защиты от разрушающих программных воздействий.

Основные задачи, решаемые в рамках информационной безопасности по отношению к работоспособности ИТС, должны обеспечивать защиту от:

— нарушения функционирования телекоммуникационной системы, выражающегося в воздействии на информационные каналы, управления и удаленной загрузки БД;

— разрушения встраиваемых и внешних средств защиты;

— несанкционированного доступа к информационным ресурсам, приводящих к утечке данных, нарушению целостности данных, изменению функционирования подсистем распределения информации, доступности баз данных.

Тенденции развития информационных технологий дают все основания сделать вывод о постоянном возрастании роли криптографических методов при решении задач аутентификации в распределенных системах, обеспечения секретности данных при их передаче по открытым каналам связи. Основу криптографических методов составляет криптографическое преобразования информации, производимого по определенным математическим методам, с целью исключить доступ к данной информации посторонних пользователей, а также с целью обеспечения невозможности бесконтрольного изменения информации [2].

Применение криптографических методов защиты обеспечивает решение основных задач информационной безопасности:

— конфиденциальность;

— скрытия информации от неавторизованных пользователей;

— предотвращение изменения информации при передаче или хранении;

— целостность;

— идентифицируемость.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Основная часть. Разработка криптографических систем строиться на нескольких фундаментальных принципах. Один из них – принцип Керкгоффса, согласна которому в засекреченном виде держится только определенный набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен иметь открытый исходный код. Системы шифрования/дешифрования данных необходимо строить так, чтобы их криптографическая сторона была известна и единственным неизвестным элементов являлся криптографический ключ, который используется в данной системе.

Криптографическая система состоит из следующих компонент:

– пространства:

a) открытых данных M;

b) ключей K;

c) зашифрованных данных C;

– функции:

a) шифрования данных: E_k : M → C;

b) дешифрования данных: D_k : C → M.

Гибридной криптосистемой принято называть способ передачи большого объема зашифрованных данных, при котором данные шифруются секретным ключом с применением симметричного алгоритма, а сам ключ передается зашифрованным асимметричным шифром. Такой способ получил широкое распространение за то, что он включает в себя преимущества как симметричной, так и асимметричной криптографии[3]. Большой блок данных шифруется очень быстрым симметричным алгоритмом, а ключ шифрования передается надежно зашифрованным с помощью асимметричного алгоритма, и это решает проблему распределения ключей, свойственную только симметричным методам. Схема гибридной криптосистемы представлена на рисунке 1.

