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,

дослідження різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень є актуальною та важливою задачею.

Останні дослідження в галузі криптоаналізу та розшифрування зашифрованих повідомлень зосереджені на вдосконаленні методів криптоаналізу та розробці нових методів для подолання криптографічних захистів. Одним з пріоритетних напрямків досліджень є дослідження методів криптоаналізу на основі машинного навчання, зокрема, нейронних мереж. На сьогоднішній день успішно використовуються нейронні мережі для розшифрування шифрів, зокрема, шифрів з використанням замін і перестановок символів. Використання нейронних мереж у криптоаналізі дозволяє знизити час, необхідний для розшифрування повідомлень, та підвищити ефективність розшифрування. Іншим напрямком досліджень є розробка нових методів криптоаналізу, зокрема, методів на основі квантових обчислень. Квантові комп'ютери можуть швидко вирішувати задачі, які є надзвичайно складними для класичних комп'ютерів, що дозволяє розв'язувати складні криптографічні проблеми. Також відбувається розробка нових методів криптоаналізу, які базуються на аналізі структури шифрів та використанні технік лінійного та диференціального криптоаналізу. Ці методи дозволяють знаходити слабкі місця в криптографічних протоколах та підвищувати рівень їх захисту. Отже, останні дослідження в галузі криптоаналізу та розшифрування зашифрованих повідомлень свідчать про постійний розвиток методів криптоаналізу та пошук нових шляхів для подолання криптографічних захистів. Дослідження в галузі криптографії є надзвичайно важливими для забезпечення безпеки та конфіденційності інформації в сучасному світі [1].

Метою даного дослідження є вивчення різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень. Для досягнення цієї мети, будуть розглянуті різні методи криптоаналізу, включаючи статистичний аналіз, методи побітового перебору, методи лінійного та диференціального криптоаналізу та інші. Крім того, будуть досліджені різні аспекти ефективності цих методів, включаючи час виконання, складність обчислень, кількість залежностей від вхідних даних та інші. Результати дослідження можуть бути використані для вдосконалення криптографічних методів та підвищення рівня захисту інформації.

Задача даного дослідження полягає в дослідженні різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень.

Конкретні цілі дослідження включають:

1. Огляд різних методів криптоаналізу, включаючи статистичний аналіз, методи побітового перебору, методи лінійного та диференціального криптоаналізу та інші.
2. Дослідження ефективності різних методів криптоаналізу, включаючи час виконання, складність обчислень, кількість залежностей від вхідних даних та інші.
3. Вивчення сучасних методів криптоаналізу на основі машинного навчання, зокрема, нейронних мереж.

4. Дослідження можливостей використання квантових обчислень для криптоаналізу.
5. Порівняння різних методів криптоаналізу та визначення їхньої ефективності в розшифруванні зашифрованих повідомлень.

Дослідження різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень може бути виконане з використанням формул та математичних методів. Основна мета такого дослідження полягає у визначенні ефективності різних методів криптоаналізу та їх можливостей в розшифруванні зашифрованих повідомлень.

Для початку, можна розглянути базові методи криптоаналізу, такі як аналіз частоти вживання символів, аналіз взаємодії символів, аналіз повторюваності та інші. Для кожного з цих методів можна розробити математичні моделі, що дозволять вивчити їх ефективність та можливості в розшифруванні зашифрованих повідомлень.

Наприклад, для аналізу частоти вживання символів можна використовувати формулу:

$$p_i = \frac{n_i}{N}, \quad (1)$$

де p_i – ймовірність вживання символу i, n_i - кількість входжень символу i в повідомленні, N – загальна кількість символів у повідомленні.

Для аналізу взаємодії символів можна використовувати формули теорії інформації, наприклад, формулу Шеннона:

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i, \quad (2)$$

де H – ентропія повідомлення, p_i – ймовірність вживання символу I [2].

Далі можна розглянути більш складні методи криптоаналізу, такі як диференціальний криптоаналіз, лінійний криптоаналіз, диференціальний криптографічний аналіз та інші. Для кожного з цих методів можна розробити відповідні математичні моделі, що дозволять вивчити їх ефективність та можливості в розшифруванні зашифрованих повідомлень.

