УДК 621.391+681.3.06

М.М. Мандрона[1], О.І. Гарасимчук[2]

[1]Національний університет «Львівська політехніка», Львівський державний університет безпеки життєдіяльності, Львів
[2]Національний університет «Львівська політехніка», Львів

КЛАСИФІКАЦІЯ КРИПТОАНАЛІТИЧНИХ АТАК

У даній роботі проводиться аналіз найбільш поширених криптоаналітичних атак та показано способи їх реалізації. Розроблено класифікацію криптоаналітичних атак на основі принципу їх здійснення. Показано, що кожна з атак, має різну складність для криптоаналітика і потребує різної тривалості часу, обчислювальних та інших можливостей.

Ключові слова: *криптоаналітичні атаки, зловмисник, криптоаналітик, шифротекст, відкритий текст, ключі шифрування, генератори псевдовипадкових чисел.*

Вступ

На даний час, проблема захисту інформаційних ресурсів набуває все більшого значення. Необхідність використання на підприємствах різних форм власності і у фінансових установах криптографічних систем зростає з кожним днем. Криптографічна система не може бути надійнішою від окремих алгоритмів, що в ній використовуються. Тобто, для того щоб подолати таку систему захисту, достатньо зламати будь-який з її компонентів. Деякі криптографічні системи втрачають свою надійність, якщо їх невірно використовують. Безпека таких систем часто залежить від даних, які повинні бути відомі лише авторизованим користувачам, і які повинні бути важко вгадуванні для зловмисника. Ще одним недоліком криптографічних засобів є генератори випадкових чисел. Система шифрування може бути виконана на високому рівні, але якщо генератор випадкових чисел видає легко вгадувані ключі, то всі інші бар'єри можна подолати без особливих труднощів. Щоб досягнути необхідного рівня непередбачуваності, за умови частої генерації випадкових чисел, потрібно мати надійне джерело випадкових чисел. На жаль, багато криптографічних програм не є надійним джерелом випадкових послідовностей значень, таких як, наприклад, тепловий шум в електричних колах або точний час між парою спрацьовувань. Замість цього доводиться використовувати генератори псевдовипадкових чисел (ГПВЧ), які отримують на вхід потік даних від джерела з низькою ентропією і намагаються його перетворити в послідовність значень, які практично неможливо відрізнити від справжньої випадкової послідовності [1].

Оскільки, більшість сучасних ГПВЧ побудовані на основі криптографічних алгоритмів шифрування, тим самим, успішна атака на такий генератор може розкрити багато криптографічних систем незалежно від того наскільки ретельно вони були спроектовані. Проте деякі системи використовують неякісно спроектовані ГПВЧ, або роблять це таким чином, що зменшує складність їх подолання зловмисникам. Більше того, потрібно лише одне єдине успішне проникнення, щоб скомпрометувати усю систему. Саме тому, розробникам ГПВЧ варто знати, які саме існують категорії і типи криптоаналітичних атак на алгоритми шифрування, щоб у майбутньому розробляти та практично реалізовувати стійкі ГПВЧ. Отже, актуальним завданням є здійснення класифікації найбільш важливих криптоаналітичних атак.

Метою даної статті є аналіз сучасного стану захисту криптографічних систем від криптоаналітичних атак та проведення класифікації найбільш відомих таких атак.

Криптоаналіз

Історія криптології та криптоаналізу нараховує багато століть, але особливо інтенсивно ця галузь знань стала розвиватися з настанням комп'ютерної ери. Криптографія ставить за мету збереження листування в таємниці від сторонніх людей, які хочуть з нею ознайомитись. Таких людей криптографи називають зловмисниками, противниками, перехоплювачами або просто ворогами. При цьому передбачається, що вони можуть перехоплювати будь-які повідомлення, якими обмінюються відправник та одержувач.

