СЕКЦІЯ 2
КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.7

Держанівська А.О., здобувач,
Покотило О.А., ст. викладач,
Щур Н.О., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ КРИПТОГРАФІЧНИХ ЗАВДАНЬ У CTF- ЗМАГАННЯХ

Capture The Flag (CTF) - це формат змагань у сфері кібербезпеки, який моделює реальні сценарії кібератак і захисту інформаційних систем. Оскільки криптографія відіграє важливу роль у кібербезпеці, забезпечуючи конфіденційність та цілісність даних, майже у всіх змаганнях з CTF існує категорія «Крипто» або «Криптографія» [1].

Такі змагання набули значної популярності серед студентів технічних спеціальностей, оскільки дозволяють перевіряти теоретичні знання на практиці. У контексті криптографії участь у CTF сприяє розвитку аналітичного мислення, розумінню принципів роботи шифрів і навчанню нестандартних способів пошуку вразливостей у реалізаціях алгоритмів.

Метою цього дослідження є аналіз та класифікація типових завдань криптографії у CTF-змаганнях, що дозволить студентам та початківцям, які планують брати участь у CTF-змаганнях, краще розуміти принципи побудови таких завдань та ефективніше готуватися до їх розв'язання.

У межах змагань CTF криптографічні завдання можна умовно поділити на кілька типів залежно від принципів шифрування, складності та підходів до розв'язання [2].

Завдання з класичними шифрами. До цієї категорії належать завдання, що базуються на історичних методах шифрування, таких як шифр Цезаря, шифр Віженера, Playfair, Rail Fence тощо. Розв'язання таких завдань зазвичай передбачає частотний аналіз, пошук повторюваних сегментів у тексті та автоматизацію дешифрування за допомогою простих скриптів або утиліт.

Завдання із сучасними алгоритмами шифрування. Ці завдання пов'язані із вивченням та експлуатацією сучасних криптосистем, зокрема RSA, AES, ECC. Учасникам може бути запропоновано знайти вразливість у реалізації алгоритмів шифрування. Такі завдання

допомагають зрозуміти, як навіть стійкі алгоритми можуть бути зламані через помилки в реалізації.

Завдання з хешування. Завдання цієї групи вимагають відновлення вихідних даних із хеш-значення або виявлення колізій. Найчастіше використовуються алгоритми MD5, SHA-1, SHA-256. Основні методи розв'язання - brute-force, словникові атаки або використання попередньо обчислених таблиць (rainbow tables). Для цього застосовуються такі інструменти, як Hashcat та John the Ripper.

Завдання з кодування та декодування. У таких завданнях необхідно розпізнати формат кодування (Base64, Hex, URL-encoding тощо) та відновити початкові дані. Ці задачі часто використовуються як підготовчий етап до складніших криптоаналізів. Найпопулярнішими інструментами є CyberChef та Python-скрипти для автоматизації декодування.

З огляду на практичне виконання цих завдань, на сучасних CTF-платформах учасники працюють в ізольованому середовищі Linux- або Docker-контейнерів. Для розв'язання криптографічних задач часто створюються спеціальні Python-скрипти, які автоматизують рутинні обчислення - наприклад, аналіз підключів, пошук періодів у шифрах потокового типу або підбір відкритих експонент у RSA. У деяких випадках завдання передбачають комбінацію кількох технік - наприклад, кодування, шифрування та хешування в одному файлі, що вимагає від учасників комплексного підходу до розв'язання.

Окрему категорію становлять завдання на криптоаналіз власних або нестандартних реалізацій шифрів, створених авторами завдань спеціально для CTF. Такі задачі дають змогу відпрацьовувати навички аналізу невідомих алгоритмів, виявлення логічних помилок у побудові та тестування гіпотез щодо способів дешифрування. Часто саме цей тип завдань є найскладнішим і вимагає поєднання знань із лінійної алгебри, теорії чисел та програмування.

Проведений аналіз узагальнює типові криптографічні завдання у CTF-змаганнях, визначає основні підходи до їх розв'язання та сприяє розвитку практичних навичок застосування криптографії. Отримані результати можуть бути використані при підготовці навчальних тренажерів з прикладної криптології та формуванні банку завдань для освітніх CTF-платформ.

Список використаних джерел:

1. Cyber University. CTF Practice: Cryptography. URL: https://cyberuniversity.tech/cryptography/ctf-practice

2. cywf. Cryptography Challenges – cywf/ctf-kit GitHub Wiki. URL: https://github-wiki-see.page/m/cywf/ctf-kit/wiki/Cryptography-Challenges