УДК 003.26:004.056.55

С.О. Гнатюк, асистент, Ю.Є. Хохлачова, асистент
(Національний авіаційний університет, Україна)

КРИТЕРІЇ ОЦІНКИ СТІЙКОСТІ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У даній роботі наведено базові критерії оцінки стійкості криптографічних систем захисту інформації з точки зору обчислювальних та інших можливостей атакуючої сторони. Розглядаються основні варіанти вирішення актуальної задачі розподілу ключів, також аналізуються основні відомі криптоаналітичні атаки з метою формулювання практичних рекомендацій щодо підвищення рівня криптографічної стійкості.

Питання оцінки стійкості криптографічних систем захисту інформації (СЗІ) є досить актуальним у наш час, коли існує багато криптоалгоритмів [1, 2] і постає задача їх вибору для побудови ефективних СЗІ і підвищення загального рівня конфіденційності. Таким чином, **метою** роботи є якісний аналіз критеріїв стійкості криптографічних СЗІ та інших актуальних проблем сучасної криптографії.

Доказ існування *абсолютно* стійких алгоритмів шифрування (АШ) був виконаний Клодом Шеноном та опублікований в праці [2]. Там же визначені вимоги до систем такого роду: ключ генерується для кожного повідомлення (кожен ключ використовується один раз); ключ статистично надійний (тобто ймовірності появи кожного з можливих символів рівні, а символи в ключовій послідовності незалежні та випадкові); довжина ключа дорівнює або більша за довжину повідомлення; вихідний (відкритий) текст (ВТ) володіє деякою надмірністю (є критерієм оцінки правильності розшифрування). Стійкість цих СЗІ не залежить від того, якими обчислювальними можливостями володіє атакуюча сторона (криптоаналітик, Єва). Практичне застосування СЗІ, що задовольняють вимогам абсолютної стійкості, обмежено міркуваннями вартості і зручності користування. Деякими аналітиками стверджується, що шифр Вернама є одночасно абсолютно криптографічно стійким і, до того ж, єдиним шифром, який задовольняє цій умові.

В основному застосовуються *практично* стійкі або *обчислювально* стійкі СЗІ. Стійкість цих систем залежить від того, якими обчислювальними можливостями володіє Єва. Практична стійкість таких систем базується на теорії складності і оцінюється виключно на якийсь певний момент часу і послідовно з двох позицій: обчислювальна складність повного перебору [1]; відомі на даний момент уразливості та їх вплив на обчислювальну складність. У кожному конкретному випадку можуть також існувати додаткові *критерії оцінки стійкості*. Базовими завданнями сьогоднішнього дня, які вирішуються криптопротоколами в мережах передачі даних, є аутентифікація, ідентифікація та ключовий обмін (розподіл ключів шифрування).

Існує також цілий ряд криптопротоколів, призначених для вирішення специфічних завдань. Слід мати на увазі, що один і той же криптопротокол може застосовуватися у різних областях. Наприклад, криптопротокол Kerberos [1] в ході своєї роботи дозволяє провести аутентифікацію користувачів і здійснити ключовий обмін між учасниками. Як приклад можна навести досить простий криптопротокол ключового обміну. Його учасники, Аліса та Боб, хочуть виробити загальний секретний ключ для симетричного АШ, використовуючи відкриті канали передачі даних. Для цього вони використовують наступну послідовність дій: 1) Боб вибирає схему асиметричного шифрування, створює пару ключів для даної схеми – відкритий і секретний; 2) Боб посилає свій відкритий ключ Алісі; 3) Аліса створює секретний ключ для симетричного АШ; зашифровує його на відкритому ключі Боба і відсилає йому отриманий результат; 4) Боб, отримавши зашифрований секретний ключ від Аліси, розшифровує його своїм секретним ключем для асиметричного АШ. Тепер Аліса та Боб, використовуючи симетричний АШ, можуть обмінюватися зашифрованою інформацією у відкритих каналах

зв'язку. Зазначений протокол не є безпечним, але вдало відображає саму ідею побудови подібних СЗІ.

Що стосується *розподілу ключів шифрування* між законними користувачами в умовах суворої секретності, то це є однією з найважливіших проблем сучасної криптографії, яка може бути вирішена за допомогою [3]:

- класичної криптографічної схеми з теоретико-інформаційної стійкістю (для її реалізації необхідний канал з перешкодами; ефективність схеми вкрай низька – 1-5%);
- класичної криптографічної схеми з відкритим ключем (схема Діфі-Хелмана [1], схема цифрового конверту; має обчислювальну стійкість);
- класичної симетричної криптографічної схеми з обчислювальною стійкістю (потребує наявності у абонентів попередньо встановленого ключа, тобто може розглядатися тільки як схема для збільшення довжини ключа, а не для його розподілення);
- квантового розподілу ключів (забезпечує теоретико-інформаційну стійкість, але потребує наявності у абонентів попередньо встановленого ключа для аутентифікації класичного каналу, тобто теж може розглядатися як схема для збільшення довжини ключа);
- методу довірених кур'єрів (висока вартість, велика залежність від людського чинника).

