*Дайте визначення та оцінку атак груба сила, при яких вхідних даних вони можуть здійснюватись?*

Силові методи також називають атаками «груба сила». До них необхідно віднести:

1) атаку з повним перебиранням ключів;
2) табличну атаку;
3) атаку зі словником.

Силові методи криптоаналізу (атаки) можуть бути застосованими до всіх детермінованих БСШ, незалежно від їх структури. При наявності у криптоаналітика необхідної початкової інформації про довжини блоків і ключа застосування силового методу практично гарантує знаходження таємного ключа або розкриття семантичного змісту. На цей час відносно перспективних БСШ не існує ефективних аналітичних атак. Це робить силові атаки єдино можливим шляхом здійснення НСД до зашифрованої інформації.

Основними факторами, що впливають на складність силових атак, є довжина ключа шифрування, розмір блоку, що шифрується, обчислювальна складність прямих і зворотних криптоперетворень. За деяких умов має значення надмірність інформації, що захищається. Розмір ключа вважається найбільш важливим із перерахованих факторів, який експоненційно впливає на складність атаки. Тому при досить великих довжинах ключа (вважається 128 і більше бітів) для проведення силових атак потрібні значні обчислювальні ресурси та часові витрати, які не можуть бути реалізовані наявними нині ресурсами. Розмір блоку шифру і складність прямих і зворотних криптоперетворень також значною мірою впливають на можливості здійснення криптоаналізу. Після довжини ключа вони також визначають складність, ресурсомісткість і необхідну продуктивність системи криптоаналізу.

Надмірність оброблюваної інформації має вплив на складність криптоаналізу в тому випадку, якщо ентропія джерела ключів перевищує ентропію джерела повідомлень. За цієї умови одній парі відкритого й зашифрованого блоків буде відповідати деяка безліч еквівалентних ключів, при використанні яких наявний відкритий блок перетворюється на заданий зашифрований. Тому отриманої інформації буде недостатньо для однозначного визначення дійсного ключа шифрування. Для успішного проведення силової атаки в цьому випадку необхідно аналізувати більше ніж один зашифрований блок. Надалі будемо розглядати три типи силових атак: повне перебирання ключів, табличну атаку та і атаку зі словником.

1) Перебірання ключів:

Основним показником ефективності методу «груба сила» є число варіантів перебирання $N_в$ і безпечний час (час перебирання) $t_б$. Безпечний час $t_б$ можна обчислити використовуючи формулу:

$$t_б = \frac{N_в}{\gamma K} P_p , \qquad (8.6)$$

де:

$N_в$ – кількість варіантів (групових операцій);

$\gamma$ – потужність криптоаналітичної системи;

$P_p$ – ймовірність успішного криптоаналізу;

$K$ – кількість секунд у році ($3{,}15\times10^7$ сек / рік).

У разі коли перебираються ключі, тобто маємо $N_к$ варіантів, безпечний час обчислюється як

$$t_б = \frac{N_к}{\gamma K} P_p , \qquad (8.7)$$

де $N_к$ – число ключів, що можуть використовуватись у криптосистемі.

2) Попередньо обчисленні дані:

Імовірність $p_s$ знайти вірний ключ залежить від кількості врахованих на етапі передобчислювання ключів $l$ та отриманих шифртекстів $n$ і для шифрів з довжиною блоку, що перевищує довжину ключа, може бути обчислена з використанням такої формули:

$$p_s = 1-\left(1-l\cdot 2^{-k}\right)^n \geq 1-e^{-l\cdot n/2^k}$$

Залежність кількості шифртекстів від обсягу передобчислювання для виконання успішної атаки алгоритму шифрування DES наведена в табл. 8.2.

*Таблиця* 8.2

Залежність кількості шифртекстів від обсягу попередніх обчислень

| Количество шифртекстов | 1 | $2^8$ | $2^{16}$ | $2^{24}$ | $2^{28}$ | $2^{32}$ | $2^{40}$ | $2^{48}$ | $2^{56}$ |
|---|---|---|---|---|---|---|---|---|---|
| Сложность предвычислений | $2^{56}$ | $2^{48}$ | $2^{40}$ | $2^{32}$ | $2^{28}$ | $2^{24}$ | $2^{16}$ | $2^8$ | 1 |

Складність табличної атаки на деякі широко поширені симетричні алгоритми наведена в табл. 8.3.

*Таблиця 8.3*

Складність табличної атаки на деякі широко поширені симетричні шифри

| Назва алгоритму | DES | TDES | Skipjack | IDEA | AES | ГОСТ 28147-89 |
|---|---|---|---|---|---|---|
| Складність атаки | $2^{28}$ | $2^{84}$ | $2^{40}$ | $2^{64}$ | $2^{64}$-$2^{128}$ | $2^{128}$ |

**Атака зі словником**

У деяких випадках, описаних вище, можливе отримання пари «відкритий блок – зашифрований блок» без знання таємного ключа шифрування. У такому разі криптоаналітик збирає ці пари у спеціальному «словнику». У простих варіантах атаки передбачається, що алгоритм шифрування використовується в режимі простої заміни, а довжина ключа менше або дорівнює довжині блоку. В такому випадку для всіх повідомлень, що зашифровані на одному ключі, складається словник. Після перехоплення шифрблоку проводиться його пошук у словнику і відразу знаходиться відповідний йому відкритий блок.

