МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

Щербина Юрій Володимирович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук, доцент
Казакова Надія Феліксівна
Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук

ДОСЛІДЖЕННЯ ПОТОЧНОГО ШИФРУ, ПОБУДОВАНОГО НА ОСНОВІ XORSHIFT-ГЕНЕРАТОРА

Зростання рівню загроз в сучасних системах кіберзахисту вимагає пошуку нових ефективних швидкодіючих алгоритмів поточного шифрування, що забезпечують захист даних, які передаються в каналах зв'язку сучасних автоматизованих систем управління в реальному часі.

Потокові шифри (stream cipher) – це окремий клас симетричних криптографічних систем, в яких елементи відкритого тексту перетворюються в елементи шифртексту шляхом гамування без розділення на окремі блоки фіксованої довжини. Таке шифрування відбувається шляхом побітного складання вхідної послідовності з бінарними символами псевдовипадкової послідовності чисел (ПВЧ) і називається гамуванням [1]. Перевага надається поточним системам коли необхідно виконувати шифрування у швидкісному режимі в реальному часі. Зазвичай у якості джерела шифруючої гами використовується програмний генератор ПВЧ, побудований з використанням простих, з точки зору програмної реалізації, операцій, що не вимагають значних витрат обчислювальних ресурсів. Саме через це, вже багато десятиріч, актуальною проблемою є пошук ефективних генераторів такого типу [2].

Ціллю дослідження є обґрунтування стійкості поточного алгоритму шифрування, побудованого на основі запропонованого Джорджем Марсальєю алгоритму генерації псевдовипадкових чисел Xorshift, який використовує такі економічні операції, як складання "по модулю два" (xor) і "зсув" (shift) [3].

Оцінка стійкості Xorshift-генератора

Основним достоїнством Xorshift-генератора є його простота, яка забезпечується використанням операцій зсуву кодового слова "вліво" (<<) або "вправо" (>>). Фрагмент програми, що реалізує такий алгоритм, має наступний вигляд.

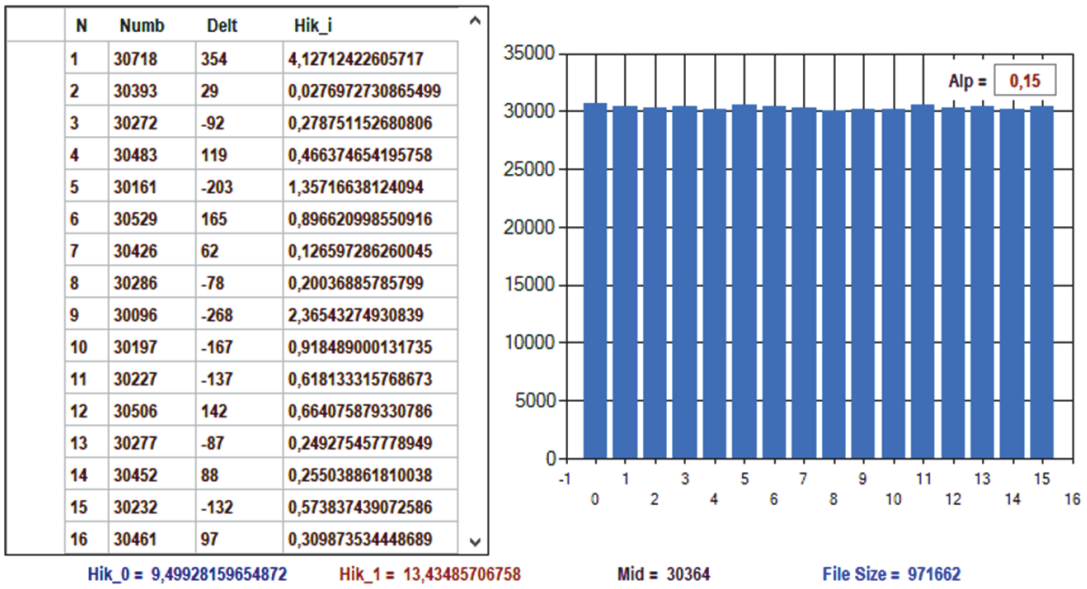
```
C++
x = 123456789; y = 362436069; z = 521288629; w = 88675123;
t = x ^ ((x << 11) & 0xFFFFFFFF);
x = y;
y = z;
z = w;
w = (w ^ (w >> 19)) ^ (t ^ (t >> 8));
```

