УДК 004.4'277.2.056.55

І. Л. Медяна[1]
Р. С. Белзецький [1]

ОБГРУНТУВАННЯ ВИБОРУ ГЕНЕРАТОРА ПСЕВДО ВИПАДКОВИХ ВЕЛИЧИН ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ АУДІО ПОВІДОМЛЕННЯ

[1] Вінницький національний технічний університет.

Анотація

Наведена класифікація та, сформовані три основні вимоги яким повинен відповідати генератор псевдовипадкових величин, проаналізовані різні алгоритми та обгрунтовано доцільність вибору алгоритмічного генератора псевдо випадкових величин.

Ключові слова: псевдовипадкова послідовність, генератор випадкових величин, потокове шифрування, аудіо повідомлення.

Abstract

The classification and three basic requirements that the pseudorandom generator must meet, the various algorithms are analyzed, and the feasibility of choosing an algorithmic pseudorandom generator is substantiated.

Keywords: pseudorandom sequence, random variable generator, streaming encryption, audio messaging.

Вступ

Псевдовипадкове число – це число, отримане детермінованим алгоритмом, що використовується в якості випадкового числа.

Генератори псевдовипадкових величин використовуються дуже широко в сотнях різновидів програмних додатків - від конструювання ядерних реакторів і радіолокаційних систем раннього виявлення до пошуків нафти і до багатоканального зв'язку.

Найважливіша характеристика генератора псевдовипадкових чисел - це інформаційна довжина його періоду, після якого числа будуть або просто повторюватися, або їх можна буде передбачити. Ця довжина практично визначає можливе число ключів криптосистеми. Чим ця довжина більше, тим складніше підібрати ключ.

Основний зміст

. Генератори випадкових величин за способом отримання випадкових значень діляться на [1]:

- апаратні;
- табличні;
- алгоритмічні.

Табличні генератори в якості джерела випадкових величин використовують заздалегідь підготовлені таблиці, що містять перевірені не корельовані числа і не є генераторами в загальному розумінні цього поняття.

Недоліками такого способу є: використання ресурсу з зовні для зберігання чисел, обмеженість послідовності, зумовленість значень.

Апаратні генератори випадкових послідовностей повинні володіти джерелом ентропії. Розробка генераторів, що використовують джерела ентропії, генерування не корельованих і статистично незалежних значень - досить складне завдання. Крім того, для більшості криптографічних додатків такий генератор псевдо випадкових чисел не повинен бути предметом вивчення, так-як вимагає застосування додаткових схемо-технічних рішень.

Алгоритмічний генератор є комбінацією фізичного генератора і детермінованого алгоритму. Такий генератор використовує обмежений набір даних, отриманий з виходу фізичного генератора для

створення довгої послідовності чисел перетвореннями вихідних чисел. Даний тип генераторів викликає найбільший інтерес в силу його очевидних переваг над генераторами випадкових чисел інших видів.

Більшість потокових шифрів працює на основі генерації псевдовипадкового потоку біт, які певним чином комбінуються з бітами відкритого тексту. Запуск такого шифру на послідовності натуральних чисел дасть нову псевдовипадкову послідовність, можливо навіть з більш довгим періодом. Такий метод безпечний тільки якщо в самому потоковому шифрі використовується надійний криптографічно стійкий генератор псевдовипадкової величини (що не завжди так). Часто для створення потокових чисел використовується регістр зсуву з зворотним зв'язком, що автоматично робить такий шифр криптографічно нестійким. Знову ж, початковий стан лічильника повинен залишатися секретним.

Враховуючи вище сказане можна сформувати три основних загальних вимоги, яким повинні задовольняти крипто графічно стійкі генератори псевдовипадкових послідовностей і одержувані з їх допомогою гами:

1. Період гами повинен бути досить великим для шифрування повідомлень різної довжини.

2. Гамма повинна бути важко передбачуваною. Це означає, що якщо відомі тип генератора і відрізок гами, то неможливо передбачити наступний за цим відрізком біт гами.