Управління ключами складається з наступних процедур: ініціалізація ключової структури для користувачів в домені; створення, розподіл і інсталяція ключового матеріалу; контроль над використанням ключового матеріалу; оновлення, відновлення та знищення ключового матеріалу; зберігання ключового матеріалу.

Основною метою управління ключами є підтримка ключових взаємин і ключового матеріалу таким чином, щоб не сталося: компрометації таємних ключів; компрометації системи аутентифікації секретної ключової інформації або відкритих ключів; неавторизованого використання секретних або відкритих ключів (наприклад, необхідно забезпечувати неможливість використання ключів, термін дії яких закінчився).

Для кожного відкритого повідомлення існує апріорна ймовірність вибору, оскільки механізм вибору відкритих повідомлень можна представити як деякий ймовірнісний процес. Аналогічно, вибір кожного ключа також має апріорну ймовірність. Супротивник, який перехоплює зашифровані повідомлення, може обчислити апостеріорні ймовірності як появи відкритого повідомлення, так і ймовірність появи ключа. Набір апостеріорних ймовірностей являє собою систему відомостей, що належать супротивнику, про ключі, які використовуються та відкриті повідомлення, які передаються. Причому, перед початком перехоплення зашифрованих повідомлень супротивник має у своєму розпорядженні деякий набір апріорних ймовірностей про відкриті повідомлення і ключі. З практичної точки зору це означає, що супротивник обізнаний про систему засекреченого зв'язку, що використовується.

Припустимо, що супротивнику відомі всі криптографічні перетворення, що використовуються в системі засекреченого зв'язку, а також ключовий простір, причому, як було сказано вище, секретність системи залежить від вибору конкретного ключа. У результаті перехоплення деякого обсягу зашифрованих повідомлень та обчислення апостеріорних ймовірностей супротивник зрозуміє, що їм буде відповідати єдине рішення про використання ключа або передачу відкритого повідомлення (точка єдності прийняття рішення), яке задовольняє даним ймовірностям. Зрозуміло, що подібний висновок цілком може привести до розкриття системи супротивником. Під *розкриттям системи засекреченого зв'язку або АШ* ми розуміємо одну з наступних операцій, що планує супротивник і які направлені на досягнення цієї мети: *повне розкриття* – супротивник знаходить шляхом обчислень секретний ключ системи; *знаходження еквівалентного алгоритму* – супротивник знаходить алгоритм, функціонально еквівалентний АШ, не маючи при цьому уяви про секретний ключ, що використовується; *знаходження відкритого повідомлення* – супротивник знаходить відкрите повідомлення, яке відповідає одному з перехоплених зашифрованих; *часткове розкриття* – супротивник отримує часткову інформацію про ключ, що використовується, або про відкрите повідомлення.

Розглянемо найпоширеніші на сьогоднішній день *причини здійснення успішних атак* на АШ: 1) наявність статистичної структури історично сформованих мов. Тобто, існують певні символи або комбінації символів, що найбільш часто зустрічаються в природній мові. Таким чином, при перехопленні зашифрованого повідомлення для деяких типів АШ можливо підрахувати частоту появи певних символів та зіставити їх з ймовірностями появи певних символів або їх комбінацій (біграми, триграми і т.д.), що в деяких випадках може привести до однозначного дешифрування окремих ділянок зашифрованого повідомлення; 2) наявність ймовірних слів. Мова йде про слова або вирази, появу яких можливо очікувати в перехопленому повідомленні. Таким чином, у діловому листуванні присутні шаблонні слова; в англійській мові, наприклад, найчастіше зустрічаються "and", "the", "are" і т.д.

Існує достатньо розповсюджений підхід до формальної оцінки цього поняття. Стійкість криптографічного алгоритму необхідно розглядати відносно пари "атака-мета", де під метою супротивника розуміють заплановану загрозу.

У роботах [4, 5] запропонована наступна узагальнена класифікація атак на криптографічні СЗІ, де кожна атака представлена математичною моделлю, що значно спрощує сприйняття та розуміння.

Атака на основі тільки шифротексту (ШТ) (*cipher text attack*) полягає у тому, що Єва володіє ШТ ($N_1, N_2,\ldots, N_i$) декількох ВТ ($P_1, P_2,\ldots, P_i$), зашифрованих одним АШ. Єва розкриває якомога більшу кількість ШТ або ключів шифрування з метою розкриття інших ШТ, зашифрованих тим самим ключем (k). Тобто, маючи $N_1=E_k(P_1)$, $N_2=E_k(P_2),\ldots, N_i=E_k(P_i)$ можна визначити ($P_1, P_2,\ldots, P_i$) та k або алгоритм відновлення P_{i+1} із $N_{i+1}=E_k(P_{i+1})$.

