МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора

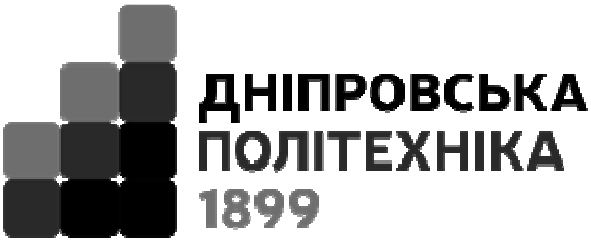
Методичні вказівки до виконання практичних робіт з дисципліни
«Основи забезпечення безпеки інформації»

Дніпро
2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ

Факультет інформаційних технологій

Кафедра безпеки інформації та телекомунікацій

Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора

Методичні вказівки до виконання практичних робіт з дисципліни «Основи забезпечення безпеки інформації»

Дніпро

2020

Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи забезпечення безпеки інформації» для бакалаврів напряму підготовки 12 Інформаційні технології/ Ю.А. Мілінчук, І.А. Сєчкін – Дніпро: НТУ «ДП», 2020. – 9 с.

Автори:

Ю.А. Мілінчук, І.А. Сєчкін

Затверджено методичною комісією за напрямом Кібербезпека (протокол № 2 від. 25.02.2020) за поданням кафедри безпеки інформації та телекомунікацій (протокол № 7 від 25.02.2020).

Відповідальний за випуск зав. кафедри БІТ В.І. Корнієнко, д-р техн. наук, проф.

Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора. Дослідження їх крипостійкості.

Мета: здобуття знань та навичок з генерації випадкових та псевдовипадкових послідовностей (ВП та ПВП), а також визначення можливості їх застосування у криптографічних перетвореннях.

Теоретичні матеріли до підготовки

Однією з основних проблем розробки систем захисту інформації є створення генераторів послідовностей випадкових чисел, рівномірно розподілених в заданому інтервалі. Генерування випадкових послідовностей великої довжини є однією з важливих проблем класичної криптографії. Для вирішення цієї проблеми широко використовуються генератори псевдовипадкових послідовностей (ГПВП).

Генератори псевдовипадкових послідовностей повинні відповідати певним умовам. Послідовності, отримані з їх допомогою, повинні володіти рівномірним розподілом (або, принаймні, близьким до рівномірного). Це означає, що в згенерованої двійковій послідовності кількість нулів має бути приблизно дорівнювати кількості одиниць, що містяться в послідовності. Крім того, випадкові значення, з яких складається згенерована послідовність, повинні бути статистично незалежні. Це означає, що не повинно бути ніяких кореляцій як між окремими бітами, так і між групами бітів.

Генератор псевдовипадкових послідовностей повинен бути ефективним. Це означає, що він повинен робити послідовності великої довжини за максимально короткий час. Така вимога особливо важливо для систем, що працюють в режимі реального часу. Крім того, генератори псевдовипадкових послідовностей, що застосовуються в задачах криптографії, повинні бути стійкі до різних атак і нестандартних ситуацій. Це означає, що у зловмисника не повинно бути можливості вгадати будь-який поточний, попередній або наступний вихід генератора навіть за тієї умови, що йому відома деяка інформація про вхідні дані генератора, про його внутрішній стан, або його поточне, або більш раннє вихідне значення.

На відміну від генераторів істинно випадкових послідовностей, генератор псевдовипадкових послідовностей завжди має певний період в силу кінцевого значення можливих станів обчислювальної системи. Він може бути як завгодно великим, але завжди є кінцевим. Після того, як довжина послідовності перевищила такий період, значення, вироблені генератором, починають повторюватися. Тому, щоб уникати появи явних закономірностей в згенерованої послідовності, необхідно, щоб її період був досить великим.

Псевдовипадкові двійкові послідовності (ПВДП) застосовуються для шифрування даних або повідомлень, так як виключається необхідність передачі ключа одержувачеві. Ключ для їх розшифровки на приймальній стороні будується за допомогою ідентичного генератора ПВДП.

