УДК 004.421.5
Б. Баняс
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ В КРИПТОГРАФІЧНИХ ЗАСОБАХ ЗАХИСТУ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМ

UDC 004.421.5
B. Banias

METHODS OF FORMING PSEUDO-RANDOM NUMBERS IN CRYPTOGRAPHIC MEANS OF PROTECTION OF BANKING INFORMATION SYSTEMS

В умовах стрімкої інформатизації суспільства, широкого застосування засобів обчислювальної техніки і комп'ютерних систем особливої актуальності набувають питання інформаційної безпеки, найскладнішими з яких є необхідність захисту цінної конфіденційної і секретної інформації. Збільшення обсягів оброблюваних і переданих даних у комп'ютерних системах і мережах, перш за все в банківських системах вимагає нових підходів до протоколів та механізмів забезпечення безпеки переданих даних [1–3]. Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту інформаційні системи схильні до різних атак і погроз. Під загрозою безпеки інформаційної системи розуміються можливі впливи на інформаційну систему, що прямо чи побічно можуть завдати шкоди її безпекці.

Для забезпечення захисту від загроз безпеки використовуються різні криптографічні механізми. Для побудови механізмів безпеки інформації традиційно використовують методи криптографічного обробки інформації. Важливе місце у розвитку сучасних механізмів забезпечення безпеки інформаційних систем і технологій займає використання випадкових чисел (ПВЧ) і відповідно генераторів псевдовипадкових чисел (ГПВЧ). Вони використовуються для вирішення наступних завдань: хешування інформації; побудови синхронних і самосінхронізірующіхся потокових шифрів; формування ключової інформації і т.д. [3–5].

Характеристики систем безпеки в більшості своїй залежать від функцій їх криптографічних підсистем, які визначаються не тільки алгоритмікою, але і якісними показниками саме використовуваних псевдовипадкових послідовностей. Так як безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому так само вразлива [5]. Формування ПВЧ здійснюється за допомогою відповідних ГПВЧ реалізованих на основі відомих методів, які можна розділити на два класи: криптостійкі і некріптостойкі. Класифікація методів формування ПСП наведена на рис. 1.

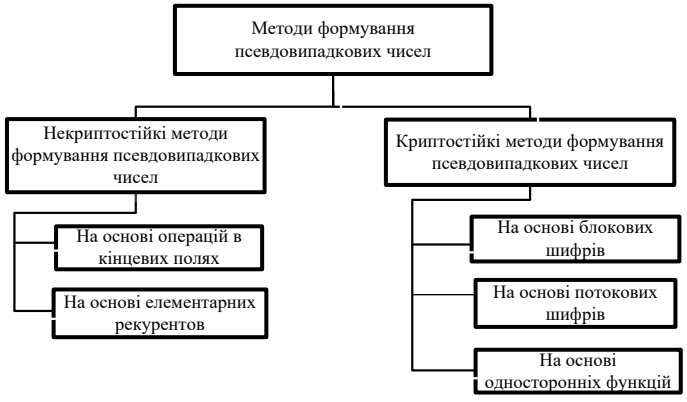

Рисунок 1. Класифікація методів і генераторів формування псевдовипадкових чисел

Прикладами генераторів на основі елементарних рекурентов є лінійний і поліноміальний конгруентний генератор, адитивний і мультиплікативний генератор Фібоначчі. Найчастіше на практиці використовуються лінійні конгруентні генератори. Лінійними конгруентними генераторами є генератори наступної форми [6, 9]:

$$x_i = (ax_{i-1} + b) \bmod m \tag{1.1}$$

де x_i – і–й елемент псевдовипадкової послідовності; $a \neq 0$ – множник; b – приріст; m – потужність послідовності (модуль).

Основними перевагами конгруентних генераторів є:

– максимальний період формуючої послідовності;

– простота програмної та апаратної реалізації;

– можливість побудови на їх основі генераторів, що володіють властивостями, необхідними для вирішення прикладних питань захисту інформації.

Недоліком таких генераторів є формування псевдовипадкових чисел некриптостійких до різних видів криптоаналізу (кореляційний, інверсний та ін.) Тому конгруентні генератори використовуються для вирішення завдань захисту інформації як складові елементи кріптосхем [6, 9–11].

До криптостійких ГПВЧ відносяться генератори, побудовані на основі потокових шифрів. Прикладами можуть служити генератор SEAL, RC4, RC5, RC6, Grain та інші. Дані генератори, використовуючи більшість потокових шифрів, створюють односпрямовану послідовність бітів: єдиним способом визначити і-ий біт, знаючи ключ і позицію і, є генерування всіх бітів аж до і-ого.

Основною перевагою генераторів ПВЧ побудованих на основі потокових шифрів є висока швидкість перетворення, співмірна зі швидкістю надходження вхідної інформації. Таким чином, забезпечується формування ПСЧ в реальному масштабі часу.

Недоліками є необхідність синхронізації на приймальній і передавальній стороні [6, 9].

