УДК 004.057.4

Дослідження методів криптоаналізу сучасних криптографічних алгоритмів

Лагун А.Е., к.т.н., доцент, a.e.lagun@gmail.com,
Кухарська Н.П., к.ф.-м.н., доцент, kukharska.n@gmail.com
Львівський державний університет безпеки життєдіяльності, м. Львів

На цей час, через бурхливий розвиток комп'ютерної техніки і відкритих мереж, сучасних методів передавання та обробки інформації, з'явилися нові види загроз і вразливостей, пов'язані з можливістю втрати, розкриття, модифікації даних, що належать різним користувачам. Для забезпечення захисту інформації в комп'ютерних системах актуальним є дослідження та вдосконалення криптографічних алгоритмів, що убезпечують користувачів від інформаційних загроз.

Визначення ефективності криптографічних алгоритмів, як правило, є складнішою задачею, ніж його проектування, оскільки воно вимагає більших знань і тому є більше науковою, ніж інженерною задачею. Це призводить до того, що існує велика кількість засобів криптографічного захисту, надійність яких не є визначеною та гарантованою, оскільки алгоритми, на яких вони базуються, є мало дослідженими.

Атаки на криптографічні алгоритми

Основною метою атаки на алгоритм шифрування є знаходження відкритого тексту за допомогою відомого шифротексту і невідомого ключа шифрування або безпосередньо пошук ключа шифрування для можливості розшифрування зашифрованих цим ключем повідомлень. Тому актуальним є проведення досліджень методів криптоаналізу для оцінки стійкості існуючих криптографічних алгоритмів. Класифікацію сучасних методів криптоаналізу наведено на рис. 1.

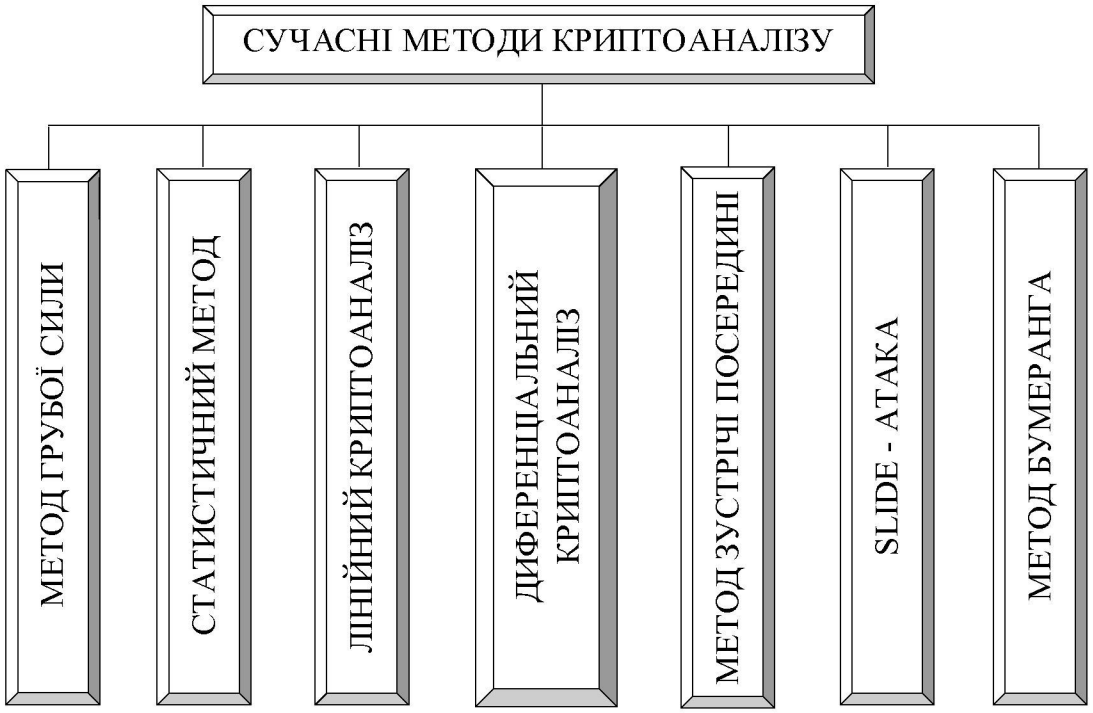

Рисунок 1 – Класифікація сучасних методів криптоаналізу

При використанні методу грубої сили відбувається перебір всіх можливих варіантів ключа шифрування, в результаті чого ключ шифрування буде обов'язково знайдено. Наприклад, якщо потрібно знайти ключ довжиною k біт, то такий пошук вимагатиме 2^{k-1} тестових операцій шифрування. Захистом від атак методом грубої сили є збільшення величини ключа, оскільки при

