**3.1 Математическая модель хэш-функции устойчивой к коллизионным атакам**

Криптографическая хэш-функция, которая устойчива к коллизионным атакам, должна быть односторонней. Это свойство означает, что для любого сообщения легко вычисляется значение хэша, в то время как задача нахождения хотя бы одного сообщения, для которого значение хэш-функции равно заданному значению должна быть вычислительно трудной (сложность вычислений экспоненциально зависит от длины хэша).

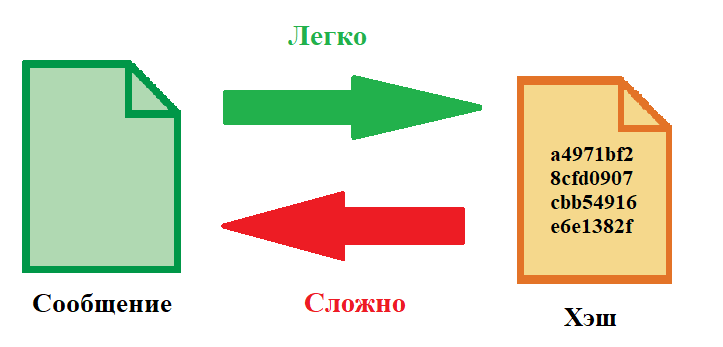


Рисунок 8 – Односторонняя хэш-функция

Другим важным свойством криптографической хэш-функции является лавинный эффект. Лавинный эффект означает свойство хэш-функции, при котором незначительное изменение входного сообщения приведет к полному изменению хэша. Более строго, выполнение свойства лавинного эффекта означает, что изменение одного бита сообщения приводит к изменению половины бит хэша.

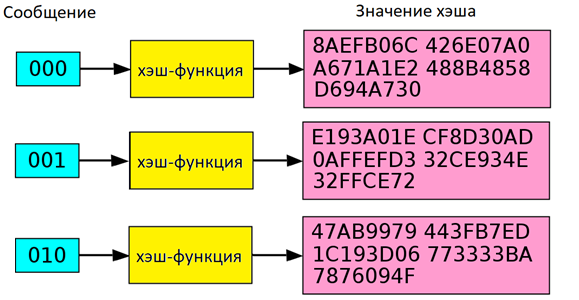


Рисунок 9 – Пример лавинного эффекта хэш-функции

Также должен выполняться критерий независимости бит, который означает, что при изменении одного бита в исходном сообщении любая пара бит хэша изменяется независимо. Таким образом, значение хэшаВ рамках данной работы разработана криптографическая хэш-функция с длиной выходного значения хэша 512 бит. Функция построена на основе структуры Миагути-Пренеля. При вычислениях используются два значения A и B длиной 512 бит каждое, которые хранятся в виде массива из 16 32-битных элементов. Сообщение, для которого необходимо вычислить хэш, разбивается на блоки длиной 512 бит. Последний блок дополняется нулями до размера 512 бит.

В начале выполнения алгоритма значение S инициализируется как 0, если функция работает в бесключевом режиме или значением ключа, если используется ключевой режим. Значение M инициализируется первым блоком обрабатываемого сообщения.

Для каждого блока сообщения вызывается функция сжатия, которая принимает в качестве параметров текущее значение внутреннего состояния и обрабатываемый блок сообщения. Блок-схема хэш-функции представлена на рисунке 10.

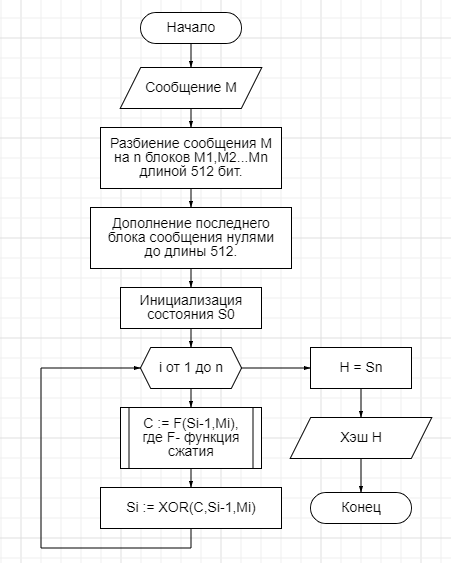
****

Рисунок 10 – Блок-схема хэш-функции

Функция сжатия принимает на вход значения A и B длиной 512 бит и вычисляет значение длиной 512 бит.  Вычисление представляет собой последовательное выполнение 32-х раундов, каждый из которых состоит из последовательного применения следующих формул:

1) На вход поступают текущие значения массивов A и B

2) Для элементов выполняется преобразование по формуле (индексы элементов берутся по модулю 16):

(3.1)

3) Выполняется циклический сдвиг массива (i-й элемент становится (i-1)-м элементом, а нулевой элемент становится последним элементом).

4) Для элементов с индексами выполняется преобразование по формуле:

(3.2)

5) Для всех элементов и выполняются преобразования по формуле:

(3.3)

где r – номер текущего раунда (для первого раунда r=0, для последнего раунда r=31)

Блок-схема функции сжатия представлена на рисунке 11.

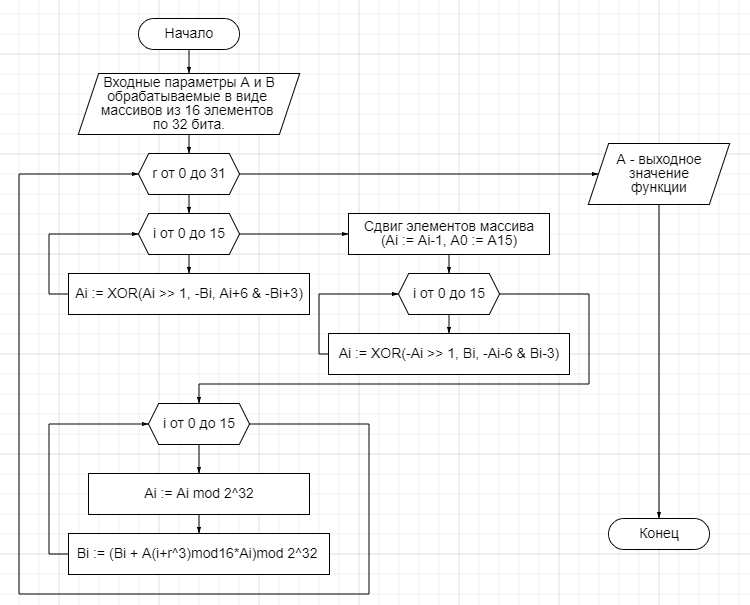
****

Рисунок 11 – Блок-схема функции сжатия