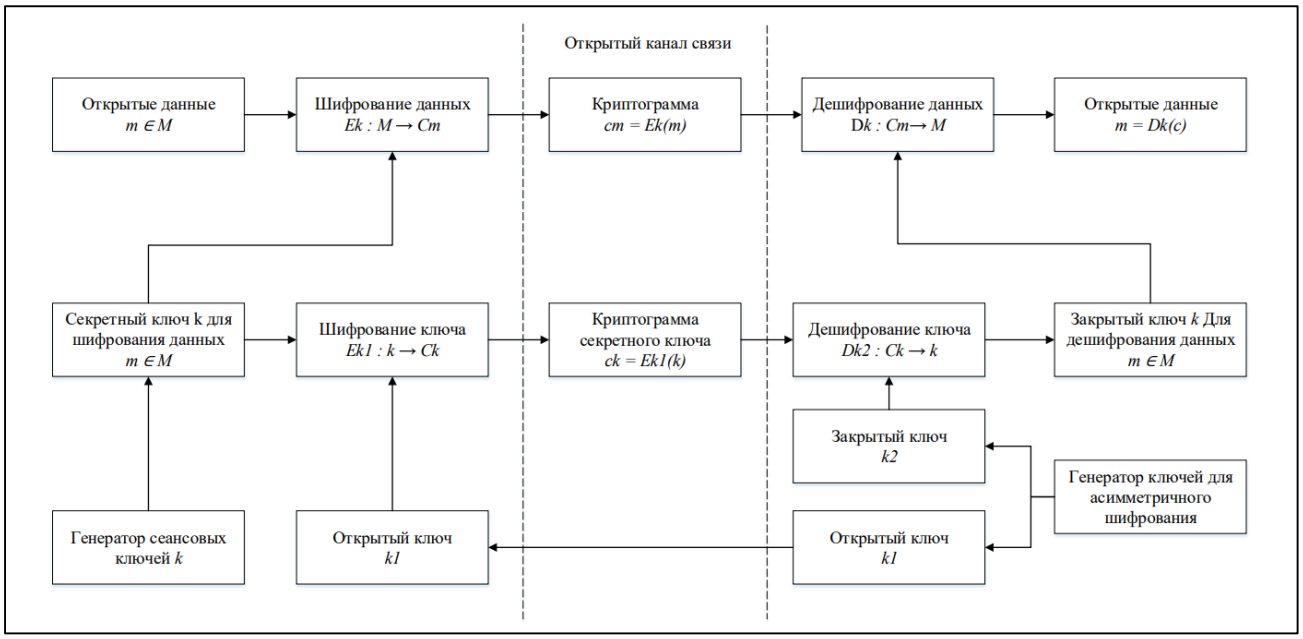

Рисунок 1 – Схема гибридной криптографической системы

Для повышения криптостойкости в гибридной криптографической системе для каждого сеанса секретной связи 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, то их криптостойкость должна быть существенно выше, чем у сеансового секретного ключа симметричного шифрования, поскольку при дискредитации, злоумышленник получит возможность расшифровывать передаваемые сеансовые секретные ключи и соответственно зашифрованные на их основе данные.

Архитектура гибридной криптосистемы описывает основные компоненты системы, их отношения и как они взаимодействуют друг с другом. Архитектура служит чертежом, предоставляющим абстракцию для управления сложностью системы, описывающим отношения (структуру) и механизм взаимодействия между компонентами. Представляет собой

структурированное решение, которое отвечает всем эксплуатационным и техническим требованиям, учитывая при этом установленную планку производительности и безопасности.

Главная цель при проектировании – выявление требований, которые влияют на структуру приложения. Продуманная архитектура снижает бизнес-риски и технические издержки. Модульная архитектура, малая связность и высокая сопряженность позволяют писать программное обеспечение обладающие большой гибкостью к изменениям и большим процентом повторного использования кода.

Модульная архитектура программного обеспечения достигается с помощью декомпозиции. Система делиться на крупные подсистемы, которые в общих чертах описывают ее работу. После полученные подсистемы анализируются и выделяются в подмодули либо объекты. Необходимо соблюдать ограничение в 2-7 модулей на один иерархический уровень. Модули выделяются исходя из тех задач, которые решает система. Подзадачи, которые могут решаться независимо друг от друга, являются конечной целью разбиения главной задачи. Модуль создается с целью решения лишь одной задачи и выполнения соответствующей функции. Важнейшей метрикой хорошей декомпозиции будет малая связность кода между модулями, которая позволяет легко вносить нужные изменения, не заботясь о зависимостях. И высокая сопряженность внутри самих модулей, свидетельствующая о фокусе на одной конкретной задаче. Для изменения высоко сопряженного модуля должна быть только одна причина. Хорошо спроектированный модуль реализует лишь одну функцию, которую выполняет только внутри себя. Подчиняется принципу Input Process Output (IPO) – получив один набор данных он возвращает тоже только один набор выходных данных. Результат работы модуля определяется только входными данными и индифферентен к работе других модулей. Обмен информацией с другими модулями минимизирован.

Архитектура разрабатываемой системы «Гибридного шифрования/дешифрования данных» представлена на рисунке 2.