Атака на основі ВТ (*plaintext attack*) реалізується таким чином, що Єва, володіючи ШТ ($N_1, N_2,\ldots, N_i$) і їх ВТ ($P_1, P_2,\ldots, P_i$), розкриває k з метою подальшого розшифрування інших ШТ, зашифрованих тим же ключем (ключами). Іншими словами, маючи $P_1, N_1=E_k(P_1), P_2, N_2=E_k(P_2),\ldots, P_i, N_i=E_k(P_i)$, можна визначити k або алгоритм відновлення P_{i+1} із $N_{i+1}=N_k(P_{i+1})$.

Атака на основі підібраного ВТ передбачає наявність у Єви шифрованих ($N_1, N_2,\ldots, N_i$) і ВТ ($P_1, P_2,\ldots, P_i$) 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, $P_1, N_1=E_k(P_1), P_2, N_2=E_k(P_2),\ldots, P_i, N_i=E_k(P_i)$ та можливість вибрати ($P_1, P_2,..., P_i$), Єва визначає k або алгоритм знаходження P_{i+1} із $N_{i+1}=E_k(P_{i+1})$.

Атака на основі адаптивно підібраного ВТ передбачає можливість Єви вибирати ВТ ($P_1, P_2,\ldots, P_i$), 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.

Атака з використанням підібраного ШТ полягає у тому, що Єва для розкриття може вибирати різні ШТ ($N_1, N_2,\ldots, N_i$) і має доступ до розшифрованих ВТ. Наприклад, маючи "чорний ящик", що реалізує автоматичне розшифрування, необхідно одержати ключ. Іншими словами, маючи $N_1P_1=D_k(N_1), N_2P_2=D_k(N_2),\ldots, N_iP_i=D_k(N_i)$, Єва визначає k. Така атака зазвичай застосовується до систем з відкритим ключем, але іноді буває ефективною і для симетричних АШ. Часто в літературі атаку на основі підібраного ВТ і атаку з використанням підібраного ШТ разом називають *атакою на основі підібраного тексту*.

Атака на основі підібраного ключа реалізується таким чином, що 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.

Атака методом повного перебору всіх можливих ключів 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 force attack*). 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.

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*.

Крім того, виділяють цілий клас *атак за допомогою побічних каналів* (*side-channel analysis attack*), тобто таких атак, за допомогою яких, на відміну від розглянутих вище, Єва намагається отримати інформацію про ключ чи ВТ не на основі теоретичного опису криптографічного АШ, а на основі даних, отриманих в результаті спостереження за фізичним процесом роботи пристрою шифрування. До даного класу атак відносять атаки *по часу, по енергоспоживанню, по електромагнітному випромінюванню, по світловому випромінюванню, акустичні атаки. Кореляційна атака (correlation attack)* основана на виявленні Євою статистичної залежності між елементами вхідної (P_1, P_2,…, P_i) і вихідної (N_1, N_2,…, N_i) послідовностей шифратора.

Бандитська криптоаналітична атака полягає у тому, що Єва загрожує, використовує тортури чи шантажує Алісу й Боба поки не отримає ключ шифрування. Досить вагомим і поширеним явищем є використання Євою хабарництва – *атака з "купленим ключем"* (*key purchase attack*). Варто також відмітити, що коли реалізуються атаки, які використовують "людський чинник", то виявляються безсилими і найстійкіші криптографічні шифри, і навіть СЗІ з безумовною стійкістю.

Висновки

Аналізуючи атаки та їх цілі, можна прийти до висновку, що найбільшу стійкість криптографічна СЗІ має в тому випадку, коли вона здатна протистояти найсильнішій атаці, яку проводить супротивник, за умови, що він переслідує найслабшу (найуразливішу) з можливих цілей атаки (загрози). Таким чином, у даній роботі наведено критерії оцінки стійкості криптографічних СЗІ, проаналізовано шляхи вирішення проблеми розподілу ключів шифрування та найпоширеніші криптоаналітичні атаки. У подальшому, на базі даного дослідження, планується формулювання практичних рекомендацій щодо підвищення криптостійкості СЗІ.

Список літератури

1. Мао В. Современная криптография : Теория и практика / Венбо Мао. — М. : Издательский дом «Вильямс», 2005. — 768 с.

2. Shannon C. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, 1949. — Vol. 28. — P. 656–715.

3. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.

4. Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.

5. Атаки в квантових системах захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. — 2010. — № 2. — С. 109–115.