За останні два десятиліття різко зросла кількість відкритих наукових праць по криптоаналізу, який стає галуззю досліджень, що розвиваються найбільш активно. З'явилась велика кількість математичних методів, які складають великий інтерес для криптоаналітика. Крім того, значне зростання продуктивності обчислювальної техніки зробило можливим такі типи атак, які раніш були практично не здійсненні.

Сам термін криптоаналіз був введений відносно недавно. Криптоаналіз полягає в отриманні доступу до відкритого тексту зашифрованого повідомлення без доступу до ключа. В ході успішного криптоаналітичного дослідження криптосистеми можуть бути знайдені не тільки відкритий текст, а й сам ключ. Криптоаналітик займається пошуками слабких місць в криптосистемі, які можуть дозволити йому прочитати зашифроване повідомлення або відшукати ключ. Якщо зловмисник певним чином дізнався ключ не за допомогою криптоаналізу, а використовуючи, якийсь інший спосіб (викрав або купив), то у такому випадку говорять, що ключ був скомпрометований.

Спроба криптоаналізу називається атакою. Успішна криптоаналітична атака зветься зломом, або розкриттям.

У сучасній криптології прийнято вважати, що надійність шифру визначається тільки секретністю ключа, що використовується. Правило, яке вперше сформулював голландець А. Керкхофф (1835-1903), свідчить про те, що весь механізм шифрування, за винятком значення ключа, ймовірно відомий зловмиснику. Це припущення є досить природним, оскільки криптосистема, що реалізує сімейство криптографічних перетворень, переважно реалізується як відкрита система. Якщо шифр неможливо зламати, знаючи абсолютно всі деталі алгоритму шифрування, значить, це тим більше не можна зробити, не володіючи подібними знаннями у всій їх повноті [2].

Атаки на алгоритми шифрування

Здійснюючи атаку, криптоаналітик може ставити собі за мету вирішення наступних завдань:

1) отримання відкритого тексту із зашифрованого;

2) обчислення ключа шифрування.

У загальному випадку, друге завдання є істотно складніше за перше. Однак, маючи ключ шифрування, криптоаналітик може згодом розшифровувати всі зашифровані дані, знайденим ключем. Така атака (в разі її успішного здійснення) називається повним розкриттям алгоритму шифрування.

Атаки на алгоритми шифрування прийнято класифікувати в залежності від набору інформації, який зловмисник має перед здійсненням своєї атаки. На даний час, в наукових працях по криптоаналізу, існують різні спроби класифікації криптоаналітичних атак. Перш за все, криптоаналітичні атаки можна розділити на дві категорії: *пасивні та активні атаки* [2-3].

Пасивні атаки. Криптоаналітик має тільки можливість пасивного прослуховування якогось каналу, по якому пересилаються зашифровані дані. В результаті у зловмисника є лише набір шифротексту, зашифрованого використовуючи, певні ключі. Така атака називається атакою з відомим шифротекстом. Вона найбільш складна, але даний варіант атаки найбільш поширений, оскільки він є «життєвим» – у переважній більшості реальних випадків криптоаналітик не має можливості отримати більше даних.

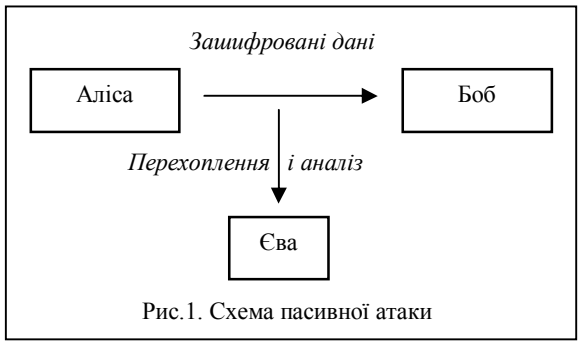

Рис.1. Схема пасивної атаки

Активні атаки. Ця категорія атак, припускає, що у криптоаналітика є якийсь пристрій шифрування з прошитим ключем шифрування, який і є метою атаки. Таким пристроєм, наприклад, може бути криптографічна смарт-карта. Криптоаналітик може виконувати з шифратором певні дії для отримання необхідної йому інформації, наприклад, «проганяти» через шифратор будь-які відкриті тексти для отримання відповідних їм шифротекстів.

