А.О. Долгих, магістр, гр. ПІ-45м, ФІКТ
Науковий керівник – к.т.н., доц. І.І. Сугоняк
Житомирський державний технологічний університет

ГЕНЕРАТОР ПСЕВДО ВИПАДКОВИХ ЧИСЕЛ

Послідовність називається псевдовипадковою, якщо вона виглядає, як безсистемна і випадкова, хоча насправді вона створювалась з допомогою суто детермінованого процесу, відомого під назвою псевдовипадкового генератора. Подібні генератори переважно задаються деяким початковим значенням і за допомогою певних алгоритмів отримують з нього випадкові послідовності. В цьому сенсі псевдовипадкові генератори можна розглядати як розповсюджувачі випадковості.

Комп'ютери є детермінованими машинами, що завжди роблять саме те на що вони запрограмовані і це усуває можливість звертатися до комп'ютерів як до джерела істинної випадковості. Саме краще, на що здатний комп'ютер - це згенерувати псевдовипадкову послідовність, яка хоча і виглядає випадковою, але, насправді, такою не є.

Згенерувати дійсно випадкову послідовність можна лише при апаратній реалізації генератора, який би для отримання випадкових чисел використовував деяке фізичне явище, наприклад, шум, який генерують напівпровідникові прилади, молодші біти оцифрованого звуку, інтервали між перериванням пристроїв або натисканням клавіш, температуру повітря і т.д. В сучасних потужних криптосистемах військового призначення використовують генератори випадкових чисел (ГВЧ), які є платами або зовнішніми пристроями, які підключаються до ЕОМ через порт вводу-виводу. а основними джерелами білого Гаусівського шуму є високоточне вимірювання теплових флуктуацій і запис радіоефіру на частоті вільній від радіомовлення.

Незважаючи на труднощі, які виникають при проектуванні генераторів псевдовипадкових чисел (ГПВЧ), вони широко використовуються в прикладних комп'ютерних програмах і легко компонуються з усіма типами комп'ютерних систем. Тому, на сьогоднішній день, більшість прикладних комп'ютерних програм використовують ГПВЧ для генерації потрібних випадкових даних.

ГПВЧ широко застосовуються в багатьох галузях, а особливо в тих, які пов'язані з використанням електронної та електронно-обчислювальної техніки. Основними сферами використання ГПВЧ є:

1. Криптографія (шифрування, розшифрування, генератор ключів);
2. Імітація моделювання (економічні дослідження, математичні дослідження, фізичні дослідження, та інші);
3. Вимірювальна техніка;
4. Розробка комп’ютерних ігор.

Оскільки збільшується передача даних через загальні і приватні мережі, стає все більш важливим захист інформації яка зберігається і передається між комп'ютерами. Один із стандартних блоків безпеки є ГВЧ.

Проблема захисту інформації є багатогранна і вирішується комплексно, з використанням великої кількості способів.

Випадкові числа - фундаментальний елемент для надання обмеженого доступу до інформації. Вони являють собою основний елемент криптографії, цифрового підпису, протоколів безпеки і іншого забезпечення надійності при зв'язку.

В галузі захисту інформації існує окремий напрям, пов’язаний з генерацією випадкових (псевдовипадкових) послідовностей, йде постійна робота по удосконаленню не тільки засобів генерації, але і теорії та термінології в цьому важливому напрямі, проводиться розробка теорії і практики тестування джерел інформаційно-телекомунікаційних мереж випадкових послідовностей, оцінки і вимірювання їх показників.

ГВЧ також часто застосовують в імітаційному моделюванні. В багатьох випадках потрібне використання різних послідовностей випадкових чисел. Наприклад для запуску однієї і тієї ж самої програми (але використовуючи різні потоки випадкових чисел) на багатьох процесорах, з метою отримання статистично незалежних результатів на кожному процесорі, а потім ці результати можуть бути усереднити. Але використання детермінованого алгоритму при генерації чисел є також корисним в багатьох випадках. Наприклад, при моделюванні всіх видів процесів, починаючи від автоматизації телефонних ліній і закінчуючи дорожнім рухом, вимагається, щоб послідовність псевдовипадкових чисел можна було повторити для досліджень поставленої задачі при інших параметрах.

