УДК 004.056(075.8)

А.Є. Москаленко

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ ІЗ КРИПТОГРАФІЇ

Вінницький національний технічний університет

Анотація

У цій статті розглядається використання Штучного Інтелекту у криптографії, важливість Штучного Інтелекту, безпеку використання Штучного Інтелекту та поєднання новітніх технологій, через які безпека даних може стати кращою.

Ключові слова: Штучний Інтелект, безпека, дані, криптографія, шифрування, дешифрування, аналіз, ключ, методи, конфіденційність

Abstract

This article examines the use of Artificial Intelligence in cryptography, the importance of Artificial Intelligence, the security of using Artificial Intelligence, and the combination of the latest technologies that can improve data security.

Keywords: Artificial Intelligence, security, data, cryptography, encryption, decryption, analysis, key, methods, privacy

Вступ

Криптографія –це наука та практика надсилання безпечних зашифрованих повідомлень чи даних між двома і більше сторонами. [1]. Іншими словами, криптографія- це наука збереження таємниці інформації та її захисту [1]. Також, можна сказати, що це навмисне приховування даних, задля їх безпеки. Криптографічні методи шифрування можна поділити на симетричні і асиметричні. Симетрична криптографія використовує один й той самий ключ для шифрування та розшифрування. Прикладом може бути: AES, DES. Асиметрична криптографія використовує для шифрування та дешифрування даних різні ключі. Наприклад: RSA, ECC.

Перспективним виглядає застосування ШІ до створення навчальних тренажерів, зокрема навчальних Maple-тренажерів [4, 5, 6, 7, 8, 9].

Особливо ефективним ШІ є у допомозі створення програмного коду, навіть для середовищ, що не входять до ТОП найпопулярніших, [10, 11, 12].

Наразі Штучний Інтелект стає незамінним у вирішенні широкого кола задач. Отже, цікавим є дослідження ефективності застосування ШІ для розв'язання задач з математичних основ криптографії. ШІ - це область науки, яка вивчає створення комп'ютерних систем, здатних аналізувати інформацію, вирішувати завдання та вчитися на власних помилках[2].

Розглянемо способи якими ШІ допомагає у вирішенні задач з криптографії:

1. Розробка нових методів шифрування : ШІ дійсно може допомогти розробникам знайти та реалізувати більш надійні шифри;
2. Аналіз даних: ШІ може допомогти аналізувати великі потоки даних та шукати в них помилки чи дані про атаки;
3. Розробка методів хешування даних: ШІ можна використовувати для створення нових хеш-функції, які будуть більш безпечні та менш вразливими;
4. Розробка нових методів дешифрування: також ШІ може допомагати розшифровувати дані підбираючи правильні ключі;

5. Попередження атак: ШІ може допомогти виявити загрозу та знищити її. Також ШІ може аналізувати підозрілі дії, тим самим сповіщаючи про це спеціалістам з безпеки;
6. Безпека користувачів: ШІ може забезпечити підсилену безпеку користувачам через наприклад, біометричні дані (обличчя, відбиток пальця);
7. Генерація безпечних ключів: ШІ може генерувати випадкові ключі та перевіряти їх на безпеку.

Штучний Інтелект також має дуже багато недоліків. Наразі відомо, що ШІ не повністю розвинутий у всіх сферах, особливо у математичній. ШІ не може обчислювати дуже великі числа та вирішувати задачі.

Визначимо недоліки ШІ:

1. ШІ може бути розробником атак: дійсно, якщо ШІ може розробляти захист, то і може розробляти атаки. Тому великий ризик, що шахраї використають ШІ у своїх цілях;
2. Порушення конфіденційності: ШІ використовуючи дані для аналізу може порушити конфіденційність користувачів, і через якусь помилку чи загрозу надати ці дані у вільний доступ.