Унікальність сформованої шифруючої гами досягається введенням у якості ключа чотирьох початкових 32-х бітних чисел x, y, z та w, які визначають початковий внутрішній стан генератора. Кожне наступне число $w = \{N_0, N_1, \dots, N_{31}\}$ уявляє собою комбінацію розрядів чисел x та попереднім значенням w так, як це показано у наведеному фрагменті коду. На кожному такті роботи відбувається зсув чисел $x \to y$, $z \to w$ та $w \to z$. В роботі [4] наведено обґрунтування того факту, що саме наявність використання операцій зсуву дає можливість підвищення випадковості молодших байт 32-х розрядних чисел w_i на виході генератора гами. У більшості присвячених цьому питанню робіт, пропонується просто відкидати молодшу частину сформованого числа, що не раціонально, з точки зору ефективності алгоритму.

Для оцінки придатності генератора Xorshift-генератора ПВЧ для криптографічних потреб, необхідно, щоб розподілення випадкових чисел на його виході w_i задовольняло вимо-

гам рівномірності розподілення ймовірностей. Тобто, числа, сформовані з бінарних комбінацій фіксованої довжини n, повинні мати параметри математичного очікування m_x, дисперсії D_x та середньо квадратичного відхилення σ_x близькі до наступних величин: $m_x = 0.5\ [2^n]$, $D_x \approx 0.0833\ [2^n]$ і $\sigma_x \approx 0.02887\ [2^n]$.

Для отримання відповіді на питання про те, наскільки послідовність ПВЧ відповідає заданому закону розподілення ймовірностей, використовують запропонований у 1900 році Карлом Пірсоном критерій "χ- квадрат" [5]. Перш за все, створюють відрізок псевдовипадкової послідовності чисел, як об'єкту дослідження. Краще, щоб його довжина дорівнювала періоду повторення, але це нереально через його величину і, тому, обмежуються її реальним розміром. Потім будується гістограма, число секторів якої обирається достатнім, виходячи із бажаної точності оцінки.



N	Numb	Delt	Hik_i
1	30718	354	4,12712422605717
2	30393	29	0,0276972730865499
3	30272	-92	0,278751152680806
4	30483	119	0,466374654195758
5	30161	-203	1,35716638124094
6	30529	165	0,896620998550916
7	30426	62	0,126597286260045
8	30286	-78	0,20036885785799
9	30096	-268	2,36543274930839
10	30197	-167	0,918489000131735
11	30227	-137	0,618133315768673
12	30506	142	0,664075879330786
13	30277	-87	0,249275457778949
14	30452	88	0,255038861810038
15	30232	-132	0,573837439072586
16	30461	97	0,309873534448689

Рис. 1. Результати статистичних випробувань генератора ПВЧ

Нехай, наприклад, способом гамування послідовністю з виходу Xorshift-генератора шифрується файл розміром у 971662 байти. Потім, після гамування він розділяється на фрагменти по два байти. Максимальним цілим числом, в такому разі, що може відповідати окремому фрагменту, буде число 65535. При абсолютно рівномірному розподіленні таких чисел на виході генератора ПВЧ, в кожен фрагмент гістограми, що містить 16 секторів, очікується попадання 30364 чисел. Однак, через відсутність абсолютної рівномірності, як це видно із таблиці, наведеної на рисунку 1, буде спостерігатись деяке відхилення від цієї величини на величину *delt*. Показник нерівномірності вихідної послідовності, обчислений за критерієм Пірсона, має вигляд

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - p_i N)^2}{p_i N}.$$

Тут n_i – кількість інтервалів гістограми, p_i – ймовірність попадання окремого числа в і-й інтервал, а N – це загальна кількість двобайтових ПВЧ в послідовності.

