УДК 519.711/.72

А.Я. Белецкий

Национальный авиационный университет, Киев

МАТРИЧНЫЙ АЛГОРИТМ ДИФФИ–ХЭЛЛМАНА

Рассмотрен криптографический алгоритм, содержащий криптопримитив, в основу которого положен матричный протокол Диффи–Хэллмана. Криптопримитив построен на преобразованиях блоков двоичных последовательностей путем их умножения в поле GF(2) на невырожденную (0, 1)-матрицу M высокого порядка, обладающую тем свойством, что элементы циклической группы, образуемой степенями M, составляют последовательность максимальной длины.

Толчком к развитию криптографических систем с открытым ключом (асимметричных шифров) послужило опубликование в 1976 году статьи У. Диффи и Р. Хэллмана (DH) [1]. Разработанный впоследствии алгоритм DH позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Однако этот алгоритм, будучи уязвимым к атакам типа «человек посередине», не решал проблему аутентификации. Без дополнительных средств ни один из пользователей не мог быть уверен, что он обменялся ключами именно с тем пользователем, который ему был нужен. Годом позже был предложен алгоритм асимметричного шифрования RSA, который решил проблему общения через незащищѐнный канал [2].

Алгоритмы DH и RSA используются в большом числе криптографических приложений. И, тем ни менее, они обладают рядом существенных недостатков, сужающих области их применения. Среди этих недостатков отметим следующие. Во-первых, поименованные шифраторы базируются на использовании больших простых чисел, длина которых может превышать несколько Кбит. Генерация таких чисел представляет собой достаточно сложную задачу, причем их простота обеспечивается с конечной вероятностью, не достигающей единицы. Во-вторых, скорость шифрования асимметричными алгоритмами на несколько порядков (три и более) ниже скорости шифрования в симметричных криптосистемах. Поэтому, и прежде всего в силу второго указанного недостатка, асимметричные алгоритмы применятся, в основном, в системах обмена ключами в корпоративных компьютерных сетях.

В работе российских ученых [3] предлагается строить блочные шифры на основе обратимых матриц над полем GF(2). Если $X, Y -$ векторы, представляющие соответственно открытый и зашифрованный текст, а M – шифрующая матрица, то зашифрование задается уравнением $Y = M \cdot X$, а расшифрование – уравнением $X = M^{-1} \cdot Y$. Для установления сеансовых ключей в системе авторы предлагают использовать протокол Диффи–Хэллмана в циклической группе матриц $\langle M \rangle$, где матрица M считается общедоступной. При этом пользователь А вырабатывает случайный показатель x, вычисляет матрицу M^x и посылает пользователю В. В свою очередь пользователь В вырабатывает случайный показатель y, вычисляет матрицу M^y и посылает пользователю А. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу $M^{xy} = M^{yx}$. Поскольку число N невырожденных матриц M, как утверждают авторы, велико, то вычисление ключа (по их мнению) имеет переборную сложность.

Вслед за упомянутой работой появилась статья [4], в которой многие утверждения, содержащиеся в [3], опровергаются. В частности, доказывается, что в том виде, в котором в [3] предлагается строить матричное шифрование DH, не обеспечивает обещанного уровня криптостойкости, а ключ зашифрования M^{xy} легко взламывается.

Основная задача, которая ставится в данном докладе, состоит в том, чтобы в какой-то мере ослабить критические замечания, высказанные в статье [4] по отношению к матричным шифрам, и предложить методы синтеза гарантированно невырожденных легко обратимых шифрующих матриц M.

Список литературы

1. Diffie W., Hellman M.E. New Directions in Cryptography // IEEE Transactions on Information Theory. – November 1976. – V. IT-22, no. 6. – C. 644-654.

2. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 318 с.

3. Ерош И.Л., Скуратов В.В. Адресная передача сообщений с использованием матриц над полем GF(2) // Проблемы информационной безопасности. – 2004. – № 1. – С. 72-78.

4. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова) [Электронный ресурс]. – Режим доступа к документу: www.ssl.stu.neva.ru/psw/crypto/rostovtsev Erosh_Skuratov.pdf.