Висновок

Штучний інтелект є вельми потужним інструментом у сфері криптографії, що важлива для забезпечення конфіденційності та безпеки інформації в сучасному світі [3]. Застосування ШІ в криптографії дозволяє зміцнювати і покращувати методи шифрування та розшифрування, генерувати безпечні ключі, аналізувати великі обсяги даних і виявляти аномалії у поведінці користувачів [3]. Але також Штучний Інтелект має недоліки, такі як розроблення атак, крадіжка даних, порушення конфіденційності. Але завдяки ШІ ми дійсно можемо зробити криптографію безпечнішою і стійкішою до атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стасюк М. Елементи математичних основ криптографії: навчальний посібник / Марта Стасюк – Львів : ЛДУ БЖД, 2021. – 216 с. 2021
2. Introducing ChatGPT. <https://openai.com/blog/chatgpt> (2023, листопад, 02).
3. Bard.< https://bard.google.com/chat> (2023, листопад, 02).
4. Михалевич В. М., Тютюнник О. І. Використання систем комп'ютерної математики у процесі навчання лінійного програмування студентів ВНЗ: монографія. Вінниця: ВНТУ, 2016. 279 с.
5. Михалевич В. М., Крупський Я. В. Розвиток системи Maple у навчанні вищої математики майбутніх інженерів-механіків : монографія. Вінниця: ВНТУ, 2013. 236 с.
6. Михалевич В. М., Туржанська О. С. Навчальний Maple-тренажер для знаходження рівняння дотичної, яка проведена до графіка функції y=f(x) у точці x0 та їх графічного відображення. LI науково-технічна конференція підрозділів Вінницького національного технічного університету (НТКП ВНТУ-2022) : збірник доповідей [Електронний ресурс].Вінниця : ВНТУ,2022. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/17048
7. Михалевич В.М., Немировська Д.О. Використання штучного інтелекту у вивченні математики. LI науково-технічна конференція підрозділів Вінницького національного технічного університету (НТКП ВНТУ-2022) : збірник доповідей [Електронний ресурс]. Вінниця : ВНТУ, 2022. URL: https://d.conf.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/17459
8. Михалевич В. М. Навчальний Maple-тренажер з обчислень за розширеним алгоритмом Евкліда/ В. М. Михалевич, О. І. Тютюнник, О. Корінний // Матеріали Всеукраїнськьої науково-методичної конференції «Сучасні науково-методичні проблеми математики у вищій школі», 23 – 24 травня 2022 р. – К.: НУХТ, 2022р. – 133 с.. – С. 80-83. https://drive.google.com/file/d/1VlroDm7xDJuf9mjRYoWK2nsRX-cVqaSR/view.
9. Mykhalevych V, Turzhanska I., Nemyrovska D. Joint use of chatgpt, maple and maxima in teaching mathematics and computer science /V. Mykhalevych, I. Turzhanska, D. Nemyrovska // в збірнику тез IV Всеукраїнської науково-практичної Інтернет-конференція «Математика та інформатика в науці й освіті: виклики сучасності», (присвячена 90-річчю кафедри математики та інформатики) 25-26 травня 2023 року, Вінниця, 2023. –С. 198-200.
10. Михалевич В. М. Комп`ютерна програма "Maple програма генерування індивідуальних завдань з теми «Порівняння першого степеня» " / Михалевич В. М.,Тютюнник О. І., Коломієць А. А., Пінчук Д. О., Фещук А. В., Добранюк Ю. В. // Свідоцтво про реєстрацію авторського права на твір № 120820 від 29.09.2023 р.
11. Михалевич В. М. Комп`ютерна програма "Навчальний Maple-тренажер з методу факторизації Ферма" / Михалевич В. М., Тютюнник О. І., Коломієць А. А., Пінчук Д. О., Салямон Я. Ю. // Свідоцтво про реєстрацію авторського права на твір № 120821 від 29.09.2023 р.

12. Михалевич В. М. Комп`ютерна програма "Maple програма генерування індивідуальних завдань з теми «Шифрувальні матриці» " / Михалевич В. М., Тютюнник О. І., Коломієць А. А., Пінчук Д. О., Магденко А. Р., Добранюк Ю. В. // Свідоцтво про реєстрацію авторського права на твір № 120822 від 29.09.2023 р.

Москаленко Аліна Євгеніївна- студентка групи 1БКС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: moskalenkoalina56@gmail.com

Науковий керівник: ***Володимир МаркусовичМихалевич***— д-р техн. наук, професор, завідувач кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail:vmykhal@gmail.com

Moskalenko Alina Evgeniivna- student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: moskalenkoalina56@gmail.com

Supervisor: ***MykhalevychVolodymyrM.*** —Dr. Sc. (Eng.), Professor, Head of the Chair for HigherMathematics, Vinnytsia National Technical University, Vinnytsia, vmykhal@gmail.com.