4.2. Криптоанализ алгоритмов с открытым ключом

Как и в случае симметричного шифрования, алгоритм шифрования с *открытым ключом* уязвим для лобовой атаки. Контрмера стандартная: использовать большие ключи.

Криптосистема с *открытым ключом* применяет определенные неинвертируемые математические функции. Сложность вычислений таких функций не является линейной от количества битов ключа, а возрастает быстрее, чем ключ. Таким образом, размер ключа должен быть достаточно большим, чтобы сделать лобовую атаку непрактичной, и достаточно маленьким для возможности практического шифрования. На практике размер ключа делают таким, чтобы лобовая атака была непрактичной, но в результате скорость шифрования оказывается достаточно медленной для использования алгоритма в общих целях. Поэтому шифрование с *открытым ключом* в настоящее время в основном ограничивается приложениями управления ключом и подписи, в которых требуется шифрование небольшого блока данных.

Другая форма атаки состоит в том, чтобы найти способ вычисления *закрытого ключа*, зная *открытый ключ*. Невозможно математически доказать, что данная форма атаки исключена для конкретного алгоритма *открытого ключа*. Таким образом, любой алгоритм, включая широко используемый *алгоритм RSA*, является подозрительным.

Наконец, существует форма атаки, специфичная для способов использования систем с *открытым ключом*. Это атака вероятного сообщения. Предположим, например, что посылаемое сообщение состоит исключительно из 56-битного ключа сессии для алгоритма симметричного шифрования. Противник может зашифровать все возможные ключи, используя *открытый ключ*, и может дешифровать любое сообщение, соответствующее передаваемому зашифрованному тексту. Таким образом, независимо от размера ключа схемы *открытого ключа*, атака сводится к лобовой атаке на 56-битный симметричный ключ. Защита от подобной атаки состоит в добавлении определенного количества случайных битов в простые сообщения.