УДК 343.9

Максим КАЛУШКА, Сергій КУЛИНА

Західноукраїнський національний університет

СХЕМА ТА АЛГОРИТМ ГІБРИДНОГО ШИФРУВАННЯ

Вступ. Зі збільшенням використання обміну даними та комунікації через Інтернет стає критично важливим захистити дані від потрапляння до рук зловмисників. Забезпечення цілісності та конфіденційності даних стає одним із ключових викликів для дослідників та фахівців у сфері кібербезпеки [1].

Мета: розробка схеми та алгоритму гібридного шифрування та подальше його впровадження в системах обробки даних.

1. Роль криптографії у кібербезпеці

Забезпечення захисту даних стає одним із ключових викликів для дослідників та фахівців у сфері кібербезпеки. Існує багато методів забезпечення ключових засад та принципів кібербезпеки, найпоширенішим з яких є застосування методів криптографії. Їх використання дає змогу забезпечити необхідний рівень конфіденційності, цілісності та невідмовності даних [2]. Що в свою чергу досягається захистом критичних даних або документів на жорсткому диску або під час їх передачі через ненадійний канал зв'язку. Дані у цьому процесі можуть бути випадково або навмисно змінені, спотворені або пошкоджені. Використання криптографії дозволяє частково уникнути таких загроз або зменшити їх вплив, а сам процес захисту інформації полягає в шифруванні та дешифруванні даних. Шифрування та дешифрування здійснюється за допомогою ключів, а сам процес поділяють на шифрування з симетричним ключем та шифрування з асиметричним ключем.

2. Симетричний алгоритм шифрування

У симетричному методі і шифрування і дешифрування здійснюються на основі єдиного ключа, який ще називається приватним або секретним ключем. Алгоритми із симетричним ключем залежно від вхідних даних поділяються на два типи: блочні та потокові шифри. У системах на основі блочного шифру дані обробляються або шифруються на фіксованій групі бітів, що називається блоком, тоді як у системах на основі потокового шифру дані обробляються у вигляді потоку бітів. Найбільш поширеними алгоритмами симетричного шифрування є AES і DES з блочних та RC4 і Blowfish з потокових шифрів [3].

Симетричне шифрування даних здійснюється одним і тим самим ключем, тому виникають додаткові недоліки його застосування:

- Проблема обміну ключами.
- Масштабованість.
- Ризик компрометації ключа.
- Відсутність підтвердження автентичності.
- Складнощі з управлінням ключами.

Представлена на рисунку 1 схема відображає процес обміну даними між двома користувачами із застосуванням симетричного шифрування даних.

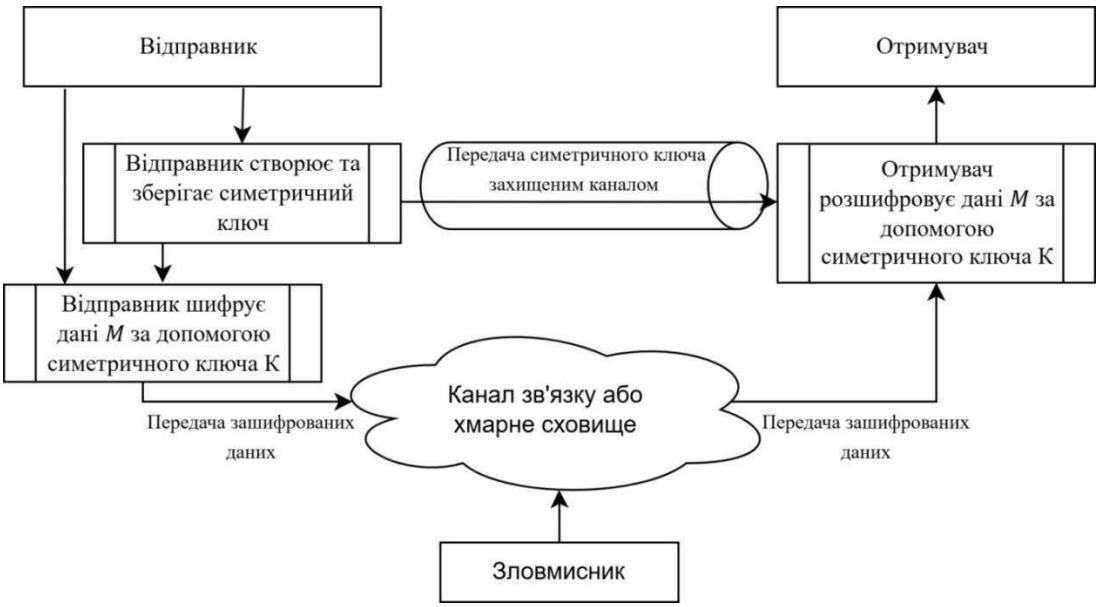

Рисунок 1 - Схема симетричного шифрування

2. Асиметричний алгоритм шифрування

Асиметричне шифрування використовує пару математично пов'язаних ключів, які називають відкритий ключ (public key) та закритий ключ (private key). Ця пара ключів дозволяє забезпечити високий рівень захисту при передачі даних та автентифікації, оскільки операції шифрування та розшифрування виконуються різними ключами. Відкритий ключ призначений для шифрування даних і доступний будь-кому, хто хоче надіслати зашифроване повідомлення отримувачу. Натомість закритий ключ використовується для розшифрування повідомлення і зберігається в таємниці, його має тільки отримувач (рисунок 2).

