УДК 681.3.06

МЕТОД ОЦІНЮВАННЯ СТІЙКОСТІ ПРАКТИЧНИХ РЕАЛІЗАЦІЙ ШИФРУ ОДНОРАЗОВОГО БЛОКНОТУ

Володимир Андреєв, Сергій Мельник
Національна академія Служби безпеки України

Анотація: **Запропоновано метод оцінювання складності направленого перебору ключів одноразових блокнотів та достовірності отриманого результату.**
Summary: **The method is proposed for the estimation of complexity of directed search method for finding keys of one-time-pad and estimation of the reliability of the result.**
Ключові слова: **шифр одноразового блокноту, практична реалізація шифру одноразового блокноту або одноразовий блокнот; методи направленого перебору ключів, оцінка криптографічної стійкості.**

Вступ

Поняття теоретичної стійкості було введено Шенноном [1] і полягає у тому, що для будь-якого відкритого тексту $x \in X$ та шифртексту $y \in Y$ виконується умова

$$P(x/y)=P(x).$$

Це означає, що шифртекст не дає криптоаналітику ніякої інформації про відповідний відкритий текст. Шеннон також ввів критерій теоретичної стійкості шифрів (постулат): невизначеність секретного ключа $k \in K$ повинна бути не менша, ніж невизначеність відкритого тексту, тобто

$$H(K) \geq H(X). \qquad (1)$$

де $H(K) = -\sum_{k \in K} P(k) \log P(k)$, $H(X) = -\sum_{x \in X} P(x) \log P(x)$ – величини, що визначають кількість інформації про множину ключів і відкритих текстів відповідно.

Як наслідок, теоретично стійкі (або досконалі) шифри характеризуються тим, що сама задача дешифрування для них стає безглуздою. Це значить, що застосування довільного методу криптоаналізу, включаючи повний перебір ключів, не дозволить не тільки відновити ключ або відкритий текст, а навіть одержати будь-яку інформацію про них. Наприклад, при спробі перебрати Z^L можливих ключів теоретично стійкого шифру (при наявності криптограми довжини L над алфавітом потужності Z) криптоаналітик одержить разом із дійсним відкритим текстом і всі інші осмислені відкриті тексти тієї ж довжини. Вибрати ж з них дійсний відкритий текст на великій довжині L не уявляється можливим.

В практичних реалізаціях теоретично стійких шифрів умова (1) буде гарантовано виконуватись тоді, коли всі можливі ключі $k \in K$ є рівноімовірними і незалежними величинами та $|K| \geq |X|$. При цьому, в [2] доведено, що теоретично стійкі шифри можуть бути реалізовані лише з використанням фізичних генераторів випадкових чисел.

Найбільш поширеним у практичному застосуванні теоретично стійким шифром є шифр одноразового блокноту (one-time pad), або шифр Віженера, тобто лінійний шифр табличного гамування над деяким алфавітом потужності Z (для бінарного випадку даний шифр отримав назву шифру Вернама). У даному разі ключем криптографічного перетворення є безпосередньо шифргама (випадкова послідовність довжини L).

В статті розглядається випадок, що передбачає наявність деякого відхилення імовірнісного розподілу символів вихідної послідовності генератора ключів від рівноімовірного. Тобто, існує можливість побудови методу направленого перебору ключів [3], ефективність якого можна оцінити імовірністю успіху за N кроків перебору. Враховуючи на це, якщо можлива побудова критерію відкритого тексту, що використовує тематичні обмеження джерела зашифрованих повідомлень, то можливий і направлений перебір ключів шифру одноразового блокноту з імовірністю успіху

$$P = P_1 P_2, \qquad (2)$$

де P_1 – імовірність успіху методу направленого перебору ключа за N кроків; P_2 – імовірність того, що критерій відкритого тексту виявить відкритий текст джерела зашифрованих повідомлень.

Криптографічна стійкість *практичних реалізацій шифру одноразового блокноту* (або одноразового блокноту) визначається статистичними властивостями генератора ключових даних та порядком експлуатації засобів криптографічного захисту інформації. Рівень криптографічної стійкості оцінюється

зокрема складністю направленого перебору ключів та величиною *достовірності*1 результату перебору, якщо його отримано. Оцінка складності методу направленого перебору визначається математичним очікуванням кількості опробувань ключа до успіху. В свою чергу, достовірність результату направленого перебору ключів визначається величиною (2).

Слід зазначити, що запропонована також в [3] оцінка імовірності успіху методу направленого перебору ключів за N кроків передбачає наявність деякого відомого відхилення δ від рівноімовірного розподілу елементів вихідної послідовності фізичного генератора ключів G:

✓ $\{\xi_i\}_{i\geq 1}$ – бітова послідовність незалежних однаково розподілених випадкових величин з виходу генератора;

✓ $\forall\, i \geq 1 \;\; P(\xi_i = 1) = p = \frac{1}{2} + \delta\,,\;\; P(\xi_i = 0) = q = \frac{1}{2} - \delta\,,\;\; 0 \leq \delta < \frac{1}{2}.$

Однак, фізичні генератори бінарних послідовностей завжди мають відхилення δ, яке не є константою, а може бути оцінене лише за деякий час T їх роботи.

