

УДК 004.042

Зайцева А.О.¹, Воскобойник В.О.²

1 студ. гр. РТ-819, НУ «Запорізька політехніка»

2 канд. техн. наук, проф. НУ «Запорізька політехніка»

ГІБРИДНИЙ АЛГОРИТМ В СУЧАСНИХ КРИПТОСИСТЕМАХ

У наш час є багато методів захисту інформації. Одним з таких методів є шифрування інформації. Шифрування — у системах обробки інформації — алгоритмічне (криптографічне) перетворення даних, яке виконується у послідовній послідовності з метою одержання шифрованого тексту. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. Їх два основних методи шифрування - симетричне та асиметричне.

На практиці, використання асиметричного шифрування призводить до істотного збільшення розміру зашифрованого тексту в порівнянні з відкритим текстом. З іншого боку, використання відкритих і секретних ключів, унікальних для кожного абонента, є затребуваним у багатьох криптографічних додатках, наприклад при реалізації конфіденційної електронної пошти.

Постає питання: що треба зробити, щоб вирішити ситуацію з недоліками методів шифрування та вимогами до захисту інформації?

Все це призводить до виникнення так званої гібридної схеми шифрування. Гібридна (або комбінована) криптосистема - це система шифрування, що поєднує переваги криптосистеми з відкритим ключем з продуктивністю симетричних криптосистем. Симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа, інакше це називається числовою упаковкою.

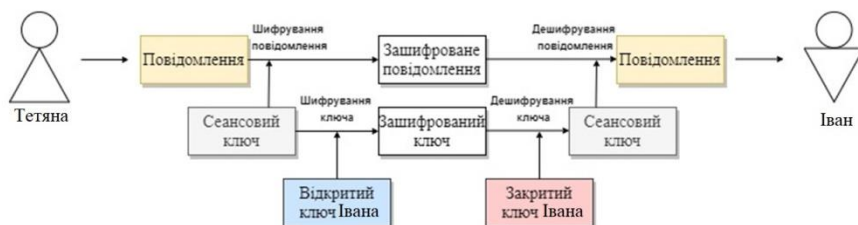


Рисунок 1 – Приклад гібридного алгоритму шифрування

Гібридні криптосистеми використовують переваги двох основних криптосистем: симетричної і асиметричної криптографії. На цьому принципі побудовані такі протоколи, як PGP і TLS.

Основний недолік асиметричної криптографії полягає в низькій швидкості через складні обчислення, необхідні її алгоритмами, в той час як симетрична криптографія традиційно показує високу швидкість роботи. Однак симетричні криптосистеми мають один істотний недолік - їх використання передбачає наявність захищеного каналу для передачі ключів. Для подолання цього недоліку вдаються до асиметричних криптосистем, які використовують пару ключів: відкритий і закритий.

Прикладом може служити надана схема спілкування (рис. 1)

На етапі відправки ми бачимо такі дії. Спочатку Тетяна генерує випадковий сеансовий ключ. Потім повідомлення Тетяни шифрується сеансовим ключем (за допомогою симетричного алгоритму). В свою чергу, сеансовий ключ шифрується відкритим ключем Івана (асиметричним

алгоритмом). В результаті Тетяна посилає Івану зашифроване повідомлення і зашифрований сеансовий ключ.

На етапі прийому. Спочатку Іван отримує зашифроване повідомлення Тетяни і зашифрований сеансовий ключ. Іван розшифровує сеансовий ключ своїм закритим ключем. За допомогою отриманого, таким чином, сеансового ключа Іван розшифровує зашифроване повідомлення Тетяни.

В наш час більшість гібридних систем працюють таким чином. Для симетричного алгоритму (3DES, AES або будь-якого іншого) генерується випадковий сеансовий ключ. Такий ключ як правило має розмір від 128 до 512 біт (в залежності від алгоритму). Потім використовується симетричний алгоритм для шифрування повідомлення. У разі блочного шифрування необхідно використовувати режим шифрування (наприклад CBC), що дозволить шифрувати повідомлення з довжиною, що перевищує довжину блоку. Що стосується самого випадкового ключа, він повинен бути зашифрований за допомогою відкритого ключа одержувача повідомлення, і саме на цьому етапі застосовується асиметричні алгоритми шифрування (RSA або алгоритм Діффі - Хеллмана). Оскільки сеансовий ключ короткий, його шифрування займає небагато часу. Шифрування набору повідомлень за допомогою асиметричного алгоритму - це завдання обчислювально більш складне, тому тут краще використовувати симетричне шифрування. Потім достатньо відправити повідомлення, зашифроване симетричним алгоритмом, а також відповідний ключ в зашифрованому вигляді. Одержувач спочатку розшифровує ключ за допомогою свого секретного ключа, а потім за допомогою отриманого ключа отримує і все повідомлення.

До речі, метод гібридного шифрування використовується в SSL / TLS сертифікатах під час послідовного зв'язку між серверами і клієнтами (веб-браузерами) в процесі, відомому як "TLS handshake". Спочатку перевіряється особистість обох сторін з використанням закритого і відкритого ключа. Після того, як обидві сторони підтвердили свою особистість, шифрування даних відбувається за допомогою симетричного шифрування з використанням ефемерного (сеансового) ключа. Це забезпечує швидку передачу великого обсягу даних, які ми відправляємо і отримуємо в Інтернеті кожну хвилину.

Отже, як бачимо з даного матеріалу, кожний метод шифрування має свої недоліки та переваги. Щоб вирішити цю проблему і вдосконалити захист інформації за допомогою шифрування була розроблена гібридна схема шифрування, яка поєднує переваги двох основних криптосистем: симетричної і асиметричної криптографії. Це призвело до більш швидкого шифрування в сполученні зі зручним розповсюдженням ключів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Иванов М. А., Ковалев А. В., Мацук Н. А., Чугунков И. В. Методы и средства защиты информации в компьютерных системах и сетях / Под ред. М.А. Иванова. – М.: КУДИЦ-ПРЕСС, 2009. 602 с.