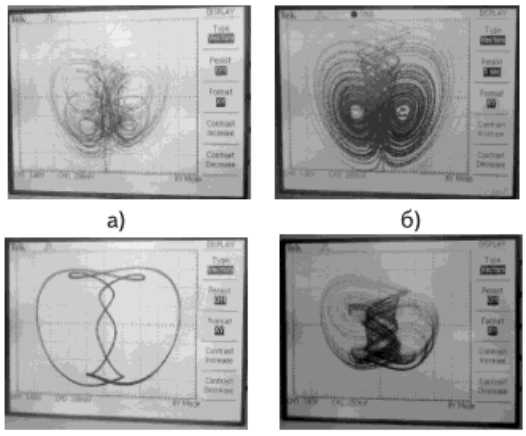

Рис. 7. Фазові траєкторії системи для зібраної схеми, що були спостережені на осцилографі в площині x-z (U_{C1} – U_{C3}): а) хаотичні коливання ; б) - гіперхаотичні коливання; в) періодичні коливання; г) квазіперіодичні коливання

Часові залежності динамічної змінної x (U_{C1}) для різних коливальних режимів приведені на рис. 8. З отриманих результатів чітко прослідковуються хаотичні, гіперхаотичні, періодичні та квазіперіодичні коливання.

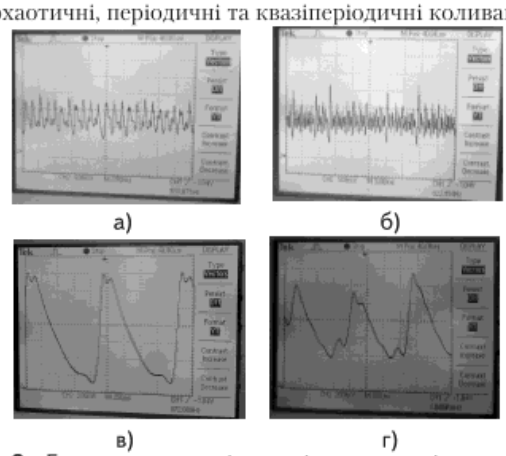

Рис. 8. Експериментальні часові залежності динамічної змінної x (U_{C3}) системи Лю для різних коливних процесів: а) хаотичні коливання ; б) – гіперхаотичні коливання; в) періодичні коливання; г) квазіперіодичні коливання.

Результати моделювання електричної схеми в програмних середовищах LabVIEW та Micro-cap практично співпадають з експериментально отриманими результатами. Різницю між значеннями опорів отриманими та експериментальними можна пояснити наближеними методами обчислення систем проектування.

V. Висновки

Проведене чисельне моделювання системи Лю в програмному середовищі LabVIEW.

Моделювання електричної схеми в програмному середовищі Micro-cap показало можливість практичної реалізації в ній різних видів коливних процесів в залежності від зміни параметрів, що описують систему Лю.

Спроектовано електричну схему на базі системи Лю, що генерує гіперхаотичні коливання.

Параметри коливань в експериментальних зразках генераторів гіперхаотичних коливань на базі системи Лю вказують на перспективу їх застосування в системах зв'язку з використанням хаотичних процесів.

Література

1. Фрадков, А. Л. Управление хаосом: Методы и приложения. II. Приложения. [Текст] / Б. Р. Андриевский, А. Л. Фрадков // Автоматика и телемеханика. – 2004. – Вып. 4. – С. 3–34.
2. Jinhu Lu, The compound structure of a new chaotic attractor. [Текст] / Jinhu Lu, Guanrong Chen, Suochun Zhang // Chaos, solitons and fractals. – 2002. – No. 14. – P. 669–672.
3. Wang Fa-Qiang, Hyperchaos evolved from the Liu chaotic system. [Текст] / Wang Fa-Qiang, Liu Chong-Xin // Chinese Physics. 2006. – Vol. 15 No. 5. – P. 963–968.
5. Luo Xiao-Hua, Circuitry implementation of a novel four-dimensional nonautonomous hyperchaotic Liu system and its experimental studies on synchronization control [Текст] / Luo Xiao-Hua at al. // Chinese Physics B. – 2009. Vol. 18 No. 6. – P. 2168–2175.
6. Кузнецов, С.П. Динамический хаос. М. [Текст] / С.П. Кузнецов. – М.: Изд-во Физматлит, 2001. – 296 с.

