ТЕМА 5. Хэш-функции

5.1. Требования к хэш-функциям

Хэш-функцией называется односторонняя функция, предназначенная для получения *дайджеста* или "отпечатков пальцев" файла, сообщения или некоторого блока данных.

Хэш-код создается функцией H: h = H (M)

Где M является сообщением произвольной длины и h является *хэш-кодом* фиксированной длины.

Хэш-функция H, которая используется для аутентификации сообщений, должна обладать следующими свойствами:

1. *Хэш-функция* H должна применяться к блоку данных любой длины.
2. *Хэш-функция* H создает выход фиксированной длины.
3. H (M) относительно легко (за полиномиальное время) вычисляется для любого значения M.
4. Для любого данного значения *хэш-кода* h вычислительно невозможно найти M такое, что H (M) = h.
5. Для любого x вычислительно невозможно найти y ≠x, что H (y) = H (x).
6. Вычислительно невозможно найти произвольную пару (x, y) такую, что H (y) = H (x).