УДК 658.012.011.56:681.3.06

[1]М.П. Карпінський, докт. техн. наук, проф., [2]Я.І. Кінах канд. техн. наук, доц., [2]О.С. Войтенко, [3]В.Р. Паславський, [4]І.З. Якименко канд. техн. наук, доц., [4]М.М. Касянчук канд. фіз.-мат. наук, доц.
[1]Академія технічно-гуманістична, Польща
[2]Тернопільський національний технічний університет імені Івана Пулюя, Україна
[3]Львівський національний аграрний університет, Україна
[4]Тернопільський національний економічний університет, Україна

ТЕОРЕТИЧНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

M.P. Karpinsky, Dr., Prof., I.I. Kinakh, Ph.D, Assoc. Prof., O.S. Vojtenko, V.R. Paslavsky, I.Z.Yakymenko, Ph.D, Assoc. Prof., M.M. Kasyanchuk, Ph.D, Assoc. Prof.

THEORETICAL ANALYSIS OF INFORMATION SECURITY IN COMPUTER NETWORKS

Використання в практичній діяльності асиметричних алгоритмів шифрування пов'язане з цілою низкою задач. Їх можна умовно поділити на дві великі групи.

Перша група - криптостійкість асиметричних алгоритмів, відсутність строгих доведень необоротності функцій, що використовуються для обміну ключами в системі.

Друга група - продуктивність даних алгоритмів. Оскільки в основних асиметричних криптосистемах використовуються математичні перетворення над числами багатократної точності, то їх продуктивність значно менша за продуктивність традиційних криптосистем.

Не дивлячись на вищезгадані труднощі, асиметричним криптосистемам притаманний ряд переваг [1]. Основна з них та, що при їх використанні немає необхідності в обміні ключами, і як наслідок підвищується захищеність системи.

Метою досліджень є оцінка рівня надійності, в обчислювальному сенсі, систем шифрування RSA та Ель-Гамала на основі використання перспективних методів криптоаналізу, розвиток методів та засобів криптоаналізу, що базуються на факторизації та дискретному логарифмуванню чисел багатократної точності [2].

Для досягнення поставленої мети необхідно ефективно розв'язати низку взаємопов'язаних задач: аналіз, вибір та оптимізація методів дослідження рівня надійності систем шифрування RSA та Ель-Гамала; розробка методів і алгоритму оцінки рівня надійності систем шифрування RSA та Ель-Гамала; дослідження та оптимізація методів факторизації чисел багатократної точності [3];

На сьогодні є різні алгоритми, що дозволяють розв'язати задачу факторизації числа, з експоненційною асимптотичною оцінкою часу роботи [4]: продовжений алгоритм фракції, група алгоритмів під назвою квадратичне решето, алгоритм еліптичної кривої, решето числового поля, алгоритм випадкових квадратів Діксона, алгоритм двох третіх Валлі та алгоритм класу Сейсена [5]. Тільки для останніх трьох алгоритмів проведений строгий аналіз асимптотичної оцінки часу їх роботи. Для алгоритму Сейсена такий аналіз здійснений за припущення, що розширена гіпотеза Рімана є справедливою [6]. Ці три алгоритми мають тенденцію бути менш практичними, ніж згадані інші. Дослідження часу роботи останнього алгоритму проведено на основі евристичних міркувань. Агоритм приймає на вхід цілі гладкі, в певному розумінні, числа. Тому очікувана кількість гладких цілих чисел в послідовності відіграє важливу роль в аналізі часу роботи.

Задовільну оцінку для числа можна дати, якщо кожне з цілих чисел однорідно розподілене по базі розкладу [1, B], для деякої верхньої межі розкладу B. Проте ні один серед згаданих алгоритмів не дає такого рівномірного розподілу по базі. Для згаданих вище останніх трьох алгоритмів дано строгий аналіз часу роботи на основі припущення справедливості розширеної гіпотези Рімана. Для інших алгоритмів, в тому числі і для алгоритму решета числового поля, для оцінки ефективності роботи кращого, ніж евристичний аналіз оцінки часу роботи, немає. Такі евристичні дослідження дозволяють дати практично-корисні оцінки ефективності алгоритму. Ці оцінки дають можливість порівнювати алгоритми один з одним і робити прогнози, що торкаються їх практичного застосування. Час роботи алгоритму загального решета числового поля оцінюється виразом $\exp\left((c+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$, c=1,526 [7].

Одержані результати розв'язку дозволяють достеменно визначити таємний ключ системи RSA.

За допомогою удосконаленого методу можна: розв'язувати задачу знаходження закритого ключа за відкритим асиметричних систем шифрування RSA та Ель-Гамала; прогнозувати оцінку їх криптографічної стійкості; оцінювати якість ключового матеріалу систем шифрування інформації RSA та Ель-Гамала.

Методи решета числового поля асимптотично більш ефективні, але застосовні тільки для чисел виду n = $r^e - s$, де r і s порівняно малі. На практиці аналізовані методи варто застосовувати для чисел з інтервалу 10130 < n < 10160. Удосконалення апаратних засобів обчислювальної техніки не послаблює рівня надійності системи шифрування RSA.

Отже удосконалення апаратних засобів ЕОМ підвищує рівень надійності згаданої вище системи шифрування. Алгоритми Ель-Гамала та RSA володіють приблизно однаковою стійкістю з точки зору оборотності функцій, що в них використовуються; алгоритм Ель-Гамала значно переважає алгоритм RSA за швидкодією при виборі вихідних параметрів та, особливо, при операції шифрування; алгоритм RSA переважає алгоритм Ель-Гамала за криптостійкістю при аналізі на основі відомих фрагментів повідомлення. Знаючи час операцій з закритими ключами, зловмисник може визначити закритий ключ симетричної системи шифрування. Тому до систем захисту інформації, які використовують систему RSA, необхідно включати засоби, що позбавлять часову атаку змісту.

Література

1. Горбенко И. Д. Уточнённые показатели прихода шифров к состоянию случайной подстановки / И. Д. Горбенко, В. И. Долгов, К. Е. Лисицкий // Прикладная радиоэлектроника. - 2014. - Т. 13, № 3. - С. 213-216.

2. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К.: Держстандарт України, 1997. – 11 с.

3. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public key cryptosystems // Commun. ACM. V.21. No 2. 1978. P. 120-126.

4. Riesel H. Prime numbers and computer methods for factorization. Birkhauser, 1985.

5. Cohen H. A course in computational algebraic number theory. GraduateTexts in Math. V. 138. New York, Springer, 1993.

6. Gordon D.M. Discrete logarithms in GF(p) , using the number field sieve. SIAM J. Disc. Math. V.6, #1, 1993. . P. 124-138.

7. Lenstra A. K., Lenstra H. W. (jr.) The Development of the Number Field Sieve. Lect. Notes in Math. V. 1554. Springer, 1993.