УДК 004.056.5
Левченко А.М. [1], Паромова Т.О. [2], Луценко Н.В.[2]
[1] студ. гр. КНТ-528 НУ «Запорізька політехніка»
[2] старш. викл. НУ «Запорізька політехніка»

АНАЛІЗ КРИПТОСТІЙКОСТІ АЛГОРИТМУ ШИФРУВАННЯ RSA

Сьогодні кожен з нас зустрічається з необхідністю захисту даних, бо зростає обсяг конфіденційної інформації в мережі. Шифрування забезпечує захист від випадкового або навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни. Тому забезпечення високої криптостійкості є першочерговим завданням при створенні надійної та безпечної системи.

В основі криптографічного алгоритму RSA (Rivest–Shamir–Adleman) лежить факторизація великих цілих чисел, що є однобічною функцією з потайним входом. Це така функція, що легко обчислюється в одному напрямку, але важко обчислюється у зворотному без спеціальної інформації (секрету), тому злом методом «грубої сили» потребує значні обчислювальні потужності. Криптосистема RSA стала першою системою, придатною і для шифрування, і для цифрового підпису.

На рис.1 зображено прогрес розв'язання задачі факторизації цілих чисел, що є ключем для злому алгоритму RSA, де вісь OY показує довжину ключа, а OX – це вісь часу. Пряма лінія – це функція, що демонструє приблизне зростання вимог до довжини ключа при збільшенні обчислювальних потужностей комп'ютерів з кожним роком. Кружечками позначені криптоаналізи науковців алгоритму RSA, а зірочками позначені відомі спроби вдалих атак [1].

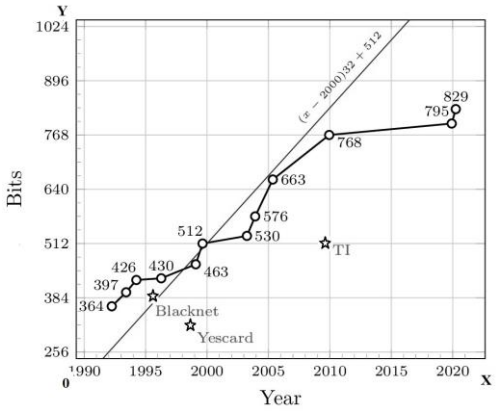

Рисунок 1 – Прогрес факторизації цілих чисел

Поточним рекордом факторизації цілих чисел є 829-бітний RSA-250, що був обрахований наприкінці лютого 2020 року. Загальний час обчислень становив приблизно 2700 базових років при використанні Intel Xeon CPUs Gold 6130 як еталон (2,1 ГГц) [2]. Тобто на даний час неможливо обчислити настільки великі обсяги даних без використання суперкомп'ютерів. Але навіть з огляду на цей факт час для злому залишається дуже великим, тому завжди є можливість збільшення криптостійкості алгоритму за допомогою збільшення довжини ключа.

Одним з напрямків для криптоаналізу алгоритму RSA є використання квантових комп'ютерів. У 1994 році Пітер Шор розробив алгоритм, що дозволяє, використовуючи квантовий комп'ютер, обчислити факторизацію цілого числа M за час $O(log^3 M)$, використовуючи $O(log\ M)$ логічних кубітів. У 2001 році його працездатність була продемонстрована групою фахівців IBM. Число 15 було розкладено на множники 3 і 5 за допомогою квантового комп'ютера з 7 кубітами [3].

У 2015 році дослідники зробили висновок, що для досить швидкого злому 2048-бітного RSA шифрування квантовому комп'ютеру знадобиться мільярд кубітів. У 2019 році Крейг Гідні та Мартін Екеро визначили, що комп'ютер з 20 млн кубітів зможе впоратися з цим завданням всього за 8 годин. За прогнозами вчених такий квантовий комп'ютер можливо розробити через 25 років, але беручи до уваги той факт, що ці прогнози не можна вважати повністю вірними, то можливо очікувати такі машини раніше зазначеного терміну [4].

На цей час алгоритм RSA є криптостійким та може постійно удосконалюватися за допомогою збільшення довжини ключа. Квантові комп'ютери можуть стати значною загрозою у майбутньому для алгоритму, тому необхідно заздалегідь вжити необхідні заходи для запобігання криптографічних атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. How big an RSA key is considered secure today? [Електронний ресурс]. – Режим доступу: https://crypto.stackexchange.com/questions/1978/how-big-an-rsa-key-is-considered-secure-today

2. Factorization of RSA-250 [Електронний ресурс]. – Режим доступу: https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

3. Алгоритм Шора [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ Алгоритм_Шора

4. How a quantum computer could break 2048-bit RSA encryption in 8 hours [Electronic resource]. – Access mode: https://www.technologyreview.com/ 2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/