НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання кваліфікаційного дослідження

НАЗВА ДОСЛІДЖЕННЯ

Виконав студент
групи ФІ-13
Дідух Максим Андрійович

Науковий керівник:
кандидат технічних наук, доцент
Кучинська Наталія Вікторівна

Київ — 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ФТІ — Фізико-технічний інститут ШІ - штучний інтелект Імовірнісна контекстно-вільна граматика (Probabilistic Context-Free Grammar) - ІКВГ

ВСТУП

1 ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИПТОГРАФІЇ, ПРИ ПІДБИРАННІ ПАРОЛІВ ТА ЇХ ГЕШІВ

У першому розділі даної роботи ми розглянемо зв'язок між криптографією та штучним інтелектом (далі ШІ), детальніше познайомимось із застосовуванням ШІ в симетричній та асиметричній криптографії. Після чого перейдемо до основної теми дослідження, а саме - проблемі вгадування паролів та їх гешів, для цього введемо поняття геш-функції (не певен що воно потрібне), розглянемо актуальні техніки для вгадування паролів та їх гешів.

1.1 використання ai в крипті

1.1.1 Використання ШІ та evolutionary computing для генерування алгоритмів шифрування

Наукова робота Cryptography using Artificial Intelligence Jonathan Blackledge норм цитуванняпредставляє інноваційний підхід до шифрування з використанням нейронних мереж та еволюційних обчислень. Автори пропонують метод, який відходить від традиційних підходів до шифрування, генеруючи персоналізовані алгоритми шифрування, а не просто використовуючи персональні ключі з відомими алгоритмами.

Основна концепція полягає у використанні природних джерел шуму, таких як атмосферний шум від радіовипромінювання та радіоактивного розпаду, для навчання систем, які можуть генерувати унікальні алгоритми шифрування. Процес починається з подачі цих природних джерел шуму в систему, яка потім вчиться апроксимувати вхідний шум для створення нелінійних функцій. Ці функції згодом використовуються як ітератори і

проходять ретельне тестування на криптографічну стійкість, включаючи перевірку на показники Ляпунова, рівні ентропії, довжину циклу і характеристики дифузії ключа.

Що робить цей підхід особливо цінним, так це його здатність генерувати необмежену кількість унікальних генераторів псевдовипадкових чисел (ГПВЧ), які можуть бути використані на індивідуальній основі. Це особливо актуально для сучасних додатків, таких як безпечні хмарні сховища, де користувачі можуть отримати персоналізовані алгоритми шифрування, а не покладатися на стандартні алгоритми, які можуть бути вразливими до відомих алгоритмічних атак.

Дослідження є значним кроком вперед у галузі криптографії, пропонуючи новий спосіб підвищити безпеку даних завдяки застосуванню штучного інтелекту.

1.1.2 Applications of Neural Network-Based AI in Cryptography

Applications of Neural Network-Based AI in Cryptography пофіксити цитування ШІ також має місце для застосування в класичних криптографічних системах, зокрема RSA і AES. Оскільки дослідники продовжують вивчати нові підходи, штучний інтелект став цінним інструментом у розумінні та оцінці цих криптографічних стандартів.

У криптографічній системі RSA штучний інтелект і нейронні мережі продемонстрували неабиякий потенціал у кількох ключових сферах. Нейронні мережі можна навчити розпізнавати складні шаблони в процесах генерації ключів RSA, потенційно виявляючи слабкі місця, які традиційний аналіз може пропустити. Наприклад моделі глибокого навчання (deep learning) можуть аналізувати великі масиви даних ключів RSA для виявлення статистичних закономірностей і потенційних вразливостей в алгоритмах генерації ключів. Алгоритми машинного навчання продемонстрували успіх в оптимізації вибору і реалізації параметрів RSA, що потенційно підвищує безпеку і продуктивність. Підходи на основі

штучного інтелекту навіть почали кидати виклик деяким традиційним припущенням про безпеку ключів RSA.