збільшенні величини ключа на один біт кількість комбінацій ключа шифрування збільшується в два рази.

Зрозуміло, що навіть при сучасному розвитку обчислювальної техніки, метод грубої сили не є ефективним, проте його можна покращити при використанні спеціальних пристроїв перебору або розпаралелюванні процесу пошуку ключів.

При використанні статистичного аналізу потрібно визначити ключ шифрування або його частину, маючи деяку кількість пар "відкритий текст – шифротекст". Основою статистичного аналізу є процедура статистичної класифікації, яка для великої кількості статистичних даних, що вибираються випадковим чином, визначає закон розподілу цих даних і шуканий параметр – ключ шифрування.

Лінійний криптоаналіз поєднує пошук лінійних статистичних аналогів для рівнянь шифрування, статистичний аналіз відкритого та шифротексту, а також методи узгодження та перебору. Даний метод досліджує статистичні лінійні залежності між окремими бітами масивів відкритого, шифротексту та ключа і використовує ці залежності для визначення статистичними методами окремих біт ключа.

У методі лінійного криптоаналізу формуються залежності між відкритим текстом, шифротекстом та ключем. Ці залежності повинні мати високу ймовірність і разом з відомими парами "відкритий текст – шифротекст" використовуються для отримання бітів ключа. Для захисту від атак з використанням лінійного криптоаналізу необхідно досягти того, щоб при будь-якій зміні відкритого тексту або ключа кожен з бітів шифротексту змінювався з різною ймовірністю.

У диференціальному криптоаналізі використовуються пари шифротексту, що мають деяку відмінність. У процесі аналізу досліджуються властивості даної відмінності при шифруванні відкритих текстів одним ключем. Зокрема, вибираються два відкритих тексти з фіксованою відмінністю і після процесу шифрування аналізується відмінність в отриманих шифротекстах. Потім різним ключам присвоюються різні ймовірності. В процесі подальшого аналізу наступних пар один з ключів стане більш ймовірним, тому він і є ключем шифрування.

Існує також посилений варіант диференціального криптоаналізу, який використовує не два, а чотири відкритих тексти та відповідних їм шифротексти, що пов'язані певною структурою, і називається методом бумеранга. Цей метод важко застосувати на практиці.

Метод зустрічі посередині використовує ідею парадоксу днів народження, яка полягає в тому, що для $x\sqrt{y}$ ключів, вибраних з множини y, ймовірність їх збігу дорівнює $(1 - exp(x^2/2))$. Пошук ключа шифрування зводиться до пошуку еквівалентної йому пари. Алгоритм працює так. На першому етапі для відкритого тексту фіксують ключ шифрування і одержаний шифротекст. На другому етапі випадковим чином вибирають ключ розшифрування довільного шифротексту. У випадку збігу шифротекстів і відкритих текстів з першого і другого етапів ключі шифрування з цих етапів будуть шуканим ключем, інакше етапи пошуку повторюють.

Висновки. Розглянуті методи криптоаналізу дають змогу виявити недоліки і слабі місця різних криптографічних алгоритмів, врахувавши які можна підвищити стійкість сучасних криптосистем.

Список літератури

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. – М. : Триумф, 2002.

2. Ковтун В. Ю. Введение в криптоанализ. Криптоанализ симетричных криптосистем: блочные шифры. – Санкт-Петербург, «БХВ-Петербург», 2009.

3. Andriy Lagun Cryptographic Strength of a New Symmetric Block Cipher Based on Feistel Network // Technical Transactions. Series "Automatic Control". – 2013. – Vol. 2-AC (10). – P. 67-80.