Проведено аналіз стану розвитку інструментальних засобів для тестування симетричних криптографічних перетворень і генераторів псевдовипадкових послідовностей, вживаних в криптографії.

Ключові слова: *псевдовипадкова послідовність, криптографічне перетворення, криптографія.*

Проведен анализ состояния развития инструментальных средств для тестирования симметричных криптографических превращений и генераторов псевдослучайных последовательностей, употребимых в криптографии.

Ключевые слова: *псевдослучайная последовательность, криптографическое превращение.*

The analysis of development status of tools is conducted for testing of outputs sequences of symmetric coding devices and generators the psevdocasual sequences applied in cryptography.

Keywords: *pseudo-random sequence, kriptografiches-something conversion.*

УДК 519.876.5.:621.391; 621.391:519.72

СТАТИСТИЧНЕ ТЕСТУВАННЯ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

О. О. Скопа

Кандидат технічних, доцент

Кафедра інформаційних систем в економіці

Одеський державний економічний університет

вул. Преображенська, 8, м. Одеса, 65082

Контактний тел.: (048) 703-64-23,

050-504-17-81, 094-955-94-23,

E-mail: skopa2003@ukr.net

Постановка проблеми в загальному вигляді та її зв'язок з важливими науковими або практичними завданнями

Безперервне вдосконалення симетричних шифрів та розробка інструментальних засобів їх тестування пояснюється зацікавленістю до них фахівців, які забезпечують конфіденційність, достовірність та цілісність інформації, яка циркулює в сучасних інформаційно-телекомунікаційних системах. Саме цим пояснюється різноманіття існуючих тестуючих пакетів і пошук нових способів тестування. Проблема полягає в тому, що до теперішнього часу роботи, опубліковані в цій області, розрізнені і ця область криптоаналізу, що базується на фундаментальних положеннях математичної статистики, ще остаточно не сформувалася як самостійний розділ. Це створює серйозні проблеми і для фахівців, які розробляють нові шифри, і для організацій, що займаються сертифікацією криптографічних засобів.

Аналіз останніх досліджень і публікацій, в яких покладено початок вирішення проблеми; виділення невирішених питань загальної проблеми

Проведений аналіз доступних літературних джерел показав, що не існує універсальних засобів, які дозволяють швидко і без додаткових інтелектуальних зусиль оцінити новий криптографічний алгоритм або криптографічне перетворення. Створені до сьогоднішнього часу інструментальні засоби, дозволяють проводити лише попередню оцінку їх якості.

У кожному конкретному випадку, не дивлячись на існування загальних підходів, для оцінки нової розробки, необхідно розробляти свій, унікальний метод криптографічного аналізу. З цієї причини шифри, пропоновані на роль державних стандартів, або вже прийняті як такі, прийнято вважати стійкими, до тих пір, поки не стане відомо про їх ефективний злом.

Враховуючи, що більшість відомих симетричних криптографічних систем застосовуються в режимі гамування, фахівцями, що працюють в області практичної криптографії, створено безліч тестів, які дозволяють проводити оцінку розподілу вірогідності як формованих гаммуючих псевдовипадкових послідовностей, так і зашифрованих текстів. Високий ступінь їх відповідності рівномірному закону розподілу вірогідності якщо і не гарантує їх високої криптографічної стійкості, то, в усякому разі, є попередньою обов'язковою умовою для хорошого шифру.

Зазвичай розробники шифрів самі створюють програмне забезпечення, що дозволяє на різних етапах проектування здійснювати попередню проміжну оцінку отриманих результатів. Для точнішої об'єктивної оцінки кінцевого продукту застосовують відомі пакети тестів, які отримали широке визнання в середовищі криптоаналітиків [1...3]. Проте проблема ця не так проста.

На основі сказаного, сформулюємо ***раніше невирішені частини загальної проблеми***. Не дивлячись на відносну доступність програмного забезпечення, що реалізовує набори згаданих тестів, їх докладне наукове обгрунтування не публікується. В кращому разі, можна скористатися керівництвом користувача. У цьому полягає перша частина проблеми. Друга частина полягає в тому, що згадані набори тестів не є чимось закінченим і, очевидно, їх склад поповнюватиметься. Отже, ***постановкою завдання і метою роботи*** є аналіз стану питання по розробці нових тестів, орієнтованих на потреби криптографії, що само по собі представляє окремий напрям в цій області.