Штучний інтелект також відкриває нові підходи до криптоаналізу алгоритмів симетричного шифрування, тут буде згадані тільки деякі результати для алгоритму AES, але слід зазначити, що аналогічні результит можна отримати і для інших алгоритмів. Нейронні мережі успішно застосовуються для аналізу процесів шифрування та дешифрування, намагаючись виявити тонкі закономірності або слабкі місця, які можуть бути використані. Методи машинного навчання виявилися особливо цінними при проведенні атак побічних каналів, коли системи штучного інтелекту аналізують найдрібніші зміни в енергоспоживанні, електромагнітних випромінюваннях і хронометражі під час операцій шифрування. Ці підходи показали багатообіцяючі результати в прогнозуванні ключових бітів AES і підтримці ширших криптоаналітичних зусиль. Дослідники також розробили моделі штучного інтелекту, здатні аналізувати статистичні властивості операцій AES, потенційно виявляючи раніше невідомі вразливості. Застосування глибокого навчання для диференціального та лінійного криптоаналізу AES відкрило нові шляхи для розуміння властивостей безпеки шифру.

Хоча штучний інтелект продемонстрував значний потенціал у криптографічному аналізі, наразі він слугує скоріше додатковим інструментом, ніж заміною традиційним методам. Подальший розвиток методів штучного інтелекту в криптографії відкриває нові можливості для майбутніх досліджень і розробок.

1.2 означення геш функцій, ???мд5 геш функції???

1.3 Password Guessing via Neural Language Modeling, щось типу імовірності та нейро підходи до взламу паролів, мб розділити на дві секції

Паролі є найбільш поширешим способом аутентифікації, імовірніше за все, через те, що їх легко запам'ятати та реалізувати. Незважаючи на цінність даних, доступ до яких надає кожен конкретний пароль, середньостатистичний користувач все ще використовує відносно прості паролі, що мають семантичний зміст та легко запам'ятовуються. Все це робить користувацькі паролі все більш вразливи до загроз реального світу. Посилаючись на дослідження Пірмана [14], 40% користувачів використовують один і той же пароль на декількох різних платформах. Існує велика кількість різних технік для вгадування паролів, всі вони націлюються на взлам як можна більшої кількості паролів за найменшу кількість спроб. Виділяють два основних типи атак - онлайн та оффлайн.

Означення 1.1. Оффлайн атака - атака під час якої, атакуючий якимось чином отримати певну кількість криптографічних гешів паролів користувачів та намагається відновити їх вгадуючи та тестуючи велику кількість паролів.

Означення 1.2. Онлайн атака - атака під час якої, атакуючий робить спроби вгадати пароль через web-інтерфейс або додаток.

Зауваження. Слід зазначити, що онлайн атаки є більше обмеженими тому, що більшість web-інтерфейсів та додатків, обмежують можливість надсилання запитів після певної кількості невдалих спроб. Таких обмежень не може бути у випадко оффлайн атак тому, що в такому випадку, атакуючи ніяк не взаємодіє з іншими сервісам, виконуючи вгадування локально на своєму персональному комп'ютері.

До того ж існує й інші властивості атак, які визначають кількість інформації про користувача, що має атакуючий. Тут також є два основних типи - тралення (англ. trawling) та націлене вгадування.

Означення 1.3. Націлене вгадування виникає тоді, коли атакуючий намагається дізнатись пароль користувача використовуючи будь-які дані, що мають відношення до конкретного користувача.

Ванг [15] запропонував класифікувати таку інформацію на дві категорії в залежності від ступеня конфіденційності. Перший тип - це особиста інформація користувача інформація, що надає змогу ідентифікувати користувача, включаючи ім'я, електронну пошту, тощо. Другий тип - це ідентифікаційні дані користувача, які є частково публічними (наприклад, ім'я користувача) і частково приватними (наприклад, пароль).

Означення 1.4. Тралення (англ. trawling) - атака, під час якої, атакуючий намагається знайти користувача, що відповідає уже відомому паролю.

Означення 1.5. Більшість користувачів не заслуговують націлених атак, як правило кількість ресурсів які атакуючий витратить на націлену атаку перевищить кількість ресурсів, які він отримає після успішного взламу. Сконцентрованої уваги заслуговують лише спеціальні користувачі, що стосуються критичної інфраструктури, фінансових установ або документів.