У разі якщо розмір ключа перевершує розмір блоку, ймовірність того, що різним відкритим текстум відповідає один і той же зашифрований текст, є малоймовірною подією.

## Атака методом створення колізій

Сутність атаки міститься у спробі формувати 2 криптограми та реалізувати атаку з вибором повідомлень або з вибором криптограм, для яких використаний один і той же ключ.

У такій постановці вже були розглянуті задачі криптоаналізу типу «повне розкриття» для еліптичних кривих (розділ 3 цієї монографії) та оцінки колізій геш-значень (розділ 4 цієї монографії). Тут ми розглянемо у скороченому вигляді застосування методу колізій для здійснення атаки на БСШ. Відмітимо універсальність атаки та можливість її застосування практично до будь-якого симетричного шифру.

У нашому випадку є цілочисленна випадкова величина з рівноймовірним розподілом значень від 1 до $n$, та є вибірка із $k$ значень випадкової величини ($k \le n$). Знайдемо ймовірність $P(n, k)$ того, що серед значень $F(M)$ у виборці принаймні дві співпадають:

$$F(M_i) = F(M_j). \qquad (8.8)$$

Використовуючи підхід, що базується на узагальненому «парадоксі про день народження», отримаємо:

$$P(n,k) = 1 - \frac{n!}{(n-k)!n^k}. \qquad (8.9)$$

Для спрощення розрахунків вираз (8.9) можна спростити. Для цього справедливим є вираз

$(1-x) \le e^{-x}$ для всіх $x \ge 0$. (8.10)

Крім того, при малих значеннях *x* (наприклад, $x \le 0{,}1$) можна вважати, що

$$(1-x) \approx e^{-x}. \quad (8.11)$$

Далі запишемо (8.9) у вигляді:

$$P(n,k) = 1 - \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{n^k} =$$
$$= 1 - \left[\frac{n-1}{n}\cdot\frac{n-2}{n}\cdot\ldots\cdot\frac{n-k+1}{n}\right] = \quad (8.12)$$
$$= 1 - \left[\left(1-\frac{1}{n}\right)\cdot\left(1-\frac{2}{n}\right)\cdot\ldots\cdot\left(1-\frac{k-1}{n}\right)\right].$$

Оскільки в нашому випадку $\frac{1}{n},..\frac{k-1}{n} \le 0{,}1$, то зробимо у (8.12) заміну, використовуючи (8.10). У результаті маємо:

$$P(n,k) = 1 - \left[\left(e^{-1/n}\right)\cdot\left(e^{-2/n}\right)\cdot\ldots\cdot\left(e^{-k-1/n}\right)\right] =$$
$$= 1 - e^{-\left[(1/n)+(2/n)+\ldots+((k-1)/n)\right]} = \quad (8.13)$$
$$= 1 - e^{-(k(k-1))/2n}.$$

Результат можна отримати, розв'язавши (8.13)

$1 - e^{-(k(k-1))/2n} = P_з$, оскільки $P_з$ відомо і реально $P_з \le 1$,

то

$$1 - P_з = e^{-(k(k-1))/2n}$$

або

$$\ln(1-P_з) = -k(k-1)/2n,$$

і далі

$$\frac{k(k-1)}{2n} = -\ln(1-P_з);$$
$$k(k-1) = -2n\ln(1-P_з).$$

У кінцевому вигляді маємо рівняння:

$$k^2 - k + 2n\ln(1-P_з) = 0. \quad (8.14)$$

Нехай $P_з$=0, 5, тоді маємо

$$k^2 - k + 2n\ln 0{,}5 = k^2 - k - 2n\ln 2 = 0.$$

При $n=2^m$ рівняння набуває вигляду:

$$k^2 - k - 2^{m+1}\ln 2 = 0. \qquad (8.15)$$

Дамо оцінку значення $k$, враховуючи що $k$ достатньо велике і $k^2 >> k$.

Тоді із (8.14) маємо

$$k^2 = -2n\ln(1 - P_з).$$

При $P_з$ =0,5 отримуємо

$$k^2 = -2n\ln\left(1 - 1/2\right) = 2n\ln 2$$

і

$$k = \sqrt{2(\ln 2)\cdot n} = 1{,}18\sqrt{n}. \qquad (8.16)$$

При $n=2^{160}$ маємо $k=\sqrt{2^{160}}=2^{80}$. При $n=2^{256}$ маємо $k=2^{128}$.

При довільному значенні $P_з$

$$k = \sqrt{2\ln\left(\frac{1}{1-P_з}\right)\cdot n} = 1{,}41\sqrt{\ln\left(\frac{1}{1-P_з}\right)\cdot n}. \qquad (8.17)$$

Співвідношення (8.17) дозволяє оцінити число експериментів, які необхідно виконати для здійснення