Щоб обчислити показник критерію χ^2-Пірсона, слід задатися числом ступенів свободи, що в даному випадку вимірюється як зменшене число секторів гістограми $\nu = k - 1 = 16 - 1 = 15$, а можливе відхилення від рівномірного розподілення α, задається у відсотках.

Теоретичне порогове значення показника χ^2 можна отримати з таблиць або через спеціальну функцію вбудовану в бібліотеку мови С++, а практичне – через оброблення даних, наведених в таблиці на рисунку 1.

Сучасний стан розвитку автоматизованих розподілених інформаційних систем вимагає пошуку нових інженерно технічних рішень в галузі криптографічного захисту інформації. Зазвичай, поточні шифри, що використовуються для шифрування даних в реальному часі, уявляють собою комбінацію декількох компонентів: програмних генераторів ПВЧ, засобів пост оброблення вихідного числового потоку та синхронізації. Основною ціллю досліджень в цьому напрямку є пошук ефективних, з точки зору криптографічної стійкості і простоти формування псевдовипадкових чисел, процедур програмної реалізації генераторів ПВЧ. Як показують результати виконаних досліджень, одним із можливих рішень цієї проблеми є використання запропонованого Джорджем Марсальєю економічного лінійного генератора Xorshift.

Список використаних джерел

1. Schneier B. Applied Cryptography : Protocols, Algorithms, and Source Code in C. 2nd ed. 1995. 662 p.

2. Ferguson N., Schneier B. Practical cryptography. 2003. 539 p.

3. Panneton F., L'Ecuyer P. On the Xorshift Random Number Generators. *ACM Transactions on Modeling and Computer Simulation*. 2005. Vol. 15, Iss. 4. P. 346–361. DOI:10.1145/1113316.1113319. URL: https://web.archive.org/web/20210126143346/http://www.iro.umontreal.ca/~lecuyer/myftp/papers/xorshift.pdf

4. Rueppel R. A. Good stream ciphers are hard to design. *International Carnahan Conference on Security Technology* : Proceedings, Zurich, Switzerland, 3–5 Oct. 1989. DOI:10.1109/CCST.1989.751974. URL: https://www.researchgate.net/publication/3790837_Good_stream_ciphers_are_hard_to_design

5. Knuth D. E. The Art of Computer Programming. Vol. 2. Seminumerical Algorithms. 3rd ed. Boston, Mass, USA : Addison-Wesley, Longman Publishing, 1997. 762 p.

Ключові слова: Поточные шифры, Блочные шифры, Критерий Пирсона, фоновый трафик, Равномерное распределение вероятностей.

Keywords: Stream ciphers, Block ciphers, Pearson criterion, background traffic, Uniform probability distribution.

Грезіна Олена Миколаївна

Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій, доктор філософії у галузі права

ЦИФРОВА МАЙСТЕРНІСТЬ ТА ІННОВАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ – БЕЗПЕКОВІ ВИКЛИКИ ДЛЯ СФЕРИ ОСВІТИ

У сучасну цифрову епоху інформаційні технології є невід'ємною складовою сфери освіти, відкриваючи безліч можливостей для покращення освітнього процесу та підвищення якості освіти. Цифрова майстерність, що означає вміння ефективно використовувати інформаційні технології, стає ключовим компетентним елементом сучасної освіти. Проте разом з цими перевагами постають і значні безпекові виклики, які можуть стати перешкодою для успішної інтеграції технологій в освітній процес України.

Актуальність даної теми полягає в тому, що сучасна освіта стикається з різноманітними безпековими загрозами в контексті використання інформаційних технологій. Зростання кількості кібератак, витоків конфіденційної інформації, а також інші форми кіберзлочинності ставлять під загрозу якість освіти та приватність учасників освітнього процесу. Освіта є важливим фактором розвитку суспільства, розуміння і вирішення безпекових проблем, пов'язаних з інформаційними технологіями в освіті має бути невідкладним завданням для освітян, дослідників та практиків.