Далі наведені деякі з них. Слід зазначити, що всі вони використовують trawling offline guessing, коли атакуючий якимось чином здобув доступ до бази даних, що містить геші паролів.

1.4 Rule based models

На просторах мережі Інтернет можна зайти величезну кількість викрадених паролів, ось найбільші з них [16]:

Джерело	К-ть паролів
phpBB	3.0×10^5
Yahoo	4.4×10^5
Rock You	1.4×10^7
Myspace	5.5×10^4
SkullSecurityComp	6.7×10^6
LinkedIn	1.3×10^6

Таблиця 1.1 – Відомі відкриті бази паролів

Велика кілтькість викрадених паролів справжніх користувачів сильно спрощує вивчення та збір шаблонів/патернів паролів. Маючи таку велику вибірку можна створити нові паролі-кандидати, використовуючи наявні як приклад. Прикладами таких реалізацій є John The Ripper3 [17] та Hashcat 2 [18], ці програми реалізують велику варіативність методів взламу паролів, таких як прямий перебір, атаки з використанням словників та rule-based атак, яка є найшвдишею серед усіх атак.

Зауваження. Rule-based системи генерують паролі виключно базуючись на вже відомих правилах, а створення нових правид є складною задачею та вимагає великого рівня експертизи. Як наслідок, паролі, для яких складно побудувати правила будуть взламуватись набагато важче, якщо будуть взагалі.

1.5 Імовірністі моделі

1.5.1 Марковська модель

Марковська модель являє собою фундаментальний підхід до підбору паролів, що походить від принципів мовного моделювання та була представлення в статті Fast dictionary attacks on passwords using timespace tradeoff [?]. Ця модель передбачає наступні символи в послідовності на основі попередніх символів, причому довжина контексту, відома як «порядок», відіграє вирішальну роль в її ефективності. Еволюція моделі зазнала значних покращень завдяки дослідженням Ma [6], які запровадили складні методи, такі як нормалізація кінцевих символів та згладжування

Лапласа. Нормалізація кінцевих символів працює шляхом додавання певного символу до паролів, гарантуючи, що розподіли ймовірностей зберігають математичну узгодженість. Згладжування за Лапласом вирішує критичну проблему надмірної підгонки шляхом введення дельта-значення до підрахунку підрядків, що особливо корисно для марковських моделей вищих порядків, які обробляють більш обширну контекстну інформацію.

1.5.2 Модель PCFG

Модель як це має бути? краще укр? і укр і англ? Probabilistic Context-Free Grammar (PCFG), представлена Вейром [3] у 2009 році, являє собою складний підхід до аналізу паролів за допомогою структурної декомпозиції. Ця модель ґрунтується на фундаментальній передумові, що паролі можна розбити на незалежні шаблонні структури, кожна з яких містить окремі термінали. Модель обчислює ймовірності паролів шляхом множення ймовірностей структур і відповідних їм терміналів. Наприклад, пароль типу «rockyou123» аналізується шляхом розбиття його на окремі структури («L7» для літер і «D3» для цифр) і відповідні їм закінчення («rockyou» і «123»). Можливості моделі було значно розширено завдяки кільком інноваціям, включаючи інтеграцію винести означення кудись красиво піньїнь для аналізу китайських паролів у роботі Лі [5], а також включення шаблонів клавіатури та багатослівних шаблонів [4]. Ма [6] продемонстрував підвищену точність вгадування, проаналізувавши шаблони кінцевих частот у навчальних даних.

Зауваження. я б хотів щоб це було не зауваженням, а просто як ?зноска? дрібним шрифтом знизу Піньїнь, повна офіційна назва Ханьюй піньїнь — найпоширеніший стандарт латинізування китайської мови, тобто позначення звуків китайської за допомогою латинської абетки. source

1.6 Deep learning based models

На відміну від rule-based та імовірнісних моделей вгадування паролів, методи глибинного навчання не роблять жодних припущень щодо структури паролів. Множини паролів згенеровані таким методом не обмежуються лише певною підмножиною відомих паролів.