На генерації ПВП засновано шифрування методом гамування. Метод отримав свою назву від грецької букви γ, що використовується в математиці для позначення випадкових величин. Згенеровані псевдовипадкові ряди чисел, які використовуються у якості ключа, зазвичай називають гамою шифру або просто гамою.

Метод гамування полягає в генерації псевдовипадкової послідовності чисел (гами), виробленої за заданим алгоритмом, і її накладення на вихідний текст оборотним чином, наприклад з використанням операції додавання по модулю 2. Процес розшифрування зводиться до повторної генерації гами шифру і накладенню цієї гами на зашифровані дані.

Отриманий таким методом шифротекст досить важко піддається криптоаналізу, так як ключ є змінним. Гама шифру повинна змінюватися випадковим чином для кожного блоку тексту, що піддається шифруванню. Якщо період гами перевищує довжину всього тексту і зловмисникові невідома ніяка частина вихідного тексту, то такий шифр можна зламати тільки прямим перебором всіх варіантів ключа. В цьому випадку крипостійкість шифру визначається довжиною ключа.

Застосовані для генерації псевдовипадкових ПВП комп'ютерні програми, які називаються генераторами , насправді видають детерміновані числові послідовності, які за своїми властивостями схожі на випадкові.

Один з перших способів генерації ПВП на ЕОМ запропонував в 1946р. Джон фон Нейман. Суть цього способу полягає в тому, що кожне наступне випадкове число утворюється зведенням в квадрат попереднього числа з відкиданням цифр молодших і старших розрядів. Однак цей спосіб виявився ненадійним, і від нього незабаром відмовилися.

Розглянемо деякі варіанти способів генерації ПВП.

Лінійний конгруентний генератор.

Формує послідовність цілих чисел згідно з вираженням:

$$x_{i+1}=(a\,x_i+c)\bmod m, \qquad (1)$$

де

- ***a***, ***c*** и ***m*** – цілочисельні коефіцієнти;
- ***a*** - множник; ***c*** – приріст; ***m*** – модуль;

- x_{i+1} – поточне число послідовності;
- x_i – попереднє число послідовності;
- x_0 - породжує число (початкове значення).

Довжина періоду лінійної конгруентної послідовності залежить від вибору коефіцієнтів a, c і m. Довжина періоду дорівнює m тоді, коли

- ***c*** і ***m*** є взаємно простими числами;
- ***a*** – непарне число;
- ***b* = *a*-1** кратно числу ***p*** для будь-якого простого ***p***, що є дільником ***m***;
- ***b*** кратно 4, якщо ***m*** кратно **4.**

Значення модуля ***m*** береться рівним 2^n або рівним простому числу, наприклад $m = 2^{31} - 1$. Коефіцієнт ***c*** може дорівнювати ***0***. У цьому випадку отримаємо мультиплікативний датчик

$$x_{i+1} = a\, x_i \bmod m. \qquad (2)$$

Максимально можливий період при ***c* = *0*** дорівнює $\lambda(m)$, де

$$\lambda(2^e) = 2^{e-2}; \qquad \lambda(p^e) = p^{e-1}(p-1); \qquad (3)$$

Такий період реалізується, якщо:

- x_0 і ***m*** -– взаємно простими числами;
- ***a*** – первісний елемент по модулю m.

Конгруентні генератори, що працюють за алгоритмом, запропонованим Національним бюро стандартів США, використовуються, зокрема, в системах програмування. Ці генератори мають довжину і володіють хорошими статистичними властивостями. Однак така довжина мала для криптографічних застосувань. Крім того, доведено, що послідовності, що генеруються конгруентними генераторами, не є криптографічно стійкими.

