Список использованных источников

1. Шиманская-Семенова, Т. А. Применение матричных моделей для расчета и анализа электрических сетей / Т. А. Шиманская-Семенова; Белорусский национальный технический университет, Кафедра «Электрические системы». – Минск : БНТУ, 2010. – 148 с.

УДК 378.091

Алгоритмы шифрования данных в C#

Песняк И. М., студент
Нуриллоев К. А., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: преподаватель Михасик Е. И.

Аннотация:
В настоящее время все большую значимость набирает цифровая безопасность и методы криптографического шифрования. В данной статье рассмотрены алгоритмы шифрования, приведены их достоинства и недостатки.

В настоящее время все больше людей начинают задумываться о своей безопасности. Человечество все больше зависимо от компьютеров и все меньше знает о способах защиты своих личных данных от злоумышленников. Конечно, встает вопрос о том, как защитить пользователей и как пользователь может защитить себя. Каждый специалист в сфере компьютерной безопасности может предложить свой способ обезопасить пользователей, используя алгоритмы шифрования. Наука, изучающая алгоритмы шифрования – криптография. Первые шифры появились еще в Древнем Риме, Древнем Египте и Древней Греции. Одним из таких шифров является шифр Цезаря. Суть данного алгоритма в том, что у каждой буквы есть порядковый номер в алфавите, этот номер сдвигался на 3 значения влево. Сейчас существует множество алгоритмов шифрования, в том числе стандартные алгоритмы шифрования, которые дают наибольшую возможную защиту.

Алгоритм шифрования AES был принят в 1997 году как стандарт шифрования вместо алгоритма DES после организованного Институтом стандартов и технологий США открытого конкурса алгоритмов шифрования. В данном конкурсе участвовало 15 алгоритмов шифрования. Конкурс назвали в честь победителя, а именно Advanced Encryption Standard (AES).

Один из претендентов на стандартизованный алгоритм шифрования – Crypton. Данный алгоритм шифрует 128-битные блоки данных, используя ключи шифрования фиксированных алгоритмов – от 0 до 256 битов с кратностью 8 битов. Алгоритм Crypton представляет 128-битный блок шифруемых данных в виде байтового массива размером 4 на 4, над которым производится несколько раундов преобразований. В каждом раунде предполагается последовательное выполнение следующих операций:

1. Табличная замена Y.
2. Линейное преобразование π.
3. Байтовая перестановка τ – служит для преобразования строки данных в столбец данных.
4. Операция σ, представляет собой побитовое сложение всего массива данных с ключом раунда.

В алгоритме используется 12 раундов шифрования. Перед первым раундом алгоритма используется операция σ, а по завершении всех раундов выполняется выходное преобразование φe, которое состоит из последовательных операций τ, πe, τ.

К основным его достоинствам можно отнести:

1. Высокая скорость на всех целевых платформах.
2. Небольшие требования к оперативной памяти.
3. Алгоритм не подвержен атакам во время шифрования и атакам по времени взаимодействия.
4. Быстрое расширение ключа.
5. Возможность выполнения операций параллельно.
6. Размерность – установление разных размеров ключей.

Следующим алгоритмом шифрования, который был отправлен на конкурс AES – Square.

Данный алгоритм интересен по двум основным причинам:

1. Этот алгоритм был разработан теми же специалистами, которые разработали алгоритм Rijndael.

2. Структура Square легла в основу алгоритма Rijandael.

Алгоритм шифрует данные блоками по 128 бит, длина ключа составляет 128 бит. Сами данные выглядят как таблица (4 на 4). Алгоритм состоит из 8 раундов. Каждый раунд состоит из следующих основных шагов и этапов:

1. Линейное преобразование θ, выполняемое раздельно для каждой строки таблицы.

2. Нелинейное преобразование (табличная замена).

3. Байтовая перестановка π преобразует строку в столбец.

4. Операция σ представляет собой побитовое сложение.

Следующим алгоритмом, который был представлен на конкурс AES был алгоритм Twofish. Он разбивает шифруемые данные на четыре 32-битные субблока. Над этими субблоками производится 16 раундов преобразований. У алгоритма нет существенных недостатков. Эксперты конкурса AES отметили лишь один недостаток: сложность алгоритма, которая затрудняет его анализ и реализацию. Данный алгоритм был в финале конкурса AES.

Далее рассмотрим победителя конкурса AES – алгоритм шифрования Rijndael. Структура этого алгоритма практически идентична структуре алгоритма Twofish. Алгоритм AES представляет блок данных в виде двумерного байтового массива размером (4 на 4). Все операции производятся над отдельными байтами массива, которые также независимы от столбцов и строк.

В каждом раунде алгоритма выполняются следующие базовые первичные преобразования:

1. Операция SubBytes, представляющая собой табличную замену каждого байта массива данных.

2. Операция ShiftRows выполняет циклический сдвиг влево всех строк массива данных. Исключением является нулевая строка.

3. Операция MixColumns. Выполняет умножение каждого столбца массива данных.

4. Операция AddRoundKey. Выполнятся наложением на массив данных материала ключа, а именно, на *i*-й столбец массива данных побитовое сложение логической операцией «исключающее или» накладывается на определенное слово расширенного ключа.

По утверждению авторов, Rijndael не подвержен следующим видам криптоаналитических атак:

1. У алгоритма отсутствуют слабые ключи и возможность вскрыть алгоритм с помощью атак на связанных ключах.
2. Алгоритм защищен от дифференциального криптоанализа.
3. Алгоритм не восприимчив к линейному криптоанализу и усеченным дифференциалам.
4. Отсутствует Square-атака (атака на алгоритмы с простейшей структурой называемой «квадрат»).
5. Алгоритм нельзя вскрыть методом интерполяции.

Алгоритм Rijndael оказался одним из самых надежных алгоритмов, представленных на конкурс и через 6 лет он стал стандартом.

Список использованных источников

1. Алгоритмы шифрования? Финалисты конкурса AES. Часть 1. [Электронный ресурс] // ixbt.com. – 2006. – Режим доступа: https://www.ixbt.com/soft/alg-encryption-aes.shtml. – Дата доступа: 16.10.2022.
2. Криптографические алгоритмы [Электронный ресурс] // muk.iuk.kg. – 2018. – Режим доступа: https://muk.iuk.kg/wp-content/uploads/2021/12/zashita-inform.pdf. – Дата доступа: 16.10.2022.
3. Алгоритм шифрования Twofish [Электронный ресурс] // otherreferats.allbest.ru. – 2012. – Режим доступа: https://otherreferats.allbest.ru/programming/00182702_0.html. – Дата доступа: 16.10.2022.

УДК 378.091

Нетехнические профессии в IT

Песняк И. М., студент
Нуриллоев К. А., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: к.т.н., доцент Дробыш А. А.