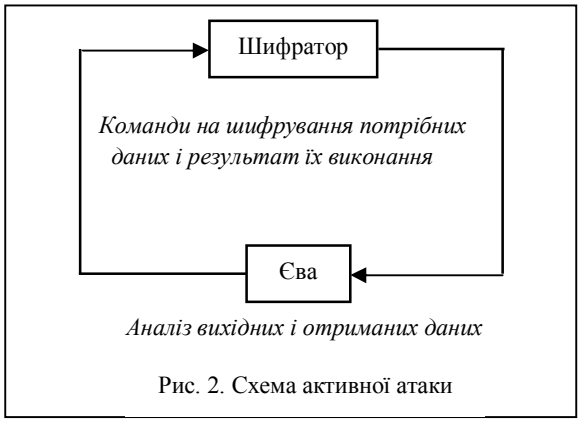

Рис. 2. Схема активної атаки

В результаті проведеного аналізу літературних джерел, нами була запропонована класифікація найбільш відомих криптоаналітичних атак, яка наведена на рис.3.

Основна мета криптоаналітика – намагання розшифрувати частини зашифрованого тексту без додаткової інформації.

Рис.3. Класифікація криптоаналітичних атак

Нижче наведено опис реалізації даних атак приблизно у порядку зростання вразливості інформації, яка є доступною для криптоаналітика або в порядку спадання рівня складності для нього [2-5].

Атака з відомим тільки шифротекстом (*cipher text attack*) полягає у тому, що Єва володіє шифротекстом (ШТ) $(N_1, N_2, ..., N_i)$ декількох відкритих текстів (ВТ) $(P_1, P_2, ..., P_i)$, зашифрованих одним алгоритмом шифрування (АШ). Єва розкриває більшу кількість ШТ або ключів шифрування з метою розкриття інших ШТ, зашифрованих тим самим ключем (*k*). Тобто, маючи $N_1 = Ek(P_1), N_2 = Ek(P_2), \ldots, N_i = Ek(P_i)$ можна визначити $(P_1, P_2, ..., P_i)$ та k або алгоритм відновлення $P_i + 1$ із $N_i + 1 = Ek(P_i + 1)$.

При виконанні цієї атаки криптоаналітику доступна деяка кількість шифротексту, що є результатом застосування одного алгоритму шифрування. Завдання криптоаналітика полягає в тому, щоб знайти якомога більше відкритих текстів, які відповідають наявним шифротекстам, а ще краще – визначити ключ, що використаний при шифруванні. Вхідні дані для атаки на основі тільки шифротекста можуть бути отримані простим перехопленням зашифрованих повідомлень, що при передачі по відкритих каналах зв'язку порівняно легко реалізувати. Дана атака є самою слабкою і незручною для криптоаналітика.

Атака з відомим відкритим текстом (*plaintext attack*) реалізується таким чином, що Єва, володіючи ШТ $(N_1, N_2, ..., N_i)$ і їх ВТ $(P_1, P_2, ..., P_i)$, розкриває *k* з метою подальшого розшифрування інших ШТ, зашифрованих тим же ключем (ключами). Тобто, маючи P_1, $N_1 = Ek(P_1)$, P_2, $N_2 = Ek(P_2), \ldots, P_i$, $N_i = Ek(P_i)$, можна визначити k або алгоритм відновлення $P_i + 1$ із $N_i + 1 = Nk(P_i + 1)$.