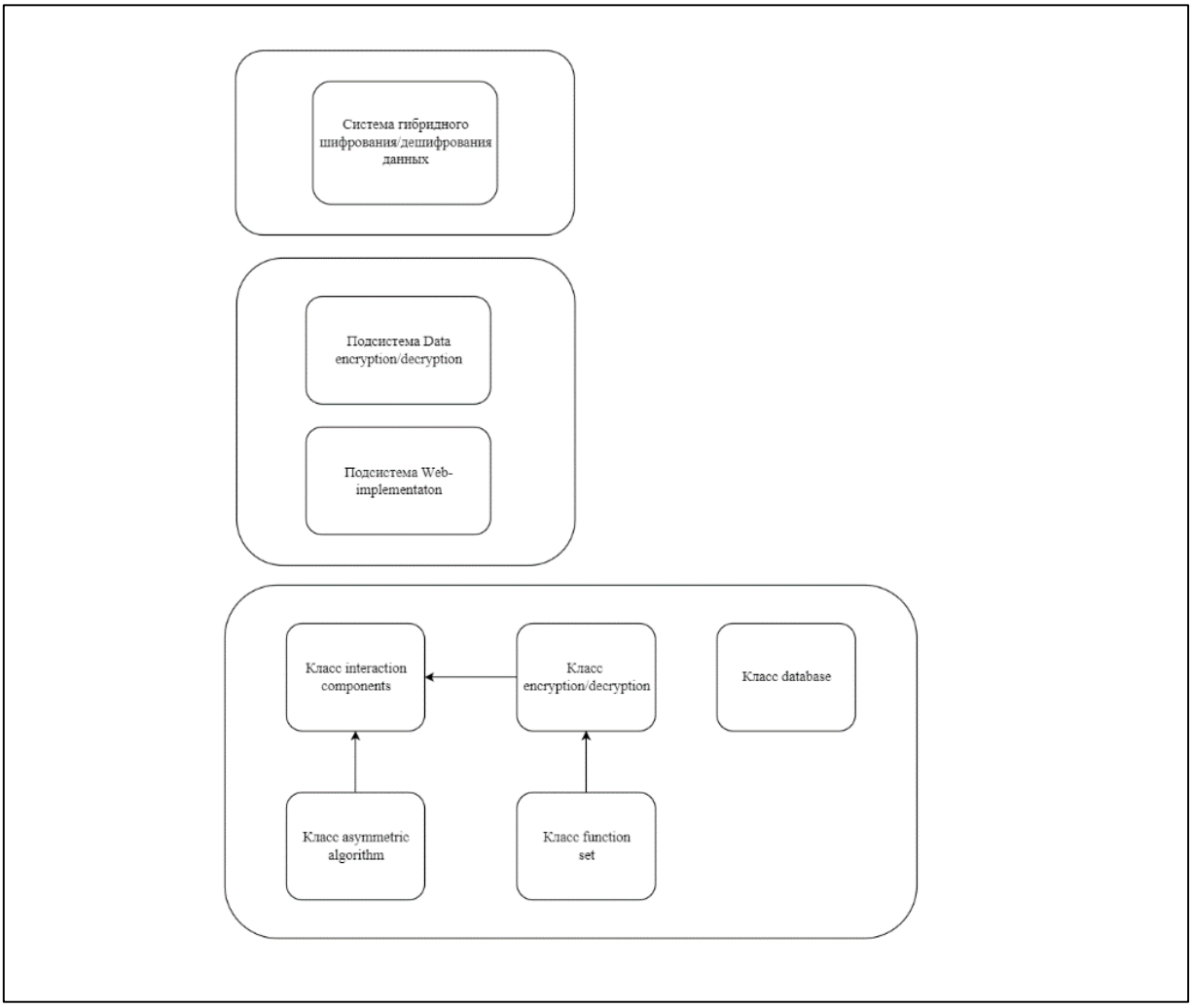

Рисунок 2 – Архитектура гибридной криптосистемы

Система «Гибридного шифрования/дешифрования данных» декомпозируется на подсистемы: Data encryption/decryption и Web-implementaton.

В подсистеме Data encryption/decryption выделяются следующие классы:

— encryption/decryption;

— function set;
— asymmetric algorithm;
— interaction components.

Класс encryption/decryption реализует алгоритм шифрования, который базируется на математических функциях. Функционально шифрование похоже на дешифрование, по этой причине выделять дешифрование в отдельный класс не следует. Класс является законченным и может использоваться повторно.

В класс function set выделяются следующие подмодули:

— генерация ключа;
— генерация псевдослучайных последовательностей;
— установка текущего ключа;
— преобразование ключа в необходимый для алгоритма вид;
— подача и накопление выходных данных;
— запись выходных данных в промежуточный буфер.

Данные, предоставляемые на вход и получаемые на выходе подаются в бинарном виде и для их хранения не нужно использовать специальные структуры. Ключ зависит от алгоритма шифрования. Он имеет определенные алгоритмом шифрования требования. Преобразование ключа в необходимый вид – это детали имплементации конкретного алгоритма шифрования. Ключ всегда поступает на вход в формате строки закодированной в base64.

Класс asymmetric algorithm реализует алгоритм шифрования/дешифрования ключа, который базируется на односторонних математических функциях.

В подсистеме Web-implementaton выделяется класс database, обеспечивающий взаимодействие с базой данных, в которой хранятся пользовательские данные, которые используются при авторизации в системе «Гибридного шифрования/дешифрования данных».

Взаимодействие классов происходит в interaction components. Для чтения/записи данных используется стандартные функции среды разработки.

Заключение. Представленное программное обеспечения «Система гибридного шифрования/дешифрования данных» направленно на обеспечение конфиденциальности информации путем шифрования передаваемых и хранимых данных. Гибридная криптосистема разработана с целью обеспечения секретности передаваемых данных, их аутентичности и целостности.

Список использованных источников:

1. Анин, Б. Ю. Защита компьютерной информации / Б. Ю. Анин. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.: ил.

2. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

3. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М.: ДМК, 2008. – 448 с.: ил.

UDC 004.4+004.056

HYBRID DATA ENCRYPTION/DECRYPTION SYSTEM

Okhtienko M.P.

Institute of Information Technologies of the Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Pryanishnikov N.A. – head of DTIS IIT BSUIR

Annotation. The article deals with cryptographic methods and information security tools, as well as symmetric/asymmetric encryption algorithms, the effectiveness of which is combined in a hybrid data encryption/decryption system. The architecture of the hybrid cryptosystem, the main components, their relationships and how they interact with each other are described.

Keywords. Cryptography, hybrid cryptosystem, encryption, algorithm, modular architecture; information security, information technology.