УДК 004.056.55

Колосова К. К., студентка 4 курсу
Римар П. В., старший викладач
кафедри інформаційних технологій

ЗАСТОСУВАННЯ СИМЕТРИЧНИХ ТА АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ КЛЮЧІВ В ІНФОРМАЦІЙНО–КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Донецький національний університет імені Василя Стуса, м. Вінниця

В сучасному світі, де обмін інформацією відбувається швидко та великими обсягами, захист цієї інформації стає дедалі важливішим завданням. Криптографія, яка є наукою про захист інформації шляхом перетворення даних у нерозбірливий вигляд, виконує важливу роль у забезпеченні безпеки передачі даних в інформаційно-комунікаційних технологіях.

Симетричні та асиметричні криптографічні ключі є основними компонентами криптографічних систем. Симетрична криптографія використовує один і той самий ключ для як шифрування, так і розшифрування даних. Це дозволяє досягти високої швидкодії при обробці даних, але вимагає безпечної передачі цього ключа між відправником і одержувачем[1].

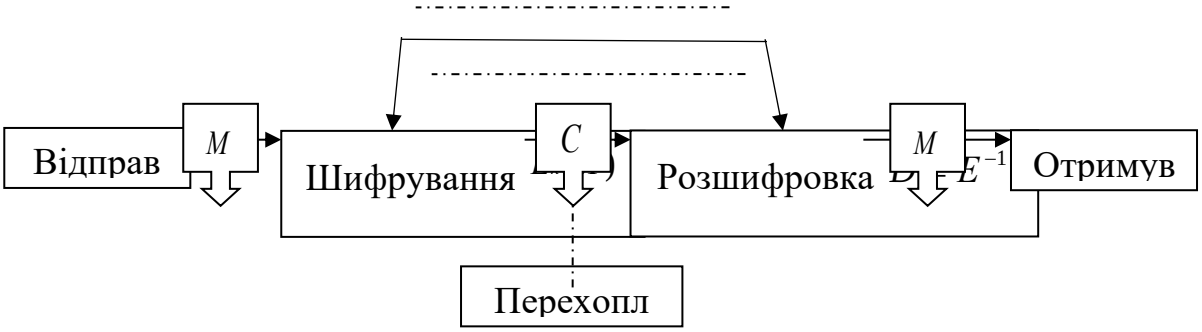

Рисунок 1.1 — Схема симетричної криптосистеми з одним ключем

Асиметрична криптографія використовує пару ключів - публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний ключ - для їх розшифрування. Ця система дозволяє безпечно обмінюватись публічними ключами, але її використання пов'язане з більшим обчислювальним навантаженням, оскільки процес шифрування та розшифрування вимагає більшої обчислювальної потужності[2].

Узагальнена схема асиметричної криптосистеми шифрування з відкритим ключем показана на рис. 1.2

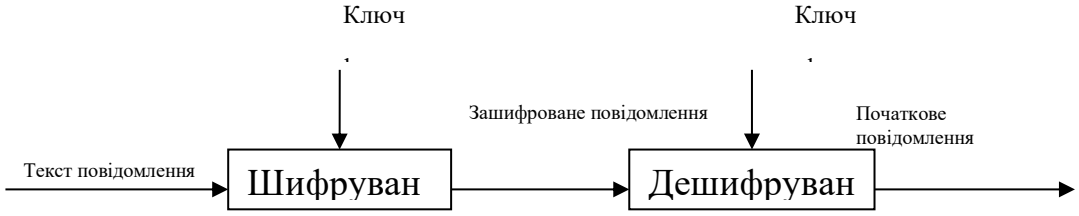

Рисунок 1.2 - Схема асиметричної криптосистеми шифрування з відкритим ключем

Застосування симетричних криптографічних ключів рекомендується для випадків, коли вимоги до швидкодії є критичними, а сторони обмінюються ключами в безпечному середовищі. Симетрична криптографія зазвичай застосовується для шифрування великих обсягів даних, таких як передача файлів або потокове відео.