Постановка задачі – оцінити достовірність результату направленого перебору ключів генератора *G* за час його використання T (зашифровано s біт відкритого тексту) при наявності $k(k < s)$ відомих елементів чистої гами.

I Оцінка імовірності успіху методу направленого перебору ключів за *N* кроків

Нехай *N* – випадкова величина, що дорівнює кількості опробувань ключів одноразового блокноту (методом оптимального перебору) до успіху. Необхідно знайти функцію розподілу випадкової величини N залежно від значень δ та n (*n* – довжина ключа в бітах). В [3] доведено, що для бінарних послідовностей $\xi_1, \xi_2, ..., \xi_n$ виходу генератора *G* справедлива оцінка

$$\lim_{n\to\infty}\left(P\left(N \leq \sum_{i=0}^{h} C_n^i \right) - \left(\Phi\left(\frac{2h - n(1-2\delta)}{\sqrt{n(1-4\delta^2)}} \right) - \Phi\left(-\sqrt{\frac{n(1-2\delta)}{1+2\delta}} \right) \right) \right) = 0\,, \tag{3}$$

де $0 \leq h \leq n$, $\Phi(x)$ – функція нормального розподілу.

Зауваження.

1. Твердження (3) можна представити також і наступним чином

$P\left(N \leq \sum_{i=0}^{h} C_n^i \right) \approx \Phi\left(\frac{2h - n(1-2\delta)}{\sqrt{n(1-4\delta^2)}} \right) - \Phi\left(-\sqrt{\frac{n(1-2\delta)}{1+2\delta}} \right)$, при цьому модуль різниці лівої і правої частини не перевищує $\frac{p^2+q^2}{\sqrt{npq}} \leq \frac{0,5}{\sqrt{0,25n}} = \frac{1}{\sqrt{n}}$.

2. Якщо V∈N таке, що $\sum_{l=0}^{h} C_n^l \leq V \leq \sum_{l=0}^{h+1} C_n^l$ та $L = V - \sum_{l=0}^{h} C_n^l$, тоді

$$P_{1.1} = P(N \leq V) \approx \Phi\left(\frac{2h - n(1-2\delta)}{\sqrt{n(1-4\delta^2)}} \right) - \Phi\left(-\sqrt{\frac{n(1-2\delta)}{1+2\delta}} \right) + Lp^{h+1}q^{n-h-1}. \tag{4}$$

II Визначення статистичного відхилення послідовності генератора ключових даних при *k* опробуваннях його виходу

Нехай: $\xi_1, \xi_2, ..., \xi_S$ – бітова послідовність незалежних однаково розподілених випадкових величин з виходу генератора *G* (шифргама) за час його використання *T*; $\forall 1 \leq i \leq s \;\; P\{\xi_i = 1\} = p\,,\; P\{\xi_i = 0\} = q\,;$

1 Імовірність того, що отриманий результат направленого перебору ключів відповідає дійсному відкритому тексту, що був зашифрований шифром одноразового блокноту.

$\{a_j\}_{1\le j\le k}$ – реалізація послідовності $\xi_1, \xi_2, ..., \xi_S$.

Оцінимо по послідовності $\{a_j\}_{1\le j\le k}$ величини p та q, відповідно, δ.

Слід зазначити, що $\forall i$ математичне очікування $M(\xi_i) = p$, тому може бути використана нерівність Чебишева:

$$P\{|\xi_i - M(\xi_i)| > \delta\} \le \frac{D(\xi_i)}{\varepsilon^2} = \frac{\sigma^2}{\varepsilon^2}, \tag{5}$$

де $\left(0 < \varepsilon < \frac{1}{2}\right)$.

Математичне очікування $M\xi_i$ оцінимо частотою ν появи 1 в послідовності $\xi_1, \xi_2, ..., \xi_S$.

Оскільки $\nu = \frac{\sum_{i=1}^{k} \xi_i}{k}$, $M(\nu) = \frac{kM(\xi_i)}{k} = M(\xi_i) = p$, $D(\xi_i) = p(1-p) = \sigma^2 < \frac{1}{4}$ та $D(\nu) = \frac{1}{k^2} D(\sum_{i=1}^{k} \xi_i) = \frac{k\sigma^2}{k^2} = \frac{\sigma^2}{k} < \frac{1}{4k}$, то нерівність (5) буде мати вид:

$$P\{|\nu - p| > \varepsilon\} \le \frac{1}{4k\varepsilon^2}. \tag{6}$$

Звідси справедливе

Твердження 1. Для заданої кількості відомих елементів шифргами k, імовірність того, що параметр p ($p = \frac{1}{2} + \delta$) визначено з відхиленням не більшим за ε дорівнює

$$P_{1.2} > 1 - \frac{1}{4k\varepsilon^2}. \tag{7}$$

Наслідок. Якщо виконується умова (7), то з імовірністю $P_{1.2}$ виконуються нерівності:

$$|p - \nu| < \varepsilon, \tag{8}$$

$$\frac{\sum_{i=1}^{k} a_i}{k} - \varepsilon < p < \frac{\sum_{i=1}^{k} a_i}{k} + \varepsilon, \tag{9}$$

або

$$\frac{\sum_{i=1}^{k} a_i}{k} - \varepsilon - \frac{1}{2} < \delta < \frac{\sum_{i=1}^{k} a_i}{k} + \varepsilon - \frac{1}{2}. \tag{10}$$

Зрозуміло, що $P_1 = P_{1.1} P_{1.2}$ (див. (2)).

