УДК 658.012.011.56:681.3.06

М.П. Карпінський – д-р., техн. наук, професор, Я.І. Кінах – канд. техн. наук, доц., І.М. Костевич – магістрант
Академія технічно-гуманістична, Польща
Тернопільський національний технічний університет імені Івана Пулюя, Україна

КРИПТОГРАФІЧНИЙ ЗАХИСТ МЕРЕЖЕВИХ ДАНИХ НА ОСНОВІ АСИМЕТРИЧНИХ АЛГОРИТМІВ

M.P. Karpinsky – Dr., Prof., I.I. Kinakh – Ph.D, Assoc. Prof., I.M. Kostevych – student.

CRYPTOGRAPHIC NETWORK DATA PROTECTION BASED ON ASYMMETRIC ALGORITHMS

Безпека комп’ютерних програм та їх даних у комп’ютерних мережах розглядається в умовах абсолютної недовіри у кіберсередовищі. Така умова дозволяє забезпечити найвищий рівень захисту інформації та уникнути непорозумінь із користувачами та ресурсами мережі [1]. Відомо, що найбільш надійним методом захисту мережевого ресурсу є криптографічні асиметричні алгоритми, що широко використовуються в розподілених технологіях обробки даних. Для розв'язку задачі конфіденційної комунікації можна запропонувати такі дві архітектури [1]. В першій архітектурі користувач шифрує своє повідомлення і посилає його в загальний термінал, який можна реалізувати у вигляді звичайного списку розсилання. Кожний користувач отримує всі повідомлення, відправлені в термінал. Однак розшифрувати він може лише ті, що зашифровані його відкритим ключем. Ця система володіє абсолютною зовнішньою анонімністю, тобто для зовнішнього спостерігача, в тому числі і для оператора терміналу. При цьому відсутні засоби, що дозволили б визначити кому послано повідомлення. Рівень криптографічної стійкості доцільно визначати на основі використання алгоритмів решета числового поля[2].

Сучасні алгоритми криптоаналізу широко використовують поліном виду[2]:

$$Q(x) = q_1 q_2 (-1)^{a_0} x \prod_{j=1}^{s} p_j^{a_i} \pmod N,$$

де q_1, q_2, p_j – прості числа з бази розкладу; a_i – степінь числа; s – порядок решета; N – модуль криптографічного перетворення.

Одна з основних вимог, що ставиться до будь-якої системи шифрування, - це надійність в обчислювальному сенсі. Надійність асиметричних систем оцінюється на основі використання перспективного методу загального решета числового поля, що розпаралелюється на блоки і кожен блок реалізується на окремому комп'ютері. Тому для конфіденційного обміну даними доцільно використовувати ключ довжиною не менше 2048 двійкових знаків.

Література

1. Якименко І.З. , Касянчук М.М., Волинський О.І, Івасьєв С.В. Теоретичні основи аналітики та алгоритми оптимізації обчислень простих чисел // Проблемно-наукова міжгалузева конференція «Інформаційні проблеми комп’ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління ПНМК-2010, Україна, Бучач, Східниця, Карпати 01-04 червня 2010.
2. Alford W.R., Granville A., Pomtrance C. There are infinitely many Carmichael numbers // Ann. Math. 140. 1994. P. 703-722.