При використанні ГПВЧ необхідно враховувати те, що вони мають бути достатньо надійними. Наприклад, електронний автомат потребує таку послідовність, яку не можна було б передбачити, знаючи попереднє значення; інакше система зазнала б невдачі, якщо б гравець визначав наступні оберти на основі аналізу моделі попередніх обертів, аналогічна ситуація при кодуванні повідомлень - потрібно забезпечити таку випадкову послідовність, щоб знаючи частину розсекреченого документа неможливо було б розсекретити весь документ.

Найчастіше ГПВЧ застосовують в криптографії. Випадковість і криптографія дуже сильно взаємопов'язані. Важко знайти добре розроблене криптографічне прикладне забезпечення, яке не використовує випадкові числа. Криптографічні ключі, їх ініціалізація, тонкощі хешування з паролями, унікальні параметри в операціях цифрового підпису системними розробниками повинні прийматися випадковими. ГПВЧ є криптографічно сильним, якщо послідовність, яку він генерує з короткого таємного вихідного ключа, є майже такою самою, як і справжня випадкова послідовність і ніяке практично легко здійснюване обчислення не може дозволити криптоаналітику отримати яку-небудь інформацію про відкритий текст при перехопленні ним шифротексту (за виключенням хіба що дуже малої ймовірності). Для застосування в криптографічних системах ГПВЧ повинні відповідати наступним вимогам:

1. послідовність, що генерується повинна мати максимально великий період;
2. послідовність, що генерується не повинна мати схованих періодичностей;
3. послідовність, що генерується повинна мати рівномірний спектр.

Найважливішою характеристикою ГПВЧ є довжина періоду повторення, після якого випадкові числа, на виході ГПВЧ почнуть повторюватися. Другою за важливістю характеристикою ГПВЧ є його продуктивність, тобто кількість чисел, які генеруються за одиницю часу. Для окремих прикладних програм (статистичне зондування, моделювання в реальному часі і т.д.) може бути потрібною продуктивністю порядку $10^{10} – 10^{12}$ випадкових чисел за секунду.

Швидкий і надійний ГПВЧ може легко слугувати поточним шифром. Оскільки для шифрування інформації достатньо її побітово скласти по модулю два з випадковою послідовністю бітів. Так наприклад працює поточний шифр A5.

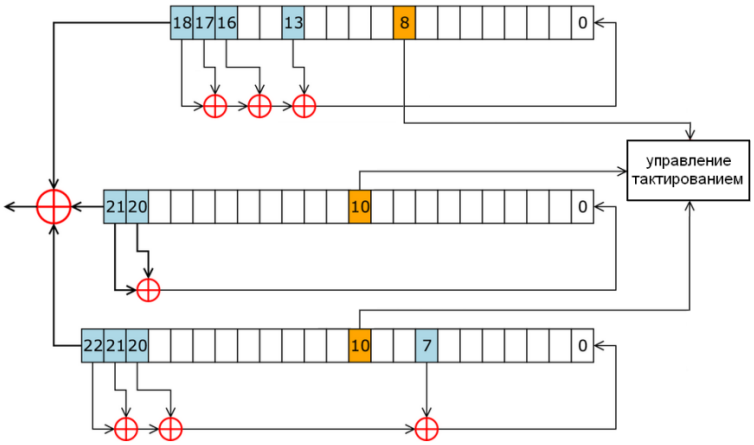

Рис. 1. Схема ГПВЧ в шифрі A5

Питанню проектування надійних і якісних ГПВЧ часто не надають належної уваги. Сама система шифрування може бути виконана на дуже високому рівні, але якщо криптографічний ГПВЧ видає ключі, які легко вгадати, то всі інші бар'єри захисту долаються без особливих зусиль. В ряді продуктів використовуються ГПВЧ, що продукують ключі, в яких відслідковується певна закономірність. В таких випадках про безпеку говорити не варто. Цікавим є те, що використання одного і того ж. генератора в деяких областях забезпечує необхідну степінь захисту, а в інших - ні. Таким чином, необхідно підкреслити важливість криптографічного ГПВЧ – якщо він розроблений погано, то він легко може стати самим вразливим елементом системи.