3. Генерування гами не повинно бути пов'язане з великими технічними і організаційними труднощами.

Друге із зазначених вище вимог пов'язане з наступною проблемою: на підставі чого можна зробити висновок, що гамма конкретного генератора дійсно є непередбачуваною. Щоб гамма вважалася випадковою і непередбачуваною, як мінімум, необхідно, щоб її період був дуже великим, а різні комбінації біт певної довжини рівномірно розподілялися по всій її довжині. Цю вимогу статистично можна тлумачити і як складність закону генерації псевдовипадкової послідовності чисел. Якщо по досить довгому відрізку цієї послідовності не можна ні статистично, ні аналітично визначити цей закон генерації, то в принципі цим можна задовільнитись.

І, нарешті, третя вимога повинна гарантувати можливість практичної реалізації генераторів псевдовипадкових послідовностей з урахуванням необхідної швидкодії і зручності практичного використання.

Алгоритм RC4 розроблений компанією RSA Data Security. Будучи потоковим шифром, в основі якого генератор псевдовипадкових чисел, RC4 широко використовується в різних криптографічних протоколах. Перевагою алгоритму є висока швидкість роботи і змінний розмір ключа [2].

Алгоритми генератора псевдовипадкових величин на основі складних математичних задач використовують складність вирішення деяких завдань для отримання псевдовипадкових чисел захищених від крипто аналізу . Іншими словами, людина, що створює ГПВВ, намагається використовувати теорію складності так, щоб рішення задачі криптоаналізу було б еквівалентно рішенню важкої теоретичної задачі [3]. Також для генерації псевдо випадкової послідовності використовується алгоритм шифрування з відкритим ключем RSA. Його перевагою є той факт, що передбачення значення генератора псевдовипадкових чисел рівносильне злому RSA. Очевидним недоліком такого алгоритму є низька швидкість і громіздкість реалізації.

Алгоритм Блюм—Блюм—Шуба (BBS). В основу алгоритму покладено використання квадратичних залишків по модулю n. На даний час це один з найпростіших і швидких алгоритмів ГПВВ, що використовують обчислювально складні завдання [4].

Висновок

Проведено аналіз існуючих методів та засобів генерації псевдовипадкових величин для потокового шифрування аудіо повідомлення та обґрунтовано доцільність вибору алгоритмічного генератора псевдо випадкової величини, так як він простий з точки зору реалізації в програмному коді. Найбільш доречним представником алгоритмічних генераторів псевдо випадкової послідовності є алгоритм BBS. Цей алгоритм має високу стійкість, яка забезпечується якістю генератора виходячи з обчислювальної складності завдання факторизації чисел.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Слеповичев И. И. Генераторы псевдослучайных чисел / И. И. Слеповичев., 2017. – 113 с.
2. Алгоритм RC4: [Електронний ресурс]. — Режим доступу: https:// http://solutionmes.wikidot.com/crypto-rc4 — (07.04. 2018).
3. Генератор_псевдовипадкових_чисел: [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/ Генератор_псевдовипадкових_чисел — (22.03.2018)
4. Алгоритм_Блум_-_Блум_-_Шуба [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/ /Алгоритм_Блум_-_Блум_-_Шуба — (09.04. 2018)

Медяна Ірина Леонідівна – студентка факультету менеджменту та інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail:fm.ub16.mediana@gmail.com;

Белзецький Руслан Станіславович – канд. техн. наук, доцент кафедри Інтеграції навчання з виробництвом, Вінницький національний технічний університет, м. Вінниця, e-mail:belzetskiyruslan@gmail.com;

Mediana Irina L. - student at the Faculty of Management and Information Technology, Vinnytsia national technical university, Vinnitsa;

Belzetskyi Ruslan S. – Ph. D., Assistant Professor of the Chair of Integration Education with Production, Vinnytsia National Technical University, Vinnytsia, e-mail: belzetskiyruslan@gmail.com.