Завдання до виконання лабораторної роботи:

1. Згенерувати ПВП лінійним конгруентним генератором *(\\S2\дисциплины\Основы информационной безопасности\Генераторы случайных и псевдослучайных последовательностей\Программное обеспечение\ПО для работы с аппаратными генераторами\LCG.exe)*

2. Провести дослідження властивостей отриманої ПВП за допомогою статистичних тестів:

   – пакету тестів американського стандарту FIPS 140-1 (*\\S2\дисциплины\Основы информационной безопасности\Генераторы случайных и псевдослучайных последовательностей\Программное обеспечение\Стандарт FIPS 140-1\Fips1401RusExplorer\TestFIPS1401eh.exe*);
   – тесту розподілення *(\\S2\дисциплины\Основы информационной безопасности\Генераторы случайных и псевдослучайных последовательностей\Программное обеспечение\Тест распределения\ TEST.exe*);
   – універсального тесту Мауера *(\\S2\дисциплины\Основы информационной безопасности\ Генераторы случайных и псевдослучайных последовательностей\ Программное обеспечение\ Тест Мауера\ TESTMAUE.exe*).

3. За результатами дослідження зробити висновки щодо криптостійкості ПВП.

Звіт повинен містити:

– тема та мета роботи;
– завдання згідно варіанта;
– схема ГПВП;
– лістинг програми реалізації ГПВП з коментаріями;
– результати виконання програми;
– результати проходження тестів представити у графічному вигляді та у числовому вигляді в таблиці(табл. 1);
– висновки з аналізом отриманих результатів.

Таблиця 1 Результати проходження статистичних тестів згенерованої ПВП

Вид тесту	**ПВП1(ЛКГ)**
Стандарт FIPS 140-1:	
– монобітний тест	
– блоковий тест	
– тест серій	
– тест довжин серій	
Універсальний тест Мауера	
Тест розподілення (частотний тест)	

Контрольні запитання:

1. Визначте основну різницю між випадковою та псевдовипадковою послідовностями, галузі їх застосування;
2. У чому полягає метод гамування?
3. Що таке «гамма шифру»?
4. Що собою являє генератор псевдовипадкових послідовностей?
5. Назвіть основні вимоги до генераторів криптографічностійких ПВП, близьких до випадкових;
6. Основні параметри лінійного конгруентного генератора;
7. Галузь застосування лінійного конгруентного генератора;
8. За якими критеріями перевіряють якість ВП та ПВП?
9. Які статистичні характеристики використовуються для оцінки ВП та ПВП?
10. Які розподілення величин використовують для дослідження ВП та ПВП?
11. Що визначає рівень значимості та довірчий інтервал? Як вони впливають на появу похибки першого та другого роду?
12. У чому полягає перевірка послідовностей за допомогою: пакету тестів американського федерального стандарту FIPS 140-1, тесту розподілення, універсального тесту Мауера?

Література:

1. Фергюссон Н., Шнайер Б. Практическая криптография. –М.: Изд. дом «Вильямс», 2005. –424 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: Триумф, 2002. –816 с.
3. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. –768 с.
4. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. М.: Издательство: АНО НПО "Профессионал", 2005. –480 с.
5. Иванов М.А., Скитев А.А., Стариковский А.В. Классификация генераторов псевдослучайных чисел, ориентированных на решение задач защиты информации // REDS: Телекоммуникационные устройства и системы. –2017. –Т. 7. –No 4. –С.484–487.
6. Коренева А.М., Фомичев В.М. Статистическое тестирование псевдослучайных последовательностей // Безопасность информационных технологий. –2016. –No 2. –С. 36–42.

Мілінчук Юлія Анатоліївна

Сєчкін Ігор Арнольдович

Генерація псевдовипадкових послідовностей за допомогою лінійного конгруентного генератора.

Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи забезпечення безпеки інформації»

Видано в редакції авторів

Комп'ютерний дизайн, верстка та обробка – Ю.А.Мілінчук

Підписано до друку 16.03.2020. Формат 30х42/4.
Папір офсет. Ризографія. Ум. друк. арк. 0,5.
Обл.-вид. арк. 0,5. Тираж 5 пр. Зам. №

Національний технічний університет «Дніпровська політехніка»
49005, м. Дніпро, просп. Д. Яворницького, 19.