Виклад основного матеріалу

Зазвичай, перша частина викладеної проблеми вирішується шляхом створення національного стандарту так, як це було зроблено фахівцями NIST, які в 1999 році в рамках проекту AES (*Advanced Encryption Standard*) розробили набір статистичних тестів NIST STS (*NIST Statistical Test Suite*) для випробування псевдовипадкових послідовностей. Очевидно, що і в наший країні доцільно було б мати подібний національний стандарт, його доступне наукове обгрунтування, а також методику його програмної реалізації. Поява такого документа послужила б відправною точкою для систематичних наукових досліджень в цьому напрямі.

Що стосується другої частини проблеми – вдосконалення та розробки нових тестів, то на цьому зупинимося докладніше.

Всі види тестів, що розробляються, можуть бути віднесені до однієї з двох груп (рис. 1).

Рис. 1. Множина тестів

Велика частина відомих тестів вирішує саме другу задачу. Вперше в найпростішому вигляді вона була сформульована Д. Кнутом в його класичній роботі «Мистецтво програмування для ЕОМ» [4] і зводилася до відповіді на питання про те, наскільки відповідає розподіл вірогідності деякої випадкової величини в спостережуваному процесі, очікуваному виду розподілу. Це найбільш рання і найбільш цитована робота, що написана за часів становлення обчислювальної техніки і не відноситься до області криптографії. Основний упор автор робив на економії обмежених в ті часи обчислювальних ресурсів і не ставив питання про точність методу, яка є особо важливою в області криптоаналізу.

При створенні симетричної криптографічної системи потрібно досягти, по можливості, найбільшого наближення до рівномірного закону розподілу вірогідності символів або на виході генератора випадкових чисел, або в зашифрованій симетричним шифром інформаційній послідовності. У загальному вигляді ці вимоги можуть бути сформульовані так [5]:

1. Відсутність аналітичної залежності між послідовно сформованими числами.

2. Спостерігаючи попередні числа на деякому інтервалі, криптоаналітик не може передбачити наступні числа з вірогідністю, відмінною від 0,5 (атака з минулого).

3. Спостерігаючи подальші числа на деякому інтервалі, криптоаналітик не може передбачити наступні числа з вірогідністю, відмінною від 0,5 (атака з майбутнього).

4. Всі числа у формованій послідовності рівноімовірні.

Ці вимоги витікають з умов досконалого шифрування, сформульованих К. Шенноном [6]. Перша з них, звичайно ж, не виконується, оскільки мова йде про псевдовипадкові послідовності. Що стосується інших трьох вимог, то, чим більшою мірою вони дотримуються, тим ближче стійкість досліджуваного шифру наближається до досконалого.

На перший погляд, перевірити рівномірність розподілу символів в псевдовипадковій послідовності, що генерується, просто. Для цього можна, наприклад, скористатися критерієм згоди χ^2 Пірсона, як це запропоновано Д. Кнутом [4]. Про те, як користуватися цим критерієм, написано багато. У Росії, наприклад, виданий державний стандарт [7], який регламентує його застосування, містить рекомендації по оптимізації вибору інтервалів розбиття тестованої величини і методики його використання для різних типів розподілу вірогідності випадкових величин.

Річ у тому, що поняття «випадковості» на філософському рівні до цих пір не визначене. З математичної ж точки зору, псевдовипадкова послідовність може бути визнана випадковою і рівномірно розподіленою, якщо всі символи, що генеруються, та їх комбінації в такій послідовності зустрічаються з рівною імовірністю. На жаль χ^2-критерий «не відчуває» схильності символів, що формуються джерелом, до групування. З цієї причини для підтвердження «випадковості» псевдовипадкових послідовностей застосовують цілі набори тестів. Їх мета – виявити будь-які можливі регулярні аномалії, які в майбутньому могли б бути використані як уразливості для організації атак на шифри, що розроблялися.

Як приклад розглянемо деякі тести, що входять в комплект *NIST STS* [1].