Нейронні мережі, особливо мережі з довгою короткочасною пам'яттю теж саме запитання що і в PCFG(LSTM) [9], представляють собою передову технологію підбору паролів. Ці мережі є обчислювальними моделями, які імітують біологічні нейронні мережі, пропонуючи складні можливості апроксимації функцій. Нейромережевий підхід долає суттєве обмеження марковських моделей - обмеження контексту фіксованої довжини - шляхом збереження довгострокових залежностей у даних. Меліхер [8] вперше застосував цей підхід, використовуючи LSTM-мережі для вилучення та прогнозування ознак паролів, хоча їхня оцінка була обмежена обмеженою обмежена обмеженими структурами та даними [10]. З тих пір ця область розвивалася за допомогою різних інноваційних підходів, включаючи впровадження Хітай [11] генеративних змагальних мереж same as for LSTM(GAN) для вгадування паролів, хоча це вимагало більше спроб вгадування, ніж моделі на основі LSTM. Лю [12] пішли далі, створивши гібридний підхід, який поєднав правила PCFG з LSTM-мережами, показавши значні покращення. Однак їхнє тестування було обмежене 10^{12} вгадуваннями, тоді як реальні сценарії тралення в автономному режимі часто вимагають до 10^{16} спроб. Сюй [13] також реалізували мережі LSTM, але обмежили їх оцінку до 10^{10} вгадувань, не проводячи комплексної оцінки.

1.7 GNPassGAN: Improved Generative Adversarial Networks For Trawling Offline Password Guessing

1.7.1 Generative Adversarial Networks (GANs) networks overview

Генеративні змагальні мережі (GAN), представлені Гудфеллоу у 2014 році [19], представляють собою революційний підхід до генеративного моделювання з використанням глибокого навчання чи глибинного?. Архітектура реалізує змагальну структуру, де дві нейронні мережі змагаються одна проти одної в грі на додати пояснення того, що таке мінімакс? мінімакс. Перша мережа, відома як Генератор (G), створює синтетичні дані, намагаючись імітувати реальний розподіл даних, тоді як друга мережа, Дискримінатор (D), має на меті розрізняти реальні та згенеровані дані.

Фундаментальна робота GAN полягає в тому, що Генератор приймає випадковий шум з латентного простору як вхідний сигнал і виробляє синтетичні зразки. Одночасно Дискримінатор функціонує як розписати про нього більше? двійковий класифікатор, виводячи ймовірність того, що будь-який вхідний сигнал є справжнім, а не згенерованим. Завдяки цьому змагальному процесу навчання обидві мережі постійно вдосконалюють свої можливості: Генератор покращує свою здатність створювати більш переконливі синтетичні дані, тоді як Дискримінатор вдосконалюється у виявленні.

1.7.2 Common use cases of GANs

GANs продемонстрували неабиякий успіх у різних галузях. У сфері комп'ютерного зору такі архітектури, як StyleGAN [20], зробили революцію у створенні синтетичних зображень, створюючи фотореалістичні людські

обличчя, які неможливо відрізнити від справжніх фотографій. Медична галузь використовує GANs для створення синтетичних даних медичних зображень, вирішення проблем конфіденційності та доповнення обмежених наборів даних для рідкісних захворювань.

Ще одним значним проривом стало перетворення тексту в зображення: такі моделі, як DALL-E [21] і Stable Diffusion [22], використовують архітектуру, натхненну GAN, для створення зображень з текстових описів. В аудіо області GAN дозволили синтезувати голос і створювати музику, в той час як в обробці відео вони сприяли прогнозуванню кадрів і поліпшенню якості відео [23].

Висновки до розділу 1

2 (НАЗВА ДРУГОГО РОЗДІЛУ)

Висновки до розділу 2

ВИСНОВКИ

Загальні висновки повинні відобразити результати вашого дослідження згідно задачі, окресленої у вступі.

Висновки не повинні містити формул, рисунків та таблиць. Вони повинні бути чіткими, сухими, лаконічними та змістовними. Ви повинні вказати, що саме було зроблено, що з цього випливає і окремо – що робити далі (напрямки подальшого дослідження, яке у вашому випадку співпадає із задачею дипломного дослідження).