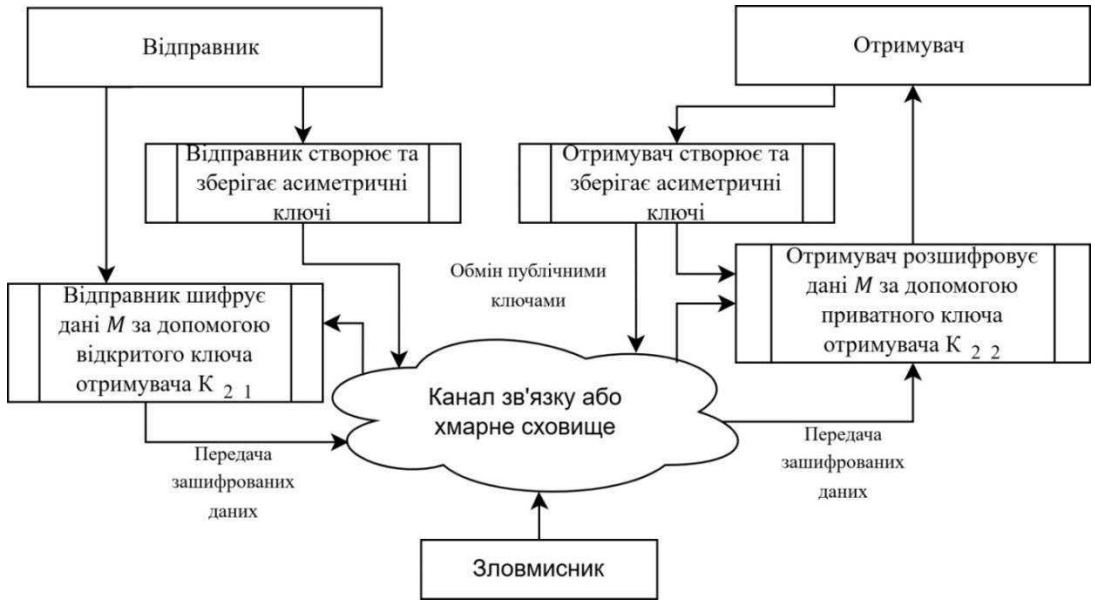

Рисунок 2 - Схема асиметричного шифрування

Основною перевагою асиметричного шифрування є безпечний обмін ключами. Завдяки своїм властивостям асиметричне шифрування дає можливість передавати публічний ключ відкритими каналами, не ризикуючи компрометацією приватного ключа [3].

Відповідно абонент, що отримав відкритий ключ іншої сторони може

зашифрувати будь які дані та переслати їх отримувачу. Використовуючи дві пари асиметричних ключів користувачі можуть без проблем обмінюватись секретною інформацією без загрози її витоку.

Представлена на рисунку 2.1 схема відображає процес обміну даними між двома користувачами із застосуванням виключно асиметричного шифрування.

Проте асиметричне шифрування має і свої недоліки, а саме:

- Низька швидкість.
- Вимоги до обчислювальних ресурсів.
- Уразливість до квантових комп'ютерів.
- Складність управління ключами.
- Ризик компрометації відкритого ключа.
- Відносна складність у розумінні та впровадженні.

Тому ключовим при використанні асиметричного шифрування є пошук шляхів компенсації недоліків даної системи шифрування [4].

3. Гібридний алгоритм шифрування

Останнім часом широко застосовується гібридне шифрування. Воно використовує переваги як симетричного, так і асиметричного шифрування, що забезпечує високу безпеку та ефективність передачі даних. Ключовою властивістю гібридного шифрування є поєднання швидкості та зручності асиметричного методу з ефективністю симетричного.

У пропонованій схемі гібридного шифрування використовуються сильні сторони обох методів, а саме: асиметричне шифрування для безпечного обміну ключами та симетричне шифрування для швидкого та ефективного шифрування великих обсягів даних (рисунок 3).