1. Частотний (монобітовий) тест (*Frequency (Monobits) Test*). У цьому тесті досліджується співвідношення між 0 і 1 в послідовності і наскільки ця послідовність близька до ідеального варіанту – рівноімовірної послідовності.

2. Частотний (блоковий) тест (*Test for Frequency within a Block*). У цьому тесті досліджувана послідовність розбивається на блоки довжиною m біт ($m > 20$), і для кожного блоку розраховується частота появи одиниць. Визначається, наскільки вона близька до еталонного значення – $m/2$.

3. Тест на серійність (*Runs Test*). У цьому тесті ідентифікуються всі серії однакових бітів, а їх розподіл порівнюється з очікуваним розподілом таких серій для випадкової послідовності.

4. Тест на максимальний розмір серії одиниць (Test *for the Longest Run of Ones in a Block*). У цьому тесті досліджується довжина найбільшої безперервної послідовності одиниць і порівнюється з довжиною такого ланцюжка для випадкової послідовності.

5. Спектральний тест на основі дискретного перетворення Фурье (*Discrete Fourier Transform (Spectral) Test*). У цьому тесті виявляються блоки, що повторюються, або підпослідовності.

6. Комплексний тест Лемпела-Зіва (*Lempel-Ziv Complexity Test*). Цей тест визначає ступінь стисливості досліджуваної послідовності.

З опису приведених тестів видно, що всі вони орієнтовані на пошук стійких залежностей між формованими символами і можуть бути віднесені до тестів другої групи. До складу пакету *NIST STS* входить ще десять тестів, які також орієнтовані на конкретні види аномалій в рівномірному розподілі вірогідності і разом з попередніми шістьма тестами дозволяють отримати достовірну і об'єктивну оцінку тестованих послідовностей. Опис перерахованих тестів і відповідне програмне забезпечення доступні за адресою http://csrc.nist.gov/groups/ST/toolkit/rng/index.html. Воно розповсюджується у вигляді початкових кодів для платформи Unix і містить як інструменти командного рядка, так і графічні утиліти. Невиконання хоч би одного з тестів автоматично відміняє все подальші тести, і тестована послідовність визнається «невипадковою».

Аналогічно влаштовані й інші пакети. Сьогодні, наприклад, відомий набір статистичних тестів під назвою *Diehard* [2] для вимірювання якості послідовності випадкових чисел. Вони були розроблені Д. Марсал'ем (*George Marsaglia*). Набір включає 12 тестів і доступний за адресою http://stat.fsu.edu/pub/diehard/.

За адресою http://www.isi.qut.edu.au/resources/cryptx/ можна зв'язатися з розробниками пакету тестів *CRYPT-X* [3] і отримати програмне забезпечення та керівництво по застосуванню.

Не дивлячись на існування тестуючих пакетів, що пройшли перевірку часом, робота в цьому напрямі продовжується. Так, наприклад, в роботі [8], на прикладі пакету *NIST STS*, запропоновано ввести деякий узагальнений показник, що обчислюється за наслідками виконання всіх тестів, які входять до пакету. Це дає можливість судити про відповідність випробовуваної послідовності криптографічним вимогам. Там же викладена і зразкова методика обчислення цього показника. Хоча ця ідея є корисною, але є простіше правило, озвучене раніше: невиконання хоч би одного з тестів свідчить про непридатність сформованої послідовності.

Основним спонукаючим мотивом до пошуку нових тестів служить робота криптоаналітиків, які досліджують стійкість шифрів, що розробляються, або фахівців, якіорганізують криптографічні атаки на такі шифри. Їх цікавить не формальний доказ стійкості шифру, заснований на деяких статистичних показниках, а їх реальні вразливості, які можуть бути покладені в основу сценарію конкретної атаки. Саме ця причина примушує будувати все нові тести, що виявляють закономірності, наявні в досліджуваних послідовностях.

