Дисциплина

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

КУРСОВАЯ РАБОТА «СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ»

СОДЕРЖАНИЕ

Обмен документами в электронном виде возможен лишь в том случае, если обеспечивается их конфиденциальность, надежная защита от подделки или несанкционированного изменения, гарантирована доставка адресату, имеется возможность разрешения споров, связанных с фальсификацией сообщений и отказом от авторства.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

В современном программном обеспечении (ПО) криптоалгоритмы широко применяются не только для задач шифрования данных, но и для аутентификации и проверки целостности. На сегодняшний день существуют хорошо известные и апробированные криптоалгоритмы (как с симметричными, так и несимметричными ключами), криптостойкость которых либо доказана математически, либо основана на необходимости решения математически сложной задачи (факторизации, дискретного логарифмирования и т.п.).

ЦЕЛЬ РАБОТЫ

Изучение одного из предложенных алгоритмов.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Принципы криптографической защиты информации

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблемы конфиденциальности (путем лишения противника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи). Проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рисунке 1.

Отправитель генерирует открытый текст исходного сообщения M , которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения M , отправитель шифрует его с помощью обратимого преобразования $Ек(M)$ и получает шифртекст (или криптограмму) $C = Ек(M)$, который отправляет получателю. Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D = E^{-1}$ и получает исходное сообщение в виде открытого текста M :

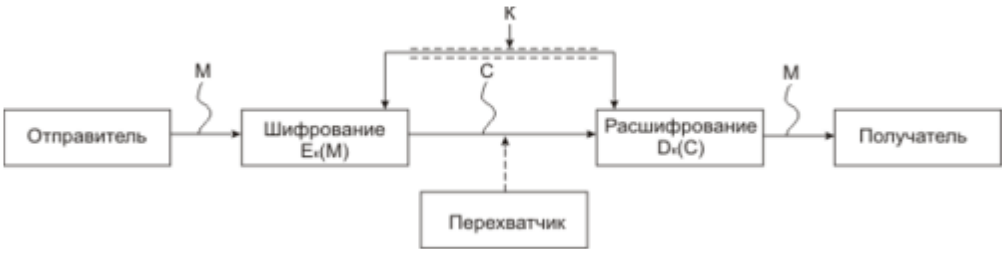

Рисунок 1 - Обобщённая схема криптосистемы.

Преобразование $Ек$ выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом K. Криптосистема имеет разные варианты

реализации: набор инструкции, аппаратные средства, комплекс программ компьютера, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа *К*.

Говоря более формально, криптографическая система - это однопараметрическое семейство обратимых преобразований из пространства *М* сообщений открытого текста в пространство *С* шифрованных текстов. Параметр *К* (ключ) выбирается из конечного множества К, называемого пространством ключей.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования.

Это важное свойство функции преобразования определяет два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двухключевые) криптосистемы (с открытым ключом).

Схема симметричной криптосистемы с одним секретным ключом показана на рисунке 1. В ней используются одинаковые секретные ключи в блоке шифрования и блоке расшифрования.

Обобщенная схема асимметричной криптосистемы с двумя разными ключами *К1* и *К2* показана на рисунке 2.

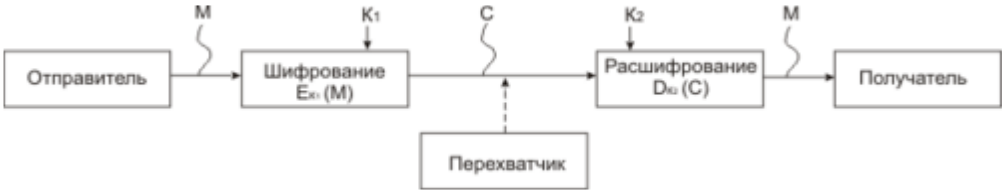

Рисунок 2 - Обобщённая схема ассиметричной криптосистемы с открытым ключом.

В этой криптосистеме один из ключей является открытым, а другой - секретным.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, такому, как курьерская служба. На рис.1 этот канал показан "экранированной" линией. Существуют и другие способы распределения секретных ключей. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.

Существуют два основных современных класса шифров: поточные и блочные шифры.

ОБЪЕКТЫ И СРЕДСТВА ИССЛЕДОВАНИЯ

Объектами исследования являются алгоритмы шифрования, алгоритмы электронной подписи и соответствующие стандарты.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

В данной работе необходимо изучить работу и подготовить отчет по одному из предложенных алгоритмов в соответствии с вариантом задания.

1. Тщательно изучить заданный криптографический алгоритм.
2. Составить свое описание данного криптографического алгоритма.
3. Составить алгоритм работы программы, выполняющей шифрование и расшифровывание по данному методу. Алгоритм показать преподавателю.
4. Придумать тестовый пример.
5. Реализовать предложенный алгоритм программно, протестировать, работающую программу продемонстрировать преподавателю.
6. Составить отчет.

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист с указанием варианта.
2. Подробное описание заданного криптографического алгоритма (от 10 страниц).
3. Блок-схема алгоритма работы.
4. Тестовый пример.
5. Код программы.
6. Иллюстрация результата работы программы.
7. Список использованной литературы.

ВАРИАНТЫ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Вариант	Алгоритм
1	Реализация алгоритма Ривеста.
2	Реализация алгоритма DES – общий.
3	Реализация алгоритма DES – режим сцепления блоков в CBC шифре.
4	Реализация алгоритма DES – режим работы ECB (электронный блокнот).
5	Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.
6	Реализация алгоритма DES – OFB – обратная связь по выходу.
7	Алгоритм формирования ключей в процессе функционирования DES.
8	Алгоритм федерального стандарта x9.9.
9	Алгоритм криптографического преобразования – общий.
10	Алгоритм криптографического преобразования в режиме простой замены.

11	Алгоритм криптографического преобразования в режиме гаммирования.
12	Алгоритм криптографического преобразования в режиме гаммирования с обратной связью
13	Алгоритм криптографического преобразования в режиме имитовставки.
14	Алгоритм RSA – общий.
15	Алгоритм, основанный на схеме шифрования Эль Гамаля.
16	Алгоритм, основанный на комбинированном методе шифрования
17	Алгоритм, основанный на комбинированном методе шифрования (симметричные системы с секретным ключом + ассиметричные системы с открытым ключом) – общий.
18	Алгоритм открытого распределения ключей Диффи-Хеллмана
19	Алгоритм на основе протокола Kerberos (Цербер) с применением алгоритма DES и других.
20	Алгоритм цифровой подписи RSA.
21	Алгоритм цифровой подписи DSA.
22	Отечественный стандарт цифровой подписи ГОСТ Р34.10-94 (близок к алгоритму DSA).
23	Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».
24	Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».
25	Реализация модели защиты ОС – Харрисона-Руззо-Ульмана (модель доступа к данным).
26	Реализация матричной модели доступа.
27	Реализация алгоритма Ривеста.
28	Реализация алгоритма DES – общий.
29	Реализация алгоритма DES – режим сцепления блоков в CBC шифре.
30	Реализация алгоритма DES – режим работы ECB (электронный блокнот).
31	Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.
32	Реализация алгоритма DES – OFB – обратная связь по выходу.
33	Алгоритм формирования ключей в процессе функционирования DES.
34	Алгоритм федерального стандарта x9.9.
35	Алгоритм криптографического преобразования – общий.