УДК 681.324.067

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

І.Д. ГОРБЕНКО, Р.І. МОРДВІНОВ

На сучасному етапі розвитку інформаційних технологій актуальними є проблеми захисту інформації. Захисту інформації, що зберігається в електронному вигляді, реалізується криптографічними методами. Для функціонування цих методів необхідно виконувати управління ключовими даними, а саме генерування ключів та параметрів.

Ключові слова: випадкова послідовність, генератор випадкових послідовностей, псевдовипадкова послідовність, детермінований генератор випадкової послідовності.

ВСТУП

На сучасному етапі розвитку інформаційних технологій актуальними є питання захисту інформації. Основними методами захисту такої інформації є криптографічні методи. Однією з умов для функціонування криптографічних систем є управління ключовими даними, а саме генерація ключових даних і параметрів. Для цього необхідно використовувати генератори випадкових / псевдовипадкових послідовностей.

1. ДЕТЕРМІНОВАНІ ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ БІТ НА ОСНОВІ ГЕШ-ФУНКЦІЙ

Ідея побудови генератора псевдовипадкових біт (ГПВБ) на основі геш-функцій лежить у використанні необоротних геш-функцій, за допомогою яких на основі початкового значення виробляються псевдовипадкові біти (ПВБ). Дані ГПВБ можуть використовувати будь-які криптографічні геш-функції, відповідні ISO / IEC 10118-3, і можуть використовуватися в додатках, які вимагають різні рівень захисту, але за умови використання відповідної геш-функції та отримання достатньої ентропії для початкового значення.

До ГПВБ на основі геш-функцій висуваються наступні вимоги:

1. Вихідні дані для геш-функцій повинні бути випадковими і різними для різних вхідних даних.

2. Початкове значення повинне мати необхідну ентропію.

ГПВБ на основі геш-функцій може проектуватися для забезпечення різних рівнів захисту в залежності від геш-функції, яка використовується. Стійкість геш-функції в даних ГПВБ дорівнює розміру вихідного блоку. При цьому необхідно зазначити, що якщо геш-функція використовується як елемент криптографічного послуги, де необхідно враховувати стійкість до колізій, то стійкість вихідних даних геш-функції оцінюється половиною розміру вихідного блоку завдяки «парадоксу дня народження».

Довжина початкового значення має бути максимально наближеною до розміру блоку гешированних даних та рівнем стійкості захисту.

ГПВБ на основі геш-функцій вимагає використання геш-функцій кілька разів, включаючи процес ініціалізації і переініціалізації. На всьому життєвому циклі генератора повинна використовуватися одна і та ж геш-функція, яка повинна відповідати бажаної стійкості захисту криптографічного програми.

Перед початком роботи ГПВБ необхідно встановити в початковий стан. Для отримання початкового значення використовуються вхідні дані ентропії.

Початкове значення використовується для отримання елементів початкового стану, що складається з:

1. Значення (V), яке оновлюється при кожному виклику ГПВБ;

2. Константи (C), яка залежить від початкового значення;

3. Лічильник, який вказує число запитів ПВБ з моменту отримання нового значення ентропії;

4. Стійкість захисту реалізації ГПВБ;

5. Довжини початкового значення;

6. Показника, який вказує на необхідність забезпечення прямої секретності ГПВБ;

7. (За бажанням) Перетворення вхідних даних ентропії з використанням односторонньої функції для подальшого порівняння з новими вхідними даними ентропії під час переініціалізації ГПВБ. Це значення необхідно для переініціалізації ГПВБ.

2. ДЕТЕРМІНОВАНІ ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ БІТ НА ОСНОВІ ФУНКЦІЙ БЛОЧНОГО ШИФРУВАННЯ

ГПВБ на основі блочного шифрування можуть використовувати будь-які алгоритми блокового шифрування, які описані в стандарті ISO / IEC 18033-3, а також можуть використовуватися в криптографічних додатках, в яких використовуються різні рівні захисту.

Для всіх операцій блочного шифрування повинні використовуватися одні й ті ж алгоритми блокового шифрування і довжина ключа.

Алгоритм блокового шифрування та розмір ключа повинні відповідати вимогам захисту програми.

Ініціалізація і переініціалізація ГПВБ на основі блочного шифрування повинна складатися з отримання початкового значення з необхідною кількістю ентропії. Вхідні дані ентропії використовуються для формування початкового значення, яке потім використовується для отримання елементів початкового стану ГПВБ. Початковий стан складається з:

1. Значення (V), яке оновлюється до кожним формуванням вихідного значення ПВБ;

2. Ключа, який оновлюється кожного разу, коли генерується задане число вихідних блоків;

3. Довжини ключа, які використовуються алгоритмом блокового шифрування;

4. Стійкість захисту ГПВБ;

5. Лічильник, який визначає число запитів, необхідних для генерації ПВБ з моменту ініціалізації або переініціалізціі;

6. Показника, що вказує на необхідність забезпечення ГПВБ стійкості до прогнозування.

В якості функції шифрування використовується функція Block_cipher (Key, data), де Key – ключ, data – дані, які шифруються. В якості алгоритмів шифрування використовуються такі алгоритми: AES, ГОСТ-28147-89, DES, TDES.