III Метод оцінювання криптографічної стійкості одноразового блокноту

Як уже зазначалося вище, рівень криптографічної стійкості одноразового блокноту до методів направленого перебору ключів визначається оцінкою складності перебору та оцінкою достовірності отриманого результату, якщо його отримано. При цьому, оцінювання першого параметру буде мати сенс лише тоді, коли оцінка другого параметру криптографічної стійкості є прийнятною величиною.

Так, згідно [3] математичне очікування кількості опробувань ключів одноразового блокноту до **успіху (оцінка складності) буде дорівнювати**

$$M(N) = p^n + \sum_{h=1}^{n} \frac{s_{h-1} + 1 + s_h}{2} \cdot C_n^h \cdot p^{n-h} \cdot q^h, \tag{11}$$

де s_{h-1}, s_h – обмеження на N таке, що $s_{h-1} < N \le s_h$, $s_h = \sum_{i=0}^{h} C_n^i$.

Враховуючи (2), (4), (7) та за умови, що $P_2 = 1$ (див. (2)) буде справедливе

Твердження 2. Достовірність результату направленого перебору ключів одноразового блокноту дорівнює

$$P \approx \Phi\left(\frac{2h - n(1-2\delta)}{\sqrt{n(1-4\delta^2)}}\right) - \Phi\left(-\sqrt{\frac{n(1-2\delta)}{1+2\delta}}\right) + Lp^{h+1}q^{n-h-1}\left(1 - \frac{1}{4k\varepsilon^2}\right), \qquad (12)$$

де: n – довжина ключа одноразового блокноту; $0 \le h \le n$; $L = V - \sum_{l=0}^{h} C_n^l$; $\sum_{l=0}^{h} C_n^l \le V \le \sum_{l=0}^{h+1} C_n^l$; V – кількість опробувань ключа; ε – задане відхилення для p; $k(k < s)$ – кількість відомих елементів чистої гами, що вибирається з *s* елементів шифртексту різних шифртелеграм.

Слід зазначити, що в результаті направленого перебору ключів у більшості випадків буде отримано декілька можливих відкритих текстів і всі вони матимуть достовірність *P*. Питання вибору критерію відкритого тексту з величиною $P_2 = 1$ є окремою науковою задачею.

Висновки

Підсумовуючи сказане, звернемо увагу на те, що класичний метод оцінки криптографічної стійкості практичних реалізацій шифру одноразового блокноту э процедурою статистичного тестування генератора ключових даних з метою перевірки виконання вимог критерія теоретичної стійкості (1).

Запропонований же в статті метод дозволяє оцінювати параметри стійкості одноразових блокнотів при відсутності фізичного доступу до генераторів ключів.

Література: ***1.*** *Шеннон К. Работы по теории информации и кибернетике/ Пер. с англ. Под ред. Н. А. Железнова. – М.: ИЛ, 1963. – 35 с.* ***2.*** *Зубов А. Ю. Совершенные шифры. М.: "Гелиос АРВ" 2003. - 54 с.* ***3.*** *Ковальчук Л. В., Мельник С. В., Бездетный В. Т. Вероятностные характеристики схем генерации ключей с неравновероятным распределением. "Радиотехника".Харьков: 2005, т. 140 - 23с.*

УДК 681.3

ЕКСПЕРТНА КІЛЬКІСНА ОЦІНКА АНТИВІРУСНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Вячеслав Шорошев
НДІ НАВС України

Анотація: **Надаються рекомендації щодо антивірусного захисту корпоративних комп'ютерних мереж Intranet, методів експертної кількісної оцінки антивірусної безпеки від потенційно загрозливих видів комп'ютерних вірусів та пропонується модель політики антивірусної безпеки комп'ютерних систем.**

Summary: **The recommendations concerning anti–virus protection of corporate computer networks Intranet are given, of methods of an expert quantitative estimation of anti–virus safety from potentially me nacing kinds of computer viruses and the model of politics of anti–virus safety of computer systems is offered.**

Ключові слова: **Антивірус, антивірусна безпека, політика антивірусної безпеки, ризик антивірусної безпеки.**

І Вступ

Проблема антивірусного захисту все більше стає не тільки актуальною, але й обов'язковою компонентою забезпечення безпеки комп'ютерних систем (КС).

З моменту появи першого комп'ютерного вірусу пройшло вже кілька десятків років, з тих пірважливість цієї проблеми не тільки не зменшилась, але навпаки, значно збільшилась. Комп'ютеризація призвела не тільки до інформатизації суспільства, але і до поширеності вірусної інфекції.

Хоча вірусні атаки в комп'ютерних системах будуть завжди, застосування деяких рекомендацій і