5.4. Использование цепочки зашифрованных блоков

Существуют различные *хэш-функции*, основанные на создании цепочки зашифрованных блоков, но без использования секретного ключа. Одна из таких *хэш-функций* была предложена Рабином. Сообщение M разбивается на блоки фиксированной длины M_1, M_2, . . . , M_N и используется алгоритм симметричного шифрования, например DES, для вычисления *хэш-кода* G следующим образом:

H_0 = начальное значение

$H_i = E_{Mi} [H_{i-1}]$

$G = H_N$

Это аналогично использованию шифрования в режиме CBC, но в данном случае секретного ключа нет. Как и в случае любой *простой хэш-функции*, этот алгоритм подвержен "атаке дня рождения", и если шифрующим алгоритмом является DES и создается только 64-битный *хэш-код*, то система считается достаточно уязвимой.

Могут осуществляться другие атаки типа "дня рождения", которые возможны даже в том случае, если противник имеет доступ только к одному сообщению и соответствующему ему зашифрованному *хэш-коду* и не может получить несколько пар сообщений и зашифрованных *хэш-кодов*. Возможен следующий сценарий: предположим, что противник перехватил сообщение с аутентификатором в виде зашифрованного *хэш-кода*, и известно, что незашифрованный *хэш-код* имеет длину m битов. Далее противник должен выполнить следующие действия:

- Используя описанный выше алгоритм, вычислить незашифрованный *хэш-код* G.
- Создать поддельное сообщение в виде Q_1, Q_2, . . . , Q_{N-2}.
  Вычислить $H_i = E_{Qi}[H_{i-1}]$ для $1 \le i \le N-2$.
- Создать $2^{m/2}$ случайных блока X и для каждого такого блока X вычислить $E_X[H_{N-2}]$. Создать дополнительно $2^{m/2}$ случайных блока Y и для каждого блока Y вычислить $D_Y[G]$, где D - дешифрующая функция, соответствующая E. Основываясь на "парадоксе дня рождения" можно сказать, что с высокой степенью вероятности эта последовательность будет содержать блоки X и Y такие, что $E_X[_{HN-2}] = D_Y[Y]$.
- Создать сообщение Q_1, Q_2, . . . ,Q_{N-2}, X, Y. Это сообщение имеет *хэш-код* G и, следовательно, может быть использовано вместе с зашифрованным аутентификатором.

Эта форма атаки известна как атака "встреча посередине". В различных исследованиях предлагаются более тонкие методы для усиления подхода, основанного на цепочке блоков. Например, Девис и Прайс описали следующий вариант: $H_i = E_{Mi} [H_{i-1}] \oplus H_{i-1}$

Возможен другой вариант: $H_i = E_{Hi-1} [M_i] \oplus M_i$

Однако обе эти схемы также имеют уязвимости при различных атаках. В более общем случае, можно показать, что некоторая форма "атаки дня

рождения" имеет успех при любом хэш-алгоритме, включающем использование цепочки шифрованных блоков без применения секретного ключа.

Дальнейшие исследования были направлены на поиск других подходов к созданию функций хэширования.