МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ, ИНФОРМАЦИОННЫХ
И АВИАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕОРИИ
УПРАВЛЕНИЯ

Рацеев С.М.

Методические указания для самостоятельной работы студентов по дисциплине «Теория псевдослучайных генераторов»

для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2019

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Теория псевдослучайных генераторов» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2019.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 2/19 от 19 марта 2019 г.).

Тема 1. Генераторы на основе регистра сдвига с линейной обратной связью

Основные вопросы темы:

Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ. Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом. Инверсный конгруэнтный генератор. Теорема о максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэтных генераторов. Квадратичный, кубический и полиномиальный конгруэнтные генераторы. Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС. Частные случаи РСЛОС. Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП. Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.

Рекомендации по изучению темы:

Все вопросы изложены на страницах 6–15 учебного пособия [1].

Контрольные вопросы:

1. Формула линейного конгруэнтного метода. 2. Регистр сдвига с линейной обратной связью. 3. Примитивные многочлены. 4. Условие максимальности периода последовательности на основе РСЛОС. 5. Схема работы РСЛОСП. 6. Максимальный период последовательности генератора РСЛОСП. 7. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием. 8. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.

Задачи для самостоятельной работы:

1. Определить, будет ли максимальным период последовательности линейного конгруэтного генератора при $a = 5$, $b = 2$, $n = 6$.

2. Построить регистр сдвига с линейной обратной связью с ассоции-

рованным многочленом $x^3 + x + 1$ и выписать состояние регистра, если он был инициализирован вектором (111).

Тема 2. Алгоритм Берлекэмпа-Месси.

Основные вопросы темы:

Алгоритм Берлекэмпа-Месси над любым полем. Алгоритм Берлекэмпа-Месси над двоич-ным полем. Алгоритм Берлекэмпа-Месси с минимальным числом вычислений обратных элементов. Обобщенный алгоритм Евклида. Взаимосвязь алгоритма Берлекэмпа-Месси и обобщенного алгоритма Евклида. Криптоанализ последовательности, выработанной с помощью регистра сдвига с линейной обратной связью, на основе алгоритма Берлекэмпа-Месси.

Рекомендации по изучению темы:

Все вопросы изложены в главе 4 учебного пособия [2].

Контрольные вопросы:

1. Алгоритм Берлекэмпа-Месси над любым полем. 2. Алгоритм Берлекэмпа-Месси над полем характеристики два. 3. Алгоритм Берлекэмпа-Месси с минимальным числом вычислений обратных элементов. 4. Обобщенный алгоритм Евклида. 5. Взаимосвязь алгоритма Берлекэмпа-Месси и обобщенного алгоритма Евклида. 6. Криптоанализ последовательности, выработанной с помощью регистра сдвига с линейной обратной связью, на основе алгоритма Берлекэмпа-Месси.

Задачи для самостоятельной работы:

1. С помощью алгоритма Берлекэмпа-Месси решить систему линейных алгебраических уравнений

$$\begin{pmatrix} 3 & 1 & 2 \\ 5 & 3 & 1 \\ 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} -5 \\ -4 \\ -6 \end{pmatrix}$$

над полем $GF(7)$.

2. Решить систему из предыдущего примера на основе обобщенного алгоритма Евклида.

3. Построить LFSR минимальной длины, который вырабатывает последовательность $0, 1, 0, 2, 1, 2, 2, 2, 1, 0, 0, 2$ над полем $GF(3)$.

Тема 3. Генераторы на основе симметричных блочных шифров.

Основные вопросы темы:

Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспе-чивающие обратимость шифра Фейстеля. Режимы

использования блочных шифров. Ре-жим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с об-ратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов. Примеры итеративных блочных шифров. Шифры "Магма" и "Кузнечик" из ГОСТ Р 34.12-2015. Шифр AES. Генераторы на основе симметричных блочных шифров.

Рекомендации по изучению темы:

Все вопросы изложены в главе 8 учебного пособия [2].

Контрольные вопросы:

1. Итеративные блочные шифры. Обратимость итеративного блочного шифра. 2. Шифры Фейстеля и их обратимость. 3. Построение раундовой функции. Входное и выходное отображения. 4. Режимы использования симметричных блочных шифров. 5. Шифр Магма из ГОСТ Р 34.12-2015. 6. Генераторы на основе симметричных блочных шифров.

Задачи для самостоятельной работы:

Построить генератор на основе блочного шифра Магма в режиме OFB.

Тема 4. Генераторы на основе хеш-функций и асимметричных блочных шифров.

Основные вопросы темы:

Система Диффи-Хеллмана. Криптосистема без передачи ключа (шифр Шамира). Описа-ние системы. Надежность системы. Шифр Эль-Гамаля. Ограничения на параметры систе-мы. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей. Построение хеш-функций. Ге-нераторы на основе асимметричных блочных шифров. Генераторы на основе хеш-функций. Алгоритм Блюма-Блюма-Шуба.

Рекомендации по изучению темы:

Все вопросы изложены в главах 9, 10 учебного пособия [2].

Контрольные вопросы:

1. Криптосистема Месси-Омуры. Вероятностный шифр Эль-Гамаля. 2. Шифр RSA. Рюкзачные криптосистемы, система Меркла-Хеллмана. 3. Криптографические хеш-функции. Способы построения криптографических хеш-функций. 4. Алгоритм Блюма-Блюма-Шуба.

Задачи для самостоятельной работы:

1. Шифр Месси-Омуры. Пусть a_1, a_2 — пара секретных ключей абонента A, b_1, b_2 — пара секретных ключей абонента B, p — простое число, m — передаваемое сообщение от A к B. Известно, что $p = 17$, $a_1 = 3$, $b_1 = 5$, $m = 6$. Найти a_2, b_2, m_1, m_2, m_3, m_4.

2. Шифр Эль-Гамаля. Пусть x, y — соответственно секретный и открытый ключи абонента A, p — простое число, g — первообразный корень по модулю p (параметры шифрсистемы), m — передаваемое сообщение абоненту A, k — случайное число. Известно, что $p = 13$, $g = 2$, $x = 5$, $k = 3$, $m = 10$. Найти y и шифрованное сообщение (c_1, c_2), передаваемое абоненту A.

3. Шифр RSA. Пусть e, d — соответственно секретный и открытый ключи абонента A, p, q — простые числа абонента A, m — передаваемое сообщение абоненту A. Известно, что $p = 5$, $q = 11$, $e = 3$, $m = 8$. Найти d и шифрованное сообщение y, передаваемое абоненту A.

4. Построить 10-битную псевдослучайную последовательность с помощью RSA-генератора при $p = 17$, $q = 11$.

5. Построить 10-битную псевдослучайную последовательность с помощью генератора Блюма-Блюма-Шуба при $p = 7$, $q = 23$.

Литература

[1] Краснов М.В. Математические методы защиты информации. Ч. 3 : методические указания. Яросл. гос. ун-т им. П. Г. Демидова. Ярославль : ЯрГУ, 2013.

[2] Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.

[3] Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.