Васяева Д.О.
Научный руководитель: к.т.н., доцент каф. ФПМ К.В. Макаров
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: v-dasha95@yandex.ru

Сравнительный анализ алгоритмов симметричного шифрования

Многие предприятия не пользуются преимуществами технологий шифрования, опасаясь, что это слишком сложно. Шифрование особо ценных данных ненамного сложнее, чем запуск антивирусного сканера или резервного копирования данных.

Шифрование данных – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит способом соблюдения конфиденциальности передаваемой информации.

Причины потери данных:

1. Отправка серверов или жестких дисков в ремонт;
2. Перевозка компьютеров из одного офиса в другой, например, при переезде;
3. Утилизация компьютеров, серверов, жестких дисков и лент;
4. Хранение магнитных лент в специальном депозитарии (off-site storage);
5. Перевозка ленты, например, в депозитарий;
6. Кража или потеря жестких дисков или лент.

В связи с этим анализ, существующих методов защиты информации является актуальной научно-технической задачей.

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Классическим примером таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

- Простая подстановка
- Одиночная перестановка по ключу
- Гаммирование

Объекты исследования в данной работе – алгоритмы шифрования: простая подстановка, одиночная подстановка по ключу и гаммирование, предмет исследования – использование одного из выше перечисленных алгоритмов шифрования защиты данных.

Целью исследования является обзор анализ и выбор одного из алгоритмов шифрования: простая подстановка, одиночная подстановка по ключу и гаммирование, для реализации его в приложении виртуальная криптографическая лаборатория для защиты данных.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор выше заявленных алгоритмов шифрования.

2. Анализ выбранных методов.
3. Представить результаты исследования.

Обзор алгоритмов шифрования

Одиночная перестановка по ключу

При шифровании простой перестановкой ключевое слово с неповторяющимися символами или цифровой ключ. Число колонок в таблице задаётся количеством символов в ключе, а число строк может быть фиксировано или может задаваться длиной сообщения. Шифруемый текст записывается последовательными строками под символами ключа. Для заполнения пустых клеток (если объём текста меньше ёмкости таблицы) можно использовать любые символы. Затем текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа или в порядке следования цифр, если ключ цифровой. В качестве примера рассмотрим шифрование сообщения: «БУДЬТЕ ОСТОРОЖНЫ С ПРЕДСТАВИТЕЛЕМ ФИРМЫ «СПЕКТР». Применим цифровой ключ - 5 1 8 3 7 4 6 2. Выписывая текст по колонкам, получаем абракадабру: УОРТМССВИТЬОДЛСЕНТМЕБТПИРРОЫАФКТЖСЕПДРЕЕЫ.

Дешифрование выполняется в следующем порядке. Подсчитываем число знаков в зашифрованном тексте и делим на число знаков ключа (41: 8=5 и 1 знак в остатке). Под знаками ключа в соответствующей последовательности записываем вертикально (колонками) символы зашифрованного текста в определенном выше количестве. В каждой колонке по 5 символов, а в одной (первой слева) - 6 символов (5+1 буква в остатке). По строкам таблицы (горизонтально) читаем исходный текст. Выше, в «Истории тайнописи», упоминается шифр называемый в некоторых книгах по криптографии «Сцитала» (наматывание ленты на жезл). Это не что иное, как перестановка по таблице с простым ключом - 1 2 3 4 …

Простая подстановка

Каждая из 33 букв русского алфавита заменяется на другую букву того же алфавита (моноалфавитная подстановка). Такой шифр (одноалфавитная замена) имеет низкую (временную) стойкость, т. к. зашифрованный (закрытый) текст имеет те же статистические характеристики, что и исходный (открытый) - каждая буква имеет свою частоту появления. Поэтому использовать этот метод целесообразно для шифрования только короткого текста.

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Гаммирование

Метод гаммирования состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой.

В потоковых криптосистемах на основе ключа вырабатывается гамма, которая затем накладывается на текст сообщения. Наложение осуществляется посредством сложения по модулю 2 (операции XOR).

Зашифрование производится следующим образом:

$c_i = m_i \otimes k_i$ для i=1,2,3...

где c_i - знак шифротекста;

m_i - знак открытого текста;

k_i - знак ключевой последовательности;

$\otimes$ - сложение по модулю 2.

Поскольку повторное применение операции XOR восстанавливает первоначальное значение, расшифрование производится повторным наложением гаммы:

$m_i = c_i \otimes k_i$ для i=1,2,3...

Преобразование текста осуществляется потоком по мере выработки гаммы. Поэтому поточные шифры подходят для шифрования непрерывных потоков данных - голоса, видео и т.д.

Принцип шифрования гаммированием заключается в генерации бесконечного ключа (гаммы шифра) с помощью датчика псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на исходные данные обратимым образом. Процесс расшифровки данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то зашифрованный текст можно раскрыть только путем прямого перебора.

Сравнительный анализ методов шифрования

После проведенного обзора было выявлено, что шифрование методом простой подставки совершенно не эффективно, так как его можно расшифровать после несложного анализа. Алгоритм одиночной перестановки гораздо надежнее подстановки, но если ключ используется несколько раз, то его можно проанализировать и взломать. Из трех проанализированных методов, алгоритм методом гаммирования является самым эффективным.

Таблица 1. Сравнительный анализ алгоритмов симметричного шифрования

	Простая подстановка	Одиночная перестановка по ключу	Гаммирование
Методы взлома	Шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифр тексте	При своей несложности система легко уязвима. Если злоумышленник имеет шифрованный и соответствующий исходный текст	Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма
Параметры ключа	Число возможных ключей мало	Число возможных ключей ограничено	Длинна шифрующей гаммы должна быть не менее защищаемого сообщения
Передача ключа	Отправитель и получатель должны некоторым тайным образом получить копии секретного ключа и сохранить их в тайне		
Стойкость	Имеет низкую стойкость	Имеет стойкость более высокую чем подстановка	Исходный текст практически невозможно восстановить без ключа
Недостатки	Использовать этот шифр целесообразно только для шифрования коротких текстов	Если ключ используется несколько раз его можно проанализировать и взломать	Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей

Результат

В результате проведенного исследования было выяснено, что из трех выбранных алгоритмов шифрования самым более надежными является алгоритм гаммирования, так как данный алгоритм обладает рядом преимуществ, а именно: имеет высокую криптостойкость (исходный текст не возможно восстановить без ключа), не требует больших вычислительных мощностей, что позволяет использовать его любому лицу, а также прост в использовании.