УДК 004.9

Генерація випадкових чисел з урахуванням параметрів їх криптостійкості

М.В. Гладка, .С. Майстренко

Національний університет харчових технологій

Випадковою називається така послідовність, яку при приведенні в дію алгоритму її генерації з усіма вхідними даними для нього неможливо в результаті отримати. Однак всі комп'ютерні системи мають ряд скінчених станів, тож в зв'язку з цим постає ряд проблем, пов'язаних з генерацією подібних послідовностей.

При розробці програмних продуктів існують задачі, які потребують генерації великої кількості випадкових чисел, що створює додаткові проблеми розробникам. В основному методи, які використовуються в програмуванні дозволяють згенерувати лише псевдовипадкову послідовність чисел. Суть цієї проблеми базується на принципі генерації псевдовипадкової послідовності. Під час генерації таких чисел обирається «зерно», відносно якого генеруються наступні числа як добуток цього числа самого на себе і вибору з нього середніх чисел. В залежності від довжини обраного «зерна», відбувається обмеження довжини випадкових чисел що гарантовано не повторяться, при вичерпанні всіх можливих варіантів, через що вона й називається псевдовипадковою. Враховуючи той факт, що існує ряд задач, для яких необхідна генерація великих об'ємів випадкових чисел, стандартні методи генерації таких чисел за допомогою «зерна» не задовольняють поставлені вимоги і, як наслідок, необхідно застосовувати інші методи, що дозволяють на комп'ютері збільшити період неповторюваних чисел на стільки, скільки необхідно для тої чи іншої задачі, тобто не допустивши їхнього повторення в рамках поставленої задачі. Тобто, необхідно генерувати таку послідовність, яка буде хоч і псевдовипадковою, але в рамках нашої задачі буде задовольняти вимогам криптостійкості, тобто буде криптографічно надійною, коли неможливо спрогнозувати наступний біт, знаючи всі попередні алгоритми генерації випадкових чисел та маючи повні дані про використовувану апаратуру тощо.

Рішенням даної проблеми є використання спеціальних алгоритмів, що хоч і базуються на псевдовипадковій генерації чисел, але все ж таки використовують такі методи для генерації, які забезпечать малу можливість передбачення наступних чисел, а також збільшать довжину періоду неповторення чисел на стільки, що в рамках однієї задачі цього буде достатньо, щоб гарантовано уникнути повторення послідовності чисел.

Подібні алгоритми засновуються на генерації чисел з використанням в істинно випадкових процесів. Наприклад, може використовуватись декілька джерел ентропії, які фактично є шумами в комп'ютері і згенеровану ними послідовність достатньо важко передбачити. До того ж подібний «шум» може використовуватись не лише для визначення початкового «зерна», а й використовуватись для вибору «зерна» на подальших етапах генерації. Це

дозволяє унеможливити передбачення наступних згенерованих чисел, навіть знаючи попередні числа і за рахунок цього значно збільшується період неповторюваної послідовності чисел. Окрім такого підходу існує ще й можливість використання спеціального апаратного забезпечення, яке може виступати в ролі джерела істинних випадковостей. Яскравим прикладом реалізації такого підходу є використання датчику розпаду радіоактивного ізотопа, адже період розпаду радіоактивних частинок є істинно випадковим процесом і на його основі можна генерувати послідовності випадкових чисел, будучи впевненими, що така послідовність не матиме великої кількості повторень. Такий підхід використовується в разі необхідності більш захищених та випадкових чисел.

До популярних математичних методів генерації псевдовипадкових чисел є лінійний конгруентний метод генерації. Метод працює за формулою (1).

$$x_{i+1} = (a*x_i + c) \mod m \quad (1)$$

де x_{i+1}, x_i – наступне і попереднє числа, a,c,m – константи, mod – оператор знаходження залишку від ділення.

В даному методі період повторення згенерованої послідовності дорівнює числу m, тобто при використанні даного методу задача зводиться до вибору такого числа m, при використанні якого період повторення чисел в згенерованій послідовності задовольняв би наші вимоги до послідовності.

Також використовуються і нелінійні конгруентні методи генерації псевдовипадкових чисел, такі як квадратний конгруентний генератор, тощо. Працюють вони за формулою (2).

$$x_{i+1} = (a*x_i^n + c) \mod m \quad (2)$$

де x_{i+1}, x_i – наступне і попереднє числа, a,c,m – константи, mod – оператор знаходження залишку від ділення, а n – степінь, що відповідає методу (2 для квадратного генератора, тощо).

Використання подібних методів збільшує період повторення чисел в згенерованій послідовності, а для значного збільшення періоду часто використовують суперпозицію нелінійних конгруентних генераторів.

Саме використання таких методів генерації чисел дозволяє збільшити криптостійкість усієї системи, що потребує надійності захисту від сторонніх посягань.

Література

1. *Дональд Э. Кнут* Исскуство программирования / Дональд Э. Кнут – М.: "Вильямс", 2000. – 832 с.

2. *Успенский В.А.* Четыре алгоритмических лица случайности / В. А. Успенский – М.: «МЦНМО», 2006. – 48 с.