

## ПОРІВНЯННЯ МЕТОДІВ ШИФРУВАННЯ

Криптографія є одним з важливих напрямків розвитку ІТ-технологій, якій націлені на підвищення та удосконалення захисту інформації. Вона розвивається в декількох напрямках, таких як забезпечення конфіденційності, забезпечення цілісності даних, автентифікації і шифрування.

Одним з методів захисту інформації є шифрування, яке застосовується для зберігання важливої інформації в ненадійних джерелах і передачі її по незахищеним каналам зв'язку. Удосконалення методів шифрування дозволить підвищити як безпеку, так і швидкість передачі даних.

Існує два види шифрування: симетричне і асиметричне [1].

У шифруванні симетричним методом використовується один і той же ключ як для шифрування повідомлення, так і для його дешифрування. Існує декілька методів симетричного шифрування, наприклад, DES, 3DES, Skipjack. Кращим симетричним алгоритмом шифрування на даний момент визнається AES, який і буде використаний для подальшого аналізу. Основним недоліком симетричного методу є те, що один і той же ключ використовується як для шифрування, так і для дешифрування. А так як ключ передається по відкритому каналу, то ймовірність його перехоплення дуже висока [2, 3].

При асиметричному методі шифрування використовується публічний ключ для шифрування і закритий для дешифрування. Так як ключі пов'язані в пару, навіть втрата публічного ключа ніяк не загрожує безпеці системи. Асиметричний метод шифрування реалізується стандартним алгоритмом RSA і новим методом шифрування, заснованим на еліптичних кривих ECC [2, 4].

Кожен алгоритм шифрування має свої переваги та недоліки і свою галузь застосування. Для використання потрібного алгоритму шифрування необхідно знати надійність його ключів і часові витрати. Дані порівняння було отримано аналітичним методом (таблиця 1) та на практиці (таблиця 2)

Аналіз даних таблиці 1 показує, що час злому шифру навіть другого рівня безпеки є занадто великим (понад  $10^5$  років) для успішного використання стандартних дешифраторів у вигляді стаціонарних комп'ютерів. Однак існує можливість використання суперкомп'ютерів, які забезпечують продуктивність на 5-10 і більше порядків. Для подальшого підвищення швидкості обчислень існує можливість об'єднати суперкомп'ютери в кластери, підсумовуючи їх обчислювальні потужності.

Таким чином, не дивлячись на збільшення часу шифрування і дешифрування, ефективним є використання шифрів підвищеної складності (4-5 і вище) рівня безпеки. Для порівняння часових витрат було використано файл розміром 500 Мб.

Таблиця 1 – Порівняння надійності ключів

| Симетричний алгоритм | Біт безпеки | RSA публічний (біт безпеки) | ECC публічний (біт безпеки) | Час на зламування (при $1 * 10^{21}$ комбінацій/с) | Рівень безпеки |
|----------------------|-------------|-----------------------------|-----------------------------|----------------------------------------------------|----------------|
| Skipjack             | 80          | 1024                        | 160                         | 20 хвилин                                          | 1              |
| 3DES                 | 112         | 2048                        | 224                         | 164 464 років                                      | 2              |
| AES-128              | 128         | 3072                        | 256                         | $10.8 * 10^9$ років                                | 3              |
| AES-192              | 192         | 7680                        | 384                         | $199 * 10^{27}$ років                              | 4              |
| AES-256              | 256         | 15360                       | 512                         | $3 * 10^{48}$ років                                | 5              |

Таблиця 2- Порівняння часових витрат

| Рівень безпеки | Алгоритм | Час генерації ключа (мс) | Час шифрування (мс) | Час дешифрування (мс) |
|----------------|----------|--------------------------|---------------------|-----------------------|
| 1              | Skipjack | 33                       | 34                  | 10                    |
|                | RSA      | 36                       | 30                  | 27                    |
|                | ECC      | 20                       | 10                  | 0                     |
| 2              | 3DES     | 35                       | 33                  | 17                    |
|                | RSA      | 40                       | 35                  | 30                    |
|                | ECC      | 22                       | 22                  | 15                    |
| 3              | AES      | 39                       | 32                  | 25                    |
|                | RSA      | 42                       | 39                  | 39                    |
|                | ECC      | 28                       | 32                  | 35                    |
| 4              | AES      | 41                       | 32                  | 30                    |
|                | RSA      | 46                       | 42                  | 41                    |
|                | ECC      | 30                       | 37                  | 39                    |
| 5              | AES      | 44                       | 33                  | 33                    |
|                | RSA      | 50                       | 47                  | 50                    |
|                | ECC      | 33                       | 40                  | 43                    |

Аналіз даних таблиці 2 показує, що час, необхідний для створення ключа, шифрування і дешифрування даних розміром 500 мб вкрай мало, однак при використанні в промислових і корпоративних масштабах, обсяг шифрованих даних можуть становити більш терабайта, що робить цей процес

неприпустимо тривалим. Тому необхідно вибрати між більшою швидкістю або безпекою.

У порівнянні з іншими алгоритмами асиметричного шифрування найбільш швидкодіючим ECC, проте на відміну від інших алгоритмів алгоритми випадкових чисел для генерації еліптичних кривих викликають сумнів, так як метод їх генерації залишається невідомий [5].

Існує ще один метод шифрування - гібридний метод. Суть даного методу полягає у тому, що дані шифруються симетричним методом, наприклад, за алгоритмом AES, а ключ для симетричного методу ще раз шифрується асиметричним методом (алгоритм RSA або ECC), і по захищеному каналу передається вже зашифрований відкритий ключ.

Аналіз таблиці 1 та таблиці 2 показує, що метод гібридного шифрування об'єднує у собі простоту реалізації та швидкість шифрування основного обсягу даних із допомогою симетричного методу шифрування та криптографічну стійкість асиметричного методу шифрування для шифрування симетричного ключа.

Поєднання цих факторів дозволяє підвищити швидкість виконання криптографічних операцій та захищеного обміну даними, що робить метод симетричного шифрування вкрай перспективним для вивчення і подальшого розвитку.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баричев С.Г. и др. «Основы современной криптографии». - М.: «Горячая линия – Телеком», 2001 - 120 с.
2. Криптография простым языком: разбираем симметричное и асимметричное шифрование на примере сюжета Звездных войн (Updated) [Електронний ресурс] - Режим доступу: <https://habr.com/ru/post/452042/>
3. Саломаа А. «Криптография с открытым ключом Пер. с англ. - М.: Мир, 1995. - 318 с.
4. Асимметричное шифрование на практике [Електронний ресурс] - Режим доступу: <https://habr.com/ru/post/449552/>
5. Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup and others «How to manipulate curve standards: a white paper for the black hat».- Ch.: University of Illinois at Chicago, 2015 – 44 с.
6. Баричев. С.Г. «Криптография без секретов» - М.: Горячая линия - Телеком, 2004. - 43 с.