Наприклад, для диференціального криптоаналізу можна використовувати формулу Хемінга для підрахунку відстані між двома бінарними послідовностями:

$$d(x, y) = \sum_i (x_i \oplus y_i), \quad (3)$$

де d(x, y) – відстань Хемінга між послідовностями x та y, Σ_i – сума, що виконується по всім позиціям i, xi - i-й біт послідовності x, yi – i-й біт послідовності y, $\oplus$ – бінарна операція "XOR" (ексклюзивне "або") [3].

Таким чином, дослідження різних методів криптоаналізу та їх ефективності в розшифруванні зашифрованих повідомлень може бути проведене з використанням різних математичних формул та методів, що дозволять вивчити їх ефективність та можливості в розшифруванні зашифрованих повідомлень.

Список літератури

1. *Lawrence C. Cryptography and Network Security: Principles and Practice [Текст] / В. Сталлінгс; пер. з англ. І. Мельниченка. - К.: Видавничий дім "Інтерсервіс", 2019. - 784 с.: іл.*
2. *Столлінгс, В. Introduction to Cryptography with Coding Theory [Текст] / В. Столлінгс; пер. з англ. І. Мельниченка. - К.: Видавничий дім "Інтерсервіс", 2018. - 704 с.: іл.*
3. *Менезес, А., ван Ооршот, П., та Ванстраффелт, Б. Handbook of Applied Cryptography [Текст] / А. Менезес, П. ван Ооршот, Б. Ванстраффелт; пер. з англ. О. Козаченко. - К.: Видавничий дім "Інтерсервіс", 2020. - 820 с.: іл.*

УДК 004.6

Мишківська Я.В., студентка 1 курсу
спеціальності 122 «Комп'ютерні науки»
Гончар В.М.,асистент
кафедри інформаційних технологій

ВИКОРИСТАННЯ ГРАФОВИХ БАЗ ДАНИХ НА ПРИКЛАДІ СИСТЕМИ УПРАВЛІННЯ БАЗАМИ ДАНИХ NEO4J

Донецький національний університет імені Василя Стуса, м. Вінниця

Графові бази даних - це нове покоління баз даних, які використовують графову модель зберігання даних, тому значення їх у сучасному світі зростає з кожним роком. Головна перевага графових баз даних полягає в тому, що вони дозволяють зручно відображати та аналізувати зв'язки між об'єктами. Однією з найбільш популярних графових баз даних є система управління базами даних Neo4j, яка надає широкі можливості для зберігання, обробки та аналізу графових даних.

Neo4j - це повнофункціональна графова база даних, яка включає в себе сім компонентів для зберігання, обробки та аналізу даних у вигляді графів[1]. Основні компоненти, можна переглянути на рис.1 :

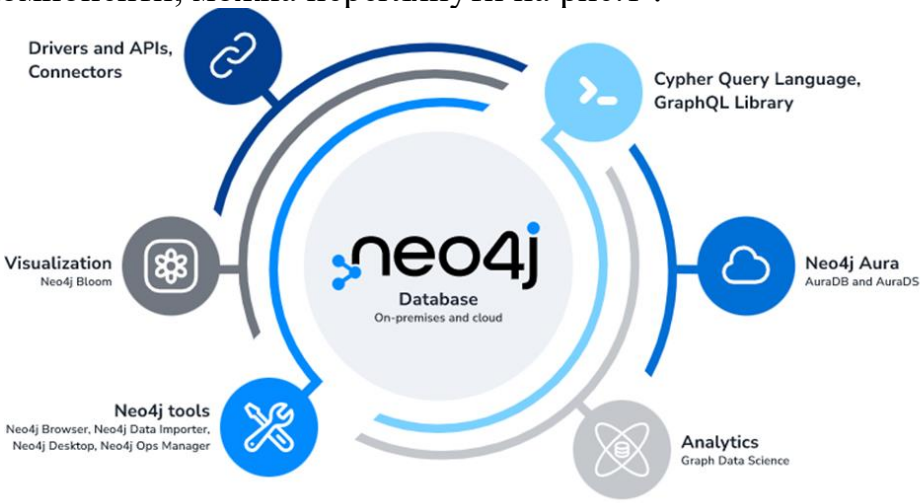

Рис. 1 Компоненти Neo4j