Практическая работа №9

ИЗУЧЕНИЕ ХЭШ-ФУНКЦИЙ ДЛЯ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И БАЗ ДАННЫХ

Цель работы. Изучить принципы работы и назначение хэш-функций.

Краткие сведения из теории

Электронная цифровая подпись

При обмене электронными документами по сети связи возникает проблема аутентификации автора документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном документе. В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет.

Электронная цифровая подпись (ЭЦП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

– гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. Система ЭЦП включает две процедуры: 1) постановки подписи; 2) проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

При формировании ЭЦП отправитель прежде всего вычисляет хэш-функцию $h(M)$ подписываемого текста M. Вычисленное значение хэш-функции $h(M)$ представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Хэш-функция предназначена для сжатия подписываемого документа M до нескольких десятков или сотен бит. Хэш-функция $h(M)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение $h(M) = m$ фиксированной длины. Обычно хэшированная информация является сжатым дво-

ичным представлением основного сообщения произвольной длины. Значение хэш-функции $h(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ M.

Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = h(M)$ принятого по каналу сообщения M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Функция $h(M)$ – является хэш-функцией, если она удовлетворяет следующим условиям:

– исходный текст может быть произвольной длины;

– само значение $h(M)$ имеет фиксированную длину;

– значение функции $h(M)$ легко вычисляется для любого аргумента;

– восстановить аргумент по значению с вычислительной точки зрения – практически невозможно;

– функция $h(M)$ – однозначна.

Из определения следует, что для любой хэш-функции есть тексты-близнецы – имеющие одинаковое значение хэш-функции, так как мощность множества аргументов неограниченно больше мощности множества значений. Такой факт получил название «эффект дня рождения».

Наиболее известные из хэш-функций – MD2, MD4, MD5 и SHA.

Три алгоритма серии MD разработаны Ривестом в 1989-м, 90-м и 91-м годах соответственно. Все они преобразуют текст произвольной длины в 128-битную сигнатуру.

Алгоритм MD2 предполагает:

– дополнение текста до длины, кратной 128 битам;

– вычисление 16-битной контрольной суммы (старшие разряды отбрасываются);

– добавление контрольной суммы к тексту;

– повторное вычисление контрольной суммы.

Алгоритм MD4 предусматривает:

– дополнение текста до длины, равной 448 бит по модулю 512;

– добавление длины текста в 64-битном представлении;

– использование процедуры Damgard-Merkle с 512-битными блоками (в отличие от хэш-функции этот класс преобразований предполагает вычисление для аргументов фиксированной длины также фиксированных по длине значений), причем каждый блок участвует в трех разных циклах.

В алгоритме MD4 довольно быстро были найдены «дыры», поэтому он был заменен алгоритмом MD5, в котором каждый блок участвует не в трех, а в четырех различных циклах.

Алгоритм SHA (Secure Hash Algorithm) разработан NIST (National Institute of Standard and Technology) и повторяет идеи серии MD. В SHA используются тексты более 2^{64} бит, которые закрываются сигнатурой длиной 160 бит.

Порядок выполнения работы

1 Изучить краткие сведения из теории.

2 Произвести анализ использования функций хэширования в используемых протоколах и технологиях.

Содержание отчета

1 Цель работы.

2 Перечень функций хэширования и технологий, в которых они используются.

3 Вывод по работе.

Контрольные вопросы

1 Назначение хэф-функции.

2 Хэш-код.

3 Что такое односторонняя функция?

4 Основные алгоритмы хэш-функций.

5 Применение хэш-функций.