УДК 005.94

АНАЛІЗ МЕТОДУ ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Д.Д. Федірко
Науковий керівник – ст. викладач кафедри БІТ Данилов А.Д.
Харківський національний університет радіоелектроніки, м. Харків, Україна
dmytro.fedirko@nure.ua

The article is devoted to the consideration of the main methods of cryptanalysis of string and block encryption systems. As an example, the article analyzes the most well-known methods of cryptanalysis - for linear codes: the method of full key search, side attacks, for block codes: full (total) key search, the method of meeting in the middle, differential cryptanalysis. Particular attention is paid to the method of linear cryptanalysis. After the analysis of open sources of information, an overview of the chosen method, its essence, advantages, disadvantages and scope of application was carried out.

У сучасному світі з кожним днем все більше розвиваються комп'ютерні технології, методи передачі та обробки інформації. На жаль, разом з цим прогресом з'являються і нові види загроз, вразливостей та атак, через які дані користувачів можуть бути втрачені, розкриті або модифіковані. Для захисту інформації в комп'ютерних системах використовуються криптографічні алгоритми, що уберігають користувачів від інформаційних загроз.

Атакуючи алгоритм шифрування, зловмисник зазвичай має дві основні цілі: знайти секретний ключ або знайти відкритий текст, що відповідає зашифрованому. Тому актуальним є проведення досліджень методів криптоаналізу для оцінки стійкості існуючих криптографічних алгоритмів.

Криптоаналіз – це наука про методи здобуття вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього [1].

Найпоширеніші методи криптоаналізу наведені на рисунку 1 [2].

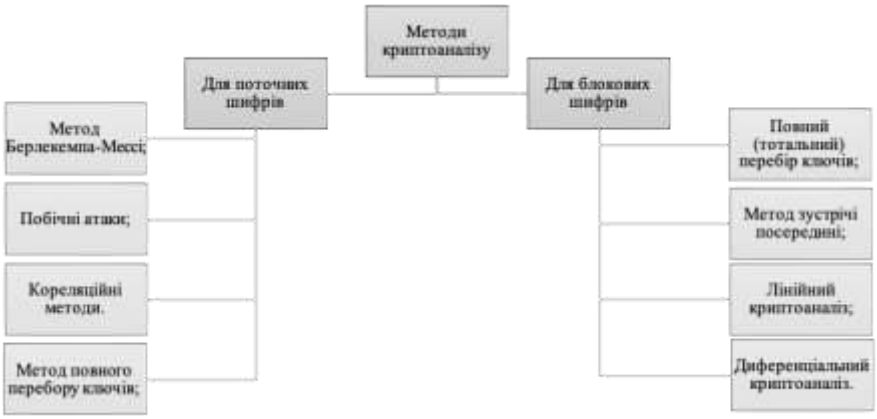

Рисунок 1 − Методи криптоаналізу.

Існує багато методів криптоаналізу, але в роботі детально розглянемо саме лінійний криптоаналіз. Лінійний криптоаналіз є ефективним для аналізу блочних шифрів, оскільки він дозволяє виявити статистичні залежності між вхідними і вихідними бітами шифру. Це допомагає знаходити ключі шифрування та розкривати секретну інформацію.

Лінійний криптоаналіз був винайдений японським криптологом Міцуру Мацуї (Mitsuru Matsui). Даний метод використовує лінійні наближення перетворень, що виконуються алгоритмом шифрування. Цей метод дозволяє знайти ключ, маючи досить велику кількість пар (незашифрований текст, зашифрований текст)[3].

Розглянемо основні принципи, на яких базується лінійний криптоаналіз. Лінійний криптоаналіз базується на тому, що існує можливість замінити нелінійну функцію на її лінійний аналог.

Метою лінійного криптоаналізу є пошук лінійного рівняння виду $P_{i1} \oplus P_{i2} \oplus \dots P_{ia} \oplus C_{j1} \oplus C_{j2} \oplus \dots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} (1)$, де P_n, C_n і K_n - n-і біти відкритого тексту, шифротекста й ключа відповідно.