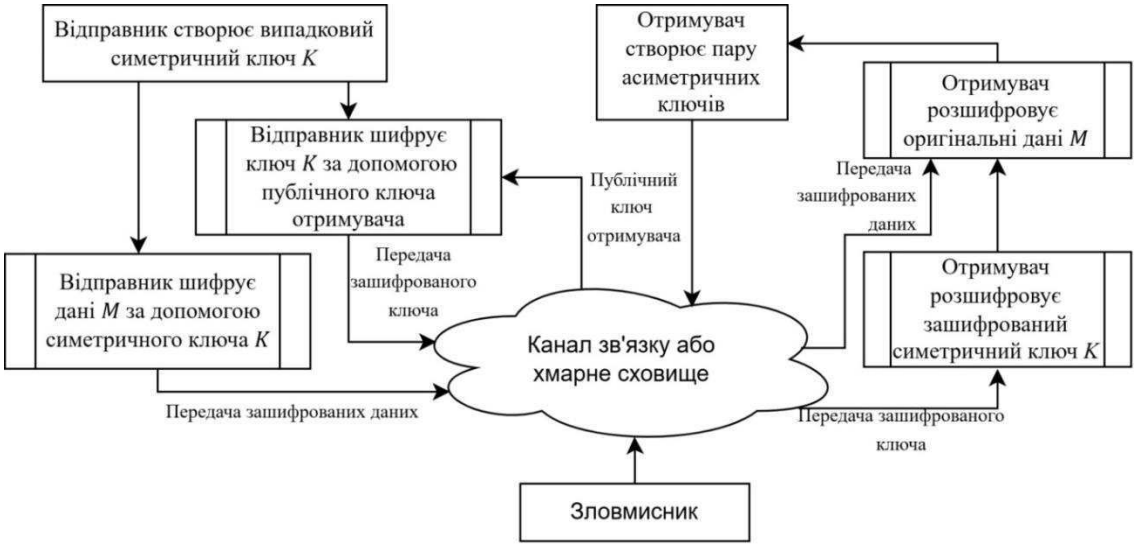

Рисунок 3 - Загальна схема гібридного шифрування

Відповідно алгоритм для гібридного шифрування складатиметься з наступних кроків:

Крок 1. Генерація симетричного ключа. Відправник створює випадковий симетричний ключ K, який буде використаний для шифрування даних.

Крок 2. Шифрування даних симетричним ключем. На поточному кроці відправник шифрує дані M за допомогою симетричного ключа K, отримуючи у результаті зашифровані дані C.

Крок 3. Шифрування симетричного ключа асиметричним алгоритмом. Щоб захистити симетричний ключ K, відправник шифрує його за допомогою публічного асиметричного ключа отримувача, отримуючи зашифрований ключ E_K.

Крок 4. Надсилання зашифрованих даних. На поточному кроці відбувається надсилання зашифрованих даних C та зашифрованого симетричного ключа E_K.

Крок 5. Розшифрування симетричного ключа. Отримувач, маючи свій приватний ключ, який є парним до публічного ключа, використаного для шифрування симетричного ключа на кроці 3, розшифровує зашифрований симетричний ключ E_K, отримуючи у результаті оригінальний симетричний ключ K.

Крок 6. Розшифровування даних. Отримувач, маючи оригінальний симетричний ключ K, використовує його для розшифровування зашифрованих даних C, отримуючи в результаті оригінальні дані M.

Як бачимо запропонований алгоритм поєднує у собі переваги симетричного та асиметричного шифрування, а саме:

- використовує симетричний ключ для шифрування даних, що збільшує як швидкість шифрування, так і швидкість дешифрування даних;
- використовує загальний канал для пересилання шифрованих даних та не потребує окремого захищеного каналу для пересилання ключа кодування;
- шифрує симетричний ключ за допомогою публічного ключа одержувача, що забезпечує достатній рівень захисту та дозволяє пересилати його відкритим каналом зв'язку.

Висновок. Отже, використання методів гібридного шифрування значно підвищує захищеність та стійкість даних при передачі між абонентами або при зберіганні на віддалених хмарних сховищах. Це досягається завдяки поєднанню переваг симетричних та асиметричних алгоритмів шифрування, а вибір самих алгоритмів залежить від завдання, яке ставить перед собою власних системи.

Перелік використаних джерел.

1. Бондаренко, Т., Шкітов, А., Шаповал, В., Шевага, В., Нещерет, І., Цикало, Ю., Лазута, Р. (2024). Мобільні особливості кібербезпеки щодо штучного інтелекту у повоєнній україні: виклики та стратегії.-Наука і техніка сьогодні, (4 (32)).

1. 2 Лубко, Д. В., Мірошниченко, М. Ю. (2024). Механізми безпеки інформації та їх виклики. Науковий вісник Таврійського державного агротехнологічного університету, 14(2).

2. Савченко, Я., Чмиренко, О. (2023). Криптографічні та стеганографічні засоби захисту інформації. Актуальні питання забезпечення кібербезпеки та захисту інформації, 94.

3. Філіп'єва, М. В., Гвоздецька, К. П. (2021). Порівняння симетричного і асиметричного шифрування. Міжнародна наукова інтернет-конференція Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення, 71.