Прикладом такої розробки є відносно недавно запропонований тест, який автори назвали «Стопка книг» [9]. Цей тест є спробою удосконалення відомого критерію згоди χ^2 Пірсона. Суть його зводиться до того, що на відміну від критерію χ^2, числа, що формуються генератором, постійно змінюють свій рейтинг усередині діапазону $[0,2; ...; n-1]$, де n – розрядність машинного слова. Сформоване генератором число переміщається на перше місце, а решта чисел з початку діапазону зрушується на крок управо до того місця, яке займало сформоване число на момент його генерації, аналогічно тому, як це відбувається зі стопкою книг, коли витягувана випадковим чином книга кладеться вгору стопки. Це приводить до того, що символи, які генеруються частіше, відповідно частіше

знаходитимуться в лівій частині діапазону. Далі весь діапазон розбивається на відносно невелике число інтервалів і оцінка рівномірності розподілу вірогідності здійснюється за допомогою критерію згоди χ^2 Пірсона. Передбачається, що, у разі рівномірного розподілу, вірогідність попадання чисел у всі діапазони буде однакова. Основною гідністю критерію, на думку авторів, є економія обчислювальних ресурсів за рахунок істотного зниження кількості інтервалів на які розбивається досліджуваний діапазон чисел. Правда, автори умовчують про те, що сама процедура моделювання «стопки книг» теж зажадає достатньо великих витрат пам'яті. Як друга гідність запропонованого тесту автори виділяють його велику чутливість до нерівномірності тестованої послідовності, що підтверджується даними проведених випробувань. Так це чи ні, покаже час.

Таким чином, робота в області побудови ефективних критеріїв якості є актуальною і науковий пошук в цьому напрямі буде продовжений.

Висновок

На сьогоднішній день відомо багато як блокових, так і потокових симетричних шифрів, які до цього часу не були розшифровані успішно проведеними на них атаками. Проте, на жаль, виявляється безліч уразливостей в телекомунікаційних протоколах, в які вбудовуються ці шифри. Це, в першу чергу відноситься, до програмних генераторів ключів. З цієї причини створення надійних інструментальних засобів, що дозволяють проводити оцінку якості розробок в області симетричної криптографії, є актуальним завданням. Більш того, необхідний національний стандарт, що закріплює прикладний пакет і методику статистичного тестування криптографічних засобів, наявність якого істотно полегшила б завдання всім зацікавленим суб'єктам, які так або інакше що беруть участь в забезпеченні інформаційної безпеки в Україні.

Розглянуто питання вимірювання параметрів ліній зв'язку та визначення характеру і місця пошкодження цих ліній, з метою визначення вихідних даних при розробці цифрового приладу для вимірювання параметрів лінії зв'язку.

Ключові слова: *електрозв'язок, вимірювання, опір, ємність, схема.*

Рассмотрены вопросы измерения параметров линий связи и определение характера и места повреждения этих линий, с целью определения исходных данных при разработке цифрового прибора для измерения параметров линии связи.

Ключевые слова: *электросвязь, измерение, сопротивление, емкость, схема.*

The problems of measurement lines and determine the nature and location of the damage these lines, in order to establish baseline data for the development of a digital device for measuring the parameters of the line.

Keywords: *telecommunications, measuring, resistance, capacitance, circuit.*

Література

1. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.
2. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness / http:// www.stat.fsu.edu/pub/diehard.
3. Statistical test suite Crypt-X //http://www.isi.qut.edu.au/resources/cryptx.
4. Кнут Д. Искусство программирования для ЭВМ. – Т.2. – М.: Мир, 1977. – 727 с.
5. Казакова Н.Ф. Поэтапное тестирование и подбор составных элементов генераторов псевдослучайных последовательностей [Текст] / Восточно-Европейский журнал передовых технологий. –2010. - №2/8(44). – С.44-48.
6. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М., ИЛ, 1963. – С. 333-369.
7. Р50.1.037-2002 Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа хи-квадрат. – 14.12.2001 / http://www.tcnti.ru/shop/catalog/index.php?docum=25096.
8. Потий А.В., Орлова С.Ю., Гриненко Т.А. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS [Текст] / http://wwww.kiev-security.org.ua/box/19/82.shtml
9. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.

УДК 621.391.01

ОПРЕДЕЛЕНИЕ МЕТОДА ИЗМЕРЕНИЯ И ПАРАМЕТРОВ ЛИНИИ СВЯЗИ ДЛЯ ЦИФРОВОГО ПРИБОРА

Ю. А. Смолин
Кандидат технических наук, доцент
Кафедра радиоэлектроники и компьютерных систем
Украинская инженерно-педагогическая академия
ул. Университетская 16, г. Харьков, Украина, 61003
Контактный тел.: 067-458-37-35