УДК 621.38 https://doi.org/10.30837/IYF.PCEIP.2024.099

# МЕТОДИ КРИПТОАНАЛІЗУ СУЧАСНИХ ШИФРІВ

Гузенко Н. В.
Науковий керівник – к.т.н. Мельникова О. А.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: nikita.huzenko@nure.ua

Nowadays, information plays a key role. Ciphers are used for information protection. Cryptanalysis deals with the discovery of the output text or key that will allow the ciphertext to be decrypted. It plays a very significant role in information security, as it is used both by cipher developers and by hackers who want to gain access to protected data. In order to understand how secure a particular cipher is, you need to analyze it and find bottlenecks in its mathematical base. Cryptanalysis is very important because it studies the security of a cipher and its key, and the key denotes the strength of the entire cryptosystem.

Інформація — це найважливіше, що може бути у сучасному світі. При передаванні та зберіганні конфіденційної інформації треба точно знати, що доступ до неї отримають тільки авторизовані користувачі. Для забезпечення безпеки інформації використовуються криптографічні засоби, які дозволяють виконувати шифрування та автентифікацію джерела інформації.

Для підтримки безпеки необхідно не тільки шифрувати дані, а й проводити аналіз безпеки того чи іншого шифру, тобто аналізувати можливості криптоаналізу. Криптоаналіз — це розділ криптології, що займається математичними методами порушення конфіденційності та цілісності інформації без знання ключа. Він дозволяє також знайти слабкі місця в криптосистемі, що у кінцевому рахунку, призведе до тих же результатів. Криптоаналізом можуть користуватись не тільки розробники, а також і ті, хто бажає отримати доступ до конфіденційних даних (зашифрованої інформації).

Стійкість криптосистеми визначається тільки таємністю ключа, тому що криптосистема являє собою сукупність апаратних і програмних засобів, яку можна змінити тільки при значних витратах часу та ресурсів, тоді як ключ є легко змінюваним об’єктом.

Виділяють такі основні методи атак:

1) на основі шифротексту;
2) на основі відкритих текстів і відповідних шифротекстів;
3) на основі підібраного відкритого тексту;
4) на основі адаптивно підібраного відкритого тексту.

Також можуть розглядатися такі додаткові методи:

1) атака на основі підібраного шифротексту;

2) атака на основі підібраного ключа;
3) “бандитський” криптоаналіз.

Для симетричних шифрів найбільш відомими є наступні методи криптоаналізу:

1) диференційний криптоаналіз (блокові або потокові шифри);
2) лінійний криптоаналіз (блокові або потокові шифри);
3) кореляційний криптоаналіз (потокові шифри);
4) статистичний криптоаналіз (блокові або потокові шифри);
5) атака “грубої сили” (перебір варіантів).

Для асиметричних шифрів можуть застосовуватись:

1) диференційний криптоаналіз;
2) лінійний криптоаналіз;
3) атака “людина посередині”;
4) атака “грубої сили”.

Атака “людина посередині” означає, що між відправником та отримувачем є деякий посередник, який перехоплює всі повідомлення. А також, на початку сесії (на етапі узгодження спільного ключа), цей посередник перехоплює дані та з їх допомогою відновлює ключ. Атака “грубої сили” припускає перебір всіх можливих варіантів ключа шифрування до знаходження пошукового ключа.

Диференційний криптоаналіз — це спроба розкриття секретного ключа блокових шифрів, які засновані на повторному застосуванні криптографічно слабкої цифрової операції шифрування *r*-разів. При аналізі передбачається, що на кожному циклі використається свій підключ шифрування. Конкретний спосіб застосування диференційного криптоаналізу залежить від алгоритму шифрування, що аналізується. Лінійний криптоаналіз використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Даний метод дозволяє знайти ключ, маючи досить велику кількість пар {незашифрований текст, зашифрований текст}.

Кількість та потужність методів криптоаналізу збільшується з кожним роком, а існуючі методи модернізуються, але й методи шифрування постійно вдосконалюються. Також на складність криптоаналізу та стійкість шифрів значно впливає вдосконалення технічної бази. У вітчизняній та іноземній практиці криптоаналізу використовуються одні й ті самі методи але, звичайно, з урахуванням індивідуальних особливостей шифрів.

Список використаних джерел

1. Cryptanalysis | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/Cryptanalysis (дата звернення: 05.03.2024).