5.6. Алгоритм MD4

Кратко рассмотрим основные цели MD4:

1. Безопасность.
2. Скорость.
3. Простота и компактность.
4. Желательна little-endian архитектура.

Эти цели преследовались и при разработке *MD5*. *MD5* является более сложным и, следовательно, более медленным при выполнении, чем MD4. Считается, что добавление сложности оправдывается возрастанием уровня безопасности. Главные различия между этими двумя алгоритмами состоят в следующем:

1. MD4 использует три цикла из 16 шагов каждый, в то время как *MD5* использует четыре цикла из 16 шагов каждый.
2. В MD4 дополнительная константа в первом цикле не применяется. Аналогичная дополнительная константа используется для каждого из шагов во втором цикле. Другая дополнительная константа используется для каждого из шагов в третьем цикле. В *MD5* различные дополнительные константы, T [i], применяются для каждого из 64 шагов.
3. *MD5* использует четыре элементарные логические функции, по одной на каждом цикле, по сравнению с тремя в MD4, по одной на каждом цикле.
4. В *MD5* на каждом шаге текущий результат складывается с результатом предыдущего шага. Например, результатом первого шага является измененное слово A. Результат второго шага хранится в D и образуется добавлением A к циклически сдвинутому влево на определенное число бит результату элементарной функции. Аналогично, результат третьего шага хранится в C и образуется добавлением D к циклически сдвинутому влево результату элементарной функции. MD4 это последнее сложение не включает.