AES – Advanced encryption standart – міжнародний стандарт, прийнятий державним стандартом США. Може використовуватися з довжинами блоку та ключа 128, 192, 256 біт.

ГОСТ 28147-89 – державний стандарт Росії. Використовує Фейстел-подібну систему. Розмір блоку дорівнює 64 біта, розмір ключа – 256 біт.

DES – був державним стандартом США до прийняття AES. Використовує Фейстел-подібну систему шифрування. Розмір блоку 64 біта, розмір ключа – 64 біта (56 біт ключа і 8 біт перевірки).

TDES - модифікація шифру DES. Являє собою скомпоновані 3 шифру DES. Як шифрування може використовуватися шифрування, розшифрування і зашифрування з використанням різних ключів. Розшифрування відбувається в зворотному порядку. Розмір блоку і ключів відповідає стандартному DES.

3. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

У табл. 1 наведено оцінку складності формування ПВБ з використанням даний ГПВБ в загальному вигляді через математичні операції. При цьому необхідно виділити 2 етапи щодо генерації ПВБ – підготовчий етап і безпосередньо етап генерації.

Для тестування даних ГПВБ використовувалася методика тестування NIST STS.

Для тестування було обрано такі параметри:

1. Довжина послідовності, яка тестується $n = 106$ біт;

2. Кількість послідовностей для тестування $m = 100$;

3. Рівень значущості $\alpha = 0{,}01$;

4. Кількість тестів $q = 189$.

Таким чином розмір вибірки для тестування дорівнює 108 біт, а статистичний портрет генератора має 18900 значень ймовірності P.

В ідеальному випадку при $m = 100$ і $\alpha = 0{,}01$ може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту дорівнює 99%. Однак це занадто жорстке правило. Тому використовується правило на основі довіреної інтервалу. При цьому нижня межа дорівнює 0,96015. Результати тестування наведені в табл. 2.

Таблиця 1

Оцінка складності ГПВБ

	ГПВБ на основі геш-функцій	ГПВБ на основі функцій шифрування
Додавання	1 + Cycles	0
Додавання за модулем 2	0	2
Додавання за модулем	2	2 + Cycles
Конкатенація	5 + Cycles	2 + Cycles
Геш-функція	3 + Cycles	0
Функція шифрування	0	2 + Cycles

* cycles – відношення кількості біт, заданих для генерації до довжини вихідного блоку шифру або геш-функції.

Таблиця 2

Результати тестування послідовностей

Генератор	Кількість тестів, які успішно пройдені при рівні $\alpha = 0{,}99$	Кількість тестів, які успішно пройдені при рівні $\alpha = 0{,}96015$	Швидкість (Мбіт/с)
BBS	134 (71%)	189 (100%)	
SHA1	132 (69%)	188 (99%)	21
SHA2 256	130 (68%)	187 (98%)	15,3
SHA2 384	133 (70%)	189 (100%)	15,8
SHA2 512	141 (74%)	189 (100%)	16,7
AES	138 (73%)	189 (100%)	21,4
DES	132 (69%)	188 (99%)	19,5
ГОСТ 28-147	132 (69%)	188 (99%)	16,2
TDES	135 (71%)	189 (100%)	16,1

В результаті аналізу отриманих даних були зроблені наступні висновки: генератори на основі SHA2-512, AES і TDES мають кращі результати по NIST STS, які вище результатів BBS. Серед цих генераторів кращу швидкість показав генератор на AES (дослідження проводилися на Intel Celeron 2.8GHz). Таким чином кращим серед цих генераторів є генератор на блочному шифрі AES.

Література

[1] ISO/IEC 18031:2005 Information technology — Security techniques — Random bit generation.

Надійшла до редколегії 16.04.2012

Горбенко Іван Дмитрович – д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, головний конструктор АТ «Інститут інформаційних технологій». Область наукових інтересів: криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Мордвінов Руслан Ігоревич – аспірант кафедри БІТ Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

УДК 681.324.067

Сравнительный анализ алгоритмов генерации псевдослучайных последовательностей / И.Д. Горбенко, Р.И. Мордвинов / Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 188–190.

На современном этапе развития информационных технологий актуальными являются проблемы защиты информации. Защита информации, которая хранится в электронном виде, реализуются криптографическими методами. Для функционирования таких методов необходимо использовать управление ключевыми данными, а именно генерация ключей и параметров.

Ключевые слова: случайная последовательность, генератор случайных последовательностей, псевдослучайная последовательность, генератор псевдослучайной последовательности.

Табл. 2. Библиогр.: 1 назв.

UDC 681.324.067

Comparative analysis of pseudorandom sequence generation algorithms / I.D. Gorbenko, R.I. Mordvinov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 188–190.

At the present-day stage of IT progress information security becomes increasingly important. The main methods of information security are cryptographic methods. To function such methods require using key data management, namely, generation of keys and parameters.

Keywords: random sequence, random sequence generator, pseudorandom sequence, pseudorandom sequence generator.

Tab. 2. Ref.: 1 items