Для випадково обраних частин відкритого тексту, шифротекста і ключа ймовірність того, що такі біти відповідають один одному, становить приблизно 1/2. Якщо криптоаналітику вдається виявити біти, де ймовірність P відрізняється від 1/2, це співвідношення можна використовувати для розкриття алгоритму.

Це рівняння означає, що при виконанні операції XOR над певними бітами незашифрованого повідомлення і певними бітами зашифрованого повідомлення отримується біт, який є результатом XOR певних бітів ключа. Цей процес відомий як лінійне наближення, яке може бути вірним з ймовірністю P.

Рівняння формуються таким чином: значення лівої частини обчислюються для значної кількості пар відповідних фрагментів незашифрованого та зашифрованого блоків. Якщо результат дорівнює нулю у більш ніж половині випадків, то вважають, що $K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} = 0$. Якщо в більшості випадків виходить $1 - K_{k1} \oplus K_{k2} \oplus \dots \oplus K_{kc} = 1$. Таким чином формується система рівнянь, рішенням якої є ключ. Подібно до диференціального криптоаналізу, результати лінійного криптоаналізу повинні враховуватися при розробці алгоритмів симетричного криптоаналізу.

Лінійний криптоаналіз часто використовується в поєднанні з атакою методом "грубої сили" – певні біти ключа виявляються за допомогою лінійного криптоаналізу, після чого здійснюється вичерпний пошук за можливими значеннями інших бітів.

Лінійний криптоаналіз має одну досить корисну властивість: за певних умов співвідношення (1) може бути перетворене до наступного:

$$C_{j1} \oplus C_{j2} \oplus \ldots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \ldots \oplus K_{kc}.$$

У даному випадку відсутні будь-які біти відкритого тексту у зазначеному співвідношенні, що означає можливість побудови атаки лише на основі шифротексту за допомогою лінійного криптоаналізу. Це ще більше розширює сферу застосування лінійного криптоаналізу, оскільки атака, яка вимагає лише перехопленого шифротексту, є найбільш практичною.

У даний час, існує багато методів криптоаналізу як для поточних шифрів, так і для блокових. Кожен метод криптоаналізу призводить до перегляду безпеки шифрів, до яких він застосовується. Лінійний криптоаналіз − це метод атаки на шифри, який базується на виявленні лінійних зв'язків між вхідними та вихідними бітами шифрувального алгоритму. Незважаючи на свою ефективність у деяких випадках, він має свої недоліки.

По-перше, для успішної реалізації атаки потрібно мати значну кількість пар тексту − шифротексту, що може бути важким завданням, особливо якщо доступ до таких даних обмежений.

По-друге, ефективність атаки може значно залежати від точності вибору початкових умов, тобто визначення правильного вихідного пункту для проведення аналізу.

Незважаючи на ці обмеження, лінійний криптоаналіз широко використовується в криптографії для атак на різні шифри, які використовують лінійні перетворення, такі як DES і AES, а також у дослідженнях нових криптографічних алгоритмів для оцінки їхньої стійкості. Наприклад, метод був успішно використаний для злому DES. У 1994 році, Matsui зміг зламати DES, використовуючи атаку лінійним криптоаналізом, використовуючи близько 2^43 пар тексту-шифротексту.

Таким чином метод лінійного криптоаналізу є доволі розповсюдженим та ефективним методом захисту інформації та може бути успішно використаний для захисту інформаційних активів організації.

Список використаних джерел:

1. Криптоаналіз. Криптографічні протоколи: веб сайт. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/36273 (дата звернення: 27.02.2024).

2. Cryptanalysis in Cybersecurity: веб сайт. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-cryptanalysis (дата звернення: 27.02.2024).

3. Криптоаналіз: веб сайт. URL: https://www.wikidata.uk-ua.nina.az/Криптоаналіз.html (дата звернення: 28.02.2024).