При виконанні цієї атаки криптоаналітик має доступ не тільки до шифротексту, але і до відкритого тексту. Завдання криптоаналітика зводиться до знаходження ключа шифрування, використаного для наявних пар текстів, або побудови алгоритму, що дозволяє розшифровувати будь-які повідомлення, зашифровані на цьому ключі. Відкриті тексти, необхідні для даної атаки, можуть бути отримані з різних джерел. Наприклад, якщо відомо, що передається зашифрований файл з певним ім'ям, то з розширення часто можна зробити припущення про вміст певних фрагментів файлу, наприклад заголовка. Дана атака сильніша, ніж атака на основі тільки шифротекста.

Атака з можливістю вибору відкритого тексту. Ця атака передбачає наявність у Єви шифрованих $(N_1, N_2, ..., N_i)$ і відкритих текстів $(P_1, P_2, ..., P_i)$ декількох повідомлень, а також можливість підібрати ВТ для шифрування. Це надає більше можливостей, ніж розкриття на основі ВТ, оскільки Єва здійснює вибір блоків ВТ, що підлягають шифруванню і це може дати більше інформації про k. Таким чином, Єва отримує ключ чи АШ, що дозволяє розкрити нові повідомлення, зашифровані тим же ключем, тобто, маючи, P_1, $N_1 = Ek(P_1)$, P_2, $N_2 = Ek(P_2), \ldots, P_i$, $N_i = Ek(P_i)$

та можливість вибрати ($P_1, P_2, ..., P_i$), Єва визначає k або алгоритм знаходження $P_i + 1$ із $N_i + 1 = Ek(P_i + 1)$.

В цьому випадку у розпорядженні криптоаналітика є деяке число шифротекстів і відповідних їм відкритих текстів. Але, крім того, криптоаналітик має можливість вибрати кілька довільних відкритих текстів і отримати відповідні їм шифротексти. Завдання криптоаналітика точно таке ж, що і при атаці з відомим відкритим текстом: визначити використаний ключ шифрування або знайти інший спосіб розшифровувати повідомлення, зашифровані на тому ж ключі. Атака на основі **вибору відкритого тексту** дає можливість вибирати блоки відкритого тексту, що може, в свою чергу, дати додаткову інформацію про ключ шифрування.

Атака з адаптивним вибором відкритого тексту (*adaptive-chosen-plaintext* attack). Це особливий варіант атаки з вибором відкритого тексту. Криптоаналітик може не тільки вибирати відкритий текст, який потім шифрується, але і змінювати свій вибір залежно від результатів попереднього шифрування. Атака передбачає можливість Єви вибирати відкритий текст ($P_1, P_2, ..., P_i$), що підлягає шифруванню, а також уточнювати наступний вибір на базі раніше отриманих результатів шифрування. При розкритті з використанням підібраного ВТ Єва бере для шифрування лише один великий блок ВТ, а при адаптивному вибирається менший блок, і потім наступний, використовуючи результати першого вибору і т.д.

При криптоаналізі з простим вибором відкритого тексту криптоаналітик може вибирати кілька великих блоків відкритого тексту для їх шифрування, а при криптоаналізі з адаптивним вибором відкритого тексту має можливість вибрати більш менший пробний блок відкритого тексту, потім наступний блок в залежності від результатів першого вибору і т. д. Ця атака дає криптоаналітику більше можливостей, ніж попередні типи атак.

Атака з адаптивним вибором шифротексту (*adaptive-chosen-ciphertext*). Криптоаналітик може провести атаку цього типу по сценарію, в якому у нього є вільне використання частини розшифровки обладнання, але він не в змозі отримати ключ розшифровки з нього.