Але, при необхідності безпечного обміну даними через незахищені канали зв'язку або відсутності можливості попередньої передачі ключів, асиметрична криптографія стає вельми ефективним рішенням. Вона дозволяє кожному користувачеві мати свою пару ключів: приватний ключ, який зберігається в секреті, та публічний ключ, який може бути розповсюджений відкрито. Використання цієї системи дозволяє забезпечити автентифікацію, цілісність даних та можливість цифрового підпису.

Використання симетричних та асиметричних криптографічних ключів дозволяє реалізувати інші важливі аспекти безпеки інформації, такі як цифровий підпис та аутентифікація. Асиметрична криптографія забезпечує можливість створення цифрового підпису, який підтверджує автентичність документа та недоторканість даних. Це важливо для забезпечення відправника, що його повідомлення не було змінене під час передачі[3].

Крім того, асиметрична криптографія дозволяє реалізувати механізми аутентифікації, такі як обмін цифровими сертифікатами. Це дозволяє сторонам перевірити автентичність один одного та підтвердити, що комунікація відбувається з довіреною стороною.

Застосування симетричних та асиметричних криптографічних ключів у інформаційно-комунікаційних технологіях є важливим для захисту конфіденційності, цілісності та автентичності даних. Вибір конкретного типу ключа залежить від потреб і вимог конкретного застосування. Ефективне комбінування цих двох методів у гібридну систему дозволяє досягти оптимального балансу між безпекою і продуктивністю в області інформаційно-комунікаційних технологій.

Отже, в інформаційно-комунікаційних технологіях застосування симетричних та асиметричних криптографічних ключів є необхідним, оскільки кожен з них має свої переваги та недоліки. Використання симетричних ключів забезпечує високу швидкодію та ефективність при обробці великих обсягів даних, тоді як асиметричні ключі забезпечують безпечний обмін даними і

використовуються для автентифікації та цифрового підпису. Оптимальне використання цих двох типів криптографічних ключів дозволяє забезпечити високий рівень безпеки та конфіденційності при передачі інформації.

Список літератури:

1. *Шифрування з симетричними ключами. URL: https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B7_%D1%81%D0%B8%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%B8%D0%BC%D0%B8_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D0%BC%D0%B8*

2. *Асиметричні алгоритми шифрування. URL: https://uk.wikipedia.org/wiki/%D0%90%D1%81%D0%B8%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%96_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B8_%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F*

3. *Колосова К. К., Римар П. В. Системи управління симетричними та асиметричними криптографічними ключами. Матеріали вісника студентського наукового товариства Донецького національного університету імені Василя Стуса. Випуск 12 том 2. Вінниця: ДонНУ імені Василя Стуса, 2022. С. 270-274.*

УДК 004.056.5

Лупол А.А., студент 1 курсу спеціальності 122 «Комп'ютерні науки»
Ніколюк П.К., професор, доктор фізико-математичних наук.

ДОСЛІДЖЕННЯ РІЗНИХ МЕТОДІВ КРИПТОАНАЛІЗУ ТА ЇХ ЕФЕКТИВНОСТІ В РОЗШИФРУВАННІ ЗАШИФРОВАНИХ ПОВІДОМЛЕНЬ

Донецький національний університет імені Василя Стуса, м.Вінниця

У сучасному світі, де мережеві технології набувають все більшого значення, криптографія стає надзвичайно важливим елементом забезпечення безпеки і конфіденційності інформації. Зашифрування повідомлень є одним з основних методів захисту інформації від небажаних переглядів та злочинної діяльності. Проте, зі зростанням потужності комп'ютерів та розвитком криптоаналітичних методів, появляється загроза порушення безпеки інформації. Тому, вивчення різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень є актуальною та важливою задачею.

Захист інформації є надзвичайно важливим елементом у сучасному світі, де інформаційні технології знаходяться на передовій розвитку. У зв'язку з цим, криптографія стає все більш важливою, оскільки вона забезпечує конфіденційність та захист інформації. Однак, зі зростанням потужності комп'ютерів та розвитком криптоаналітичних методів, необхідно вдосконалювати криптографічні протоколи та методи захисту інформації. Тому,