Наступним класом криптостійких генераторів є ГПВЧ побудовані на блокових шифрах [6, 12]. Робота таких генераторів полягає в застосуванні до блоку відкритого тексту багаторазового математичного перетворення.

Основними перевагами ГПВЧ побудованих на основі блокових шифрів є: хороші статистичні властивості формованої псевдовипадкової послідовності і стійкість до різних видів криптоаналізу (кореляційний, інверсний тощо) [6,12].

До основних недоліків блокового шифрування можна віднести:

– нечутливість кріптосхем до випадання або вставці цілого числа блоків;

– існування проблеми останнього блоку неповної довжини.

Особливим напрямком у розвитку криптостійких генераторів отримали методи, які допускають можливість застосування моделі доказовою стійкості. До них належать методи, засновані на вирішенні односторонніх функцій [6, 11, 13]. Генератори, засновані на вирішенні односторонніх функцій, називаються доказово стійкими генераторами. До доказово стійких генераторів відносяться ГПВЧ BBS і RSA.

Істотним недоліком таких генераторів є висока обчислювальна складність, яка визначається, перш за все, великою розрядністю чисел, над якими необхідно виконувати математичні операції, що істотно знижує швидкість формування ПВЧ в порівнянні з генераторами, заснованими на блокових або поточних шифрах [6, 7].

Перспективним напрямком у розвитку методів формування ПВЧ є розробка та дослідження ГПВЧ заснованих на проблемі декодування випадкового коду GPSSD (Pseudo-Random Generator Provably as Secure as Syndrome Decoding), де завдання криптоаналізу фактично зводиться до вирішення теоретико-складного завдання синдромних декодування.

Основна ідея такого генератора полягає у використанні алгебраїчного блокового коду з легко реалізованими алгоритмами кодування та декодування [7–9]. За допомогою маскування алгебраїчного коду під випадковий код, завдання декодування для зловмисника представляється як обчислювально складне.

Проведені дослідження показали, що генератор GPSSD дає кращі показники швидкодії і статистичної безпеки. Його недоліком є неможливість формування послідовності максимального періоду, а його періодичні властивості незадовільні [8].

Таким чином перспективним напрямком подальших досліджень є розробка удосконаленого методу на основі надлишкових блокових кодів, який крім високих показників статистичної безпеки та швидкодії дозволить формувати послідовності максимального періоду.

Література.

1. Задірака В.К. Методи захисту банківської інформації. / В.К. Задірака, О.С. Олесюк, Н.О. Недашковський – Киів. Вища школа, 1999 – 264 с.
2. Конеев И. Р. Информационная безопасность предприятия / И. Р.Конеев, А.В. Беляев – Спб.: БХВ-Петербург, 2003. – 752 с.
3. Дудикевич В.Б. Протоколы и механизмы безопасности информации в компьютерных системах и сетях / Дудикевич В.Б., Томашевский Б.П., Сергиенко Р.В. Технический отчет ІІТ – 003-2002
4. Кузнецов А.А. Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / Матеріали І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних і телекомунікаційних системах» 28–29 травня 2008 р. Зб. наук. статей «Управління розвитком»./ Кузнецов А.А., Король О.Г., Ткачов А.М. / ХНЕУ. № 6 – Х.: 2008. – С. 28–35.
5. Інформаційний портал Все об ІТ. [Електронний ресурс] Режим доступу до журн.: http://itc.ua
6. Шнайер Б. Практическая криптография / Шнайер Б., Фергюсон Н. – Издательский дом «Вильямс». 2005. – 423 с.
7. Кузнецов А.А. Усовершенствованный метод быстрого формирования последовательностей псевдослучайных чисел/ Зб. наук. пр. "Кібернетика та системний аналіз"/ Кузнецов А.А., Королёв Р.В., Рябуха Ю.Н./ ХНВС. – Харьков:2008.
8. Корольов Р.В. Дослідження періодичних властивостей генераторів псевдовипадкових чисел, заснованих на використанні надмірних блокових кодів / Р.В.Корольов // Системи озброєння і військова техніка. – 2008. – № 3 (15). – С. 126–128.
9. Иванов Чугунков Теория, применение и оценка качества генераторов псевдослучайной последовательности – Масква. «Кудиц-Образ». 2003 – 240с.
10. Вільна енциклопедія [Електронний ресурс] Режим доступу до журн.: http://ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел.
11. Ященко В. В. Введение в криптографию / Ященко В. В., Черемушкин А. В. – Издательский дом «Питер». 2000. – 288 с.
12. Брассар Ж. Современная криптография – Поли мед. 1999. – 178 с.
13. Кузнецов А.А. Исследование статистической безопасности генераторов псевдослучайных чисел / А.А. Кузнецов, Р.В. Королев, Ю.Н. Рябуха // Системи обробки інформації. − Х.: ХУ ПС, 2008. − Вип. 3 (70). – С. 79–82.