Атака методом повного перебору всіх можливих ключів. Атака передбачає використання Євою відомого ШТ і реалізується шляхом тотального перебору усіх можливих ключів з одночасною перевіркою змістовності отриманого ВТ. Для реалізації такої атаки Єві необхідно застосувати надпотужні обчислювальні ресурси (зважаючи на довжину ключів у сучасних стійких АШ), через це іноді така атака носить назву *силової* (*лобової*) *атаки* (*brute forceattack*). Останнім часом, зважаючи на стрімкий розвиток обчислювальних мереж, ефективність використання даного типу атак значно зросла, тобто Єва може об'єднати свої зусилля з іншими зловмисниками шляхом розпаралелювання певних операцій.

Ця атака передбачає використання аналітиком відомого шифротекста і здійснюється за допомогою повного перебору всіх можливих ключів з перевіркою, чи є осмисленим отриманий відкритий текст. Такий підхід вимагає залучення граничних обчислювальних ресурсів і називається силовою атакою.

Атака на основі апаратних помилок. Реалізується шляхом очікування або цілеспрямованої генерації Євою апаратних помилок в регістрах даних пристрою шифрування (системи, модуля). Завдяки такій атаці, Єва може з певною ймовірністю отримати фрагмент ключа шифрування, а з використанням додаткового програмного забезпечення розмір цього фрагменту може бути суттєво збільшений. Іноді даний тип атак називають *атаками аналізу збоїв*.

Цей вид атак пов'язаний з очікуванням або з цілеспрямованою генерацією апаратних помилок пристроїв шифрування. У зв'язку з масовим поширенням і використанням інтелектуальних електронних карток розгляд даного типу атак отримав важливе практичне значення. Випадок очікування помилок відрізняється від випадку генерації помилок тим, що мимовільні помилки трапляються вкрай рідко, тому найбільш небезпечними є напади шляхом умисного "струшування" пристрою шифрування. Безліч помилок апаратури в процесі шифрування можна розділити на два основних типи: помилки в області даних і помилки в області команд. В принципі помилки другого типу можуть привести до формування на виході шифратора ділянок ключа шифрування, однак ймовірність події, після випадкового модифікування буде відповідати деякій корисній для атакуючого програмі. Більш реальною є можливість цілеспрямованої генерації випадкових апаратних помилок в регістрах даних. Поширені в даний час шифри (DES, ГОСТ, RC5 тощо) не є стійкими до цього методу атак, тому що, мабуть, в той час, коли вони розроблялися, можливість навмисного введення випадкових апаратних помилок не приймалася до уваги.

Атака на основі відомого ключа шифрування. Реалізується атака таким чином: Єва має деяку інформацію про зв'язок між різними ключами. Даний тип криптоаналітичних атак часто буває дуже практичним і відрізняється від всіх раніше розглянутих. Єва вибирає зв'язок між парою

невідомих ключів, за допомогою яких зашифровані дані. У варіанті з відомим ВТ є відкритий і шифрований двома ключами текст, а у варіанті з підібраним – Єва вибирає ВТ для шифрування двома ключами.

При цьому передбачається, що криптоаналітику відома деяка частка ключа шифрування. Чим ближче до 100% значення відомої частки ключа, при якій шифр виявляється стійким, тим менше побоювань він буде викликати в реальних умовах застосування, коли ключ атакуючому невідомий.

“Бандитська” криптоаналітична атака полягає у тому, що Єва погрожує та шантажує Алісу й Боба поки не отримає ключ шифрування. У цій атаці, криптоаналітик використовує, так званий, «людський фактор», тобто намагання за допомогою шантажу, підкупу, тортур чи інших способів отримати інформацію про систему шифрування або навіть сам ключ шифрування. Наприклад, дача хабара є одним з різновидів бандитського криптоаналізу.

Досить вагомим і поширеним явищем є використання Євою хабарництва – **атака з "купленим ключем"** (*key purchase attack*). Варто також відзначити, що коли реалізуються атаки, які використовують "людський чинник", то виявляються безсилими і найстійкіші криптографічні шифри, і навіть системи захисту інформації з безумовною стійкістю.