ПЕРЕЛІК ПОСИЛАНЬ

1. Rivest, R. L. (1991). Cryptography and Machine Learning. Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, pp. 428-435. https://people.csail.mit.edu/rivest/pubs/Riv91.pdf

2. Hang Li, Mengqi Chen, Shengbo Yan, Chunfu Jia, and Zhaohui Li (2019). Password Guessing via Neural Language Modeling. Tianjin Key Laboratory of Network and Data Security, Nankai University

3. Weir, M., Aggarwal, S., De Medeiros, B., Glodek, B.: Password cracking using probabilistic context-free grammars. In: Security and Privacy, 2009 30th IEEE Symposium on. pp. 391–405. IEEE (2009 https://www.researchgate.net/publication/220713709_Password_Cracking_Using_Probabilistic_Context-Free_Grammars

4. Houshmand, S., Aggarwal, S., Flood, R.: Next gen pcfg password cracking. IEEE Trans. Information Forensics and Security 10(8), 1776–1791 (2015

5. Li, Z., Han, W., Xu, W.: A large-scale empirical analysis of chinese web passwords. In: USENIX Security Symposium. pp. 559–574 (2014

6. Ma, J., Yang, W., Luo, M., Li, N.: A study of probabilistic password models. In: Security and Privacy (SP), 2014 IEEE Symposium on. pp. 689–704. IEEE (2014)

7. Narayanan, A., Shmatikov, V.: Fast dictionary attacks on passwords using time- space tradeoff. In: Proceedings of the 12th ACM conference on Computer and communications security. pp. 364–372. ACM (2005)

8. Melicher, W., Ur, B., Segreti, S.M., Komanduri, S., Bauer, L., Christin, N., Cra- nor, L.F.: Fast, lean, and accurate: Modeling password guessability using neural networks. In: USENIX Security Symposium. pp. 175–191 (2016)

9. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. pp. 1735–1780 (1996)

10. Merity, S., Keskar, N.S., Socher, R.: Regularizing and optimizing lstm

language models. arXiv preprint arXiv:1708.02182 (2017)

11. Hitaj, B., Gasti, P., Ateniese, G., Perez-Cruz, F.: Passgan: A deep learning ap- proach for password guessing. In: International Conference on Applied Cryptogra- phy and Network Security. pp. 217–237. Springer (2019)

12. Liu, Y., Xia, Z., Yi, P., Yao, Y., Xie, T., Wang, W., Zhu, T.: Genpass: A general deep learning model for password guessing with pcfg rules and adversarial genera- tion. In: 2018 IEEE International Conference on Communications (ICC). pp. 1–6. IEEE (2018

13. Xu, L., Ge, C., Qiu, W., Huang, Z., Gong, Z., Guo, J., Lian, H.: Password guess- ing based on lstm recurrent neural networks. In: Computational Science and En- gineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on. vol. 1, pp. 785–788. IEEE (2017)

14. S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, "Let's go in for a closer look: Observing passwords in their natural habitat," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 295–310.

15. D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in Proceed- ings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1242–1254.

16. GNPassGAN: Improved Generative Adversarial Networks For Trawling Offline Password Guessing

17. todo https://github.com/openwall/john

18. todo https://github.com/hashcat/hashcat

19. https://papers.nips.cc/paper_files/paper/2014/file/
5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf

20. Karras, T., et al. (2019). "A Style-Based Generator Architecture for GANs"

21. https://openai.com/index/dall-e/

22. https://stablediffusion.com/

23. Wang, T.-C., et al. (2018). "Video-to-Video Synthesis"

ДОДАТОК А ТЕКСТИ ПРОГРАМ

Тексти інструментальних програм для проведення експериментальних досліджень необхідно виносити у додатки.

А.1 Програма 1

Зауважте, як змінилась нумерація.

ДОДАТОК Б ВЕЛИКІ РИСУНКИ ТА ТАБЛИЦІ

Якщо результати вашої роботи описуються величезними рисунками і таблицями (один аркуш та більше) у незліченній кількості, їх також необхідно виносити у додатки.