Висновки

Враховуючи все вищесказане, можна зробити висновок, що якість та правильне використання криптографічного алгоритму шифрування даних є дуже важливим чинником, який обов’язково потрібно враховувати при побудові надійної криптосистеми, в тому числі стійкого генератора псевдовипадкових чисел.

На сьогоднішній день, одну з найбільших загроз безпеці інформації становлять криптоаналітичні атаки.

Криптоаналітичні атаки можна класифікувати на основі різних принципів та підходів.

Запропонована в даній роботі класифікація криптоаналітичних атак, дозволяє чітко визначити напрямки подальших досліджень щодо розробки та реалізації ефективних і надійних алгоритмів шифрування, а також генераторів псевдовипадкових чисел.

У статті показано, що різні види криптоаналітичних атак, мають різну складність для реалізації криптоаналітику, а отже потребують різної тривалості часу, обчислювальних та інших можливостей.

Список літератури

1. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайдер – М.: Изд-во «Вильямс», 2005. – 432 с.

2. Криптоаналитические атаки. [Електронний ресурс]– Режим доступу до журналу.: http://chhm.net/index.php?articles=165

3. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во «DIRECTLINE», 2009. — 714 с.

4. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. Oorschot, S. Vanstone // CRC Press, 1996. [Електронний ресурс]– Режим доступу до ресурсу.: http://www.cacr.math.uwaterloo.ca

5. Беляев Д.А. Криптоаналитические атаки / Д.А. Беляев, Ю.В. Гольчевский // Инфомационная безопасность, криптографія. [Електронний ресурс]– Режим доступу до журналу.: http://bda-expert.com/2010/05/kriptoanaliticheskie -ataki

Рецензент: д-р техн. наук, проф. В.В. Хома,
Національний університет «Львівська політехніка», Львів

Автор[1]: ***МАНДРОНА Марія Миколаївна***
Національний університет «Львівська політехніка», Львів, аспірант; Львівський державний університет безпеки життєдіяльності, Львів, викладач.
Моб. тел..– 098-40-15-126, дом. тел. – 223-22-35, E-mail – mandrona27@gmail.com

Автор[2]: ***ГАРАСИМЧУК Олег Ігорович***
Національний університет «Львівська політехніка», Львів, кандидат технічних наук, доцент, доцент кафедри захисту інформації.
Моб. тел..– 067-94-612-12, E-mail – garasymchuk@ukr.net

УДК 621.391+681.3.06
Мандрона М.М., Гарасимчук О.І. **Класифікація криптоаналітичних атак** // Системи обробки інформації. – 2005. – Вип. 00 (00). – С. 00 – 00. – Рос.
У даній роботі проводиться аналіз найбільш поширених криптоаналітичних атак та показано способи їх реалізації. Розроблено класифікацію криптоаналітичних атак на основі принципу їх здійснення. Показано, що кожна з атак, має різну складність для криптоаналітика і потребує різної тривалості часу, обчислювальних та інших можливостей.
Іл. 3. Бібліогр. 5 назв.

Мандрона М.М., Гарасимчук О.І. **Классификация криптоаналитических атак** // Системы обработки информации. – 2005. – Вып. 00 (00). – С. 00 – 00. – Рус.
В данной работе проводится анализ наиболее распространенных криптоаналитических атак и показаны способы их реализации. Разработана классификация криптоаналитических атак на основе принципа их осуществления. Показано, что каждая из атак, имеет разную сложность для криптоаналитика и требует разной продолжительности времени, вычислительных и других возможностей.

Mandrona M.M.. Garasymchuk O.I. **Classification of cryptanalytic attacks //** Sistemi obrobki informacii. – 2005. – Issue 00 (00). – P. 00 – 00. – Rus.
This paper analyzes the most common cryptanalytic attacks and shows how to implement them. The classification of cryptanalytic attacks on the basis of their implementation there is made in this paper. It is shown that each attack has a different difficulty to the cryptanalyst and require varying lengths of time, computational and more.