МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра теории вероятностей и математической статистики

РЕШЕНИЕ НЕКОТОРЫХ ЗАДАЧ КРИПТОГРАФИИ С ПОМОЩЬЮ СИСТЕМЫ MATHEMATICA

Утверждено редакционно-издательским советом университета в качестве методических рекомендаций

Самара
Издательство «Самарский университет»
2012

УДК 511
ББК 2213

Рецензент канд. физ.-мат. наук, доцент Л. П. Усольцев

Решение некоторых задач криптографии с помощью системы MATHEMATICA: методические рекомендации / сост. Е. М. Кнутова, С. Я. Шатских. – Самара : Изд-во «Самарский университет», 2012. – 20 с.

Методические рекомендации предназначены для первоначального знакомства с математическими задачами криптографии, которые решаются с помощью системы «MATHEMATICA».

Необходимые факты из элементарной теории чисел, а также информация об использованных командах системы «MATHEMATICA» приведены в Приложении.

УДК 511
ББК 2213

Введение

Настоящее пособие предназначено для первоначального знакомства с математическими задачами криптографии, которые мы решаем с помощью системы MATHEMATICA.

Необходимые факты из элементарной теории чисел, а также информация об использованных командах системы MATHEMATICA приведены в Приложении.

Глава 1. Система шифрования RSA

Система шифрования RSA была разработана Р. Ривестом, А. Шамиром и Л. Адельманом в 1978 году (см. [1]).

В основе системы RSA лежат следующие алгоритмы шифрования и расшифрования.

1. Выбираем два простых числа: p и q.
2. Вычисляем их произведение $n = p \cdot q$.
3. Вычисляем произведение $m = (p-1)(q-1)$.
4. Выбираем натуральное число e взаимно простое с m и такое, что $2 \leq e < m$.
5. Вычисляем[1] натуральное число $d < m$ такое, что $e \cdot d \equiv 1 (mod\, m)$.
6. Пара $\{e, n\}$ - это *открытый* ключ, а пара $\{d, n\}$ - *секретный* ключ.
7. Буквы открытого сообщения преобразуются[2] в числа. Числовое представление сообщения разбивается на блоки, каждый из которых является некоторым числом $b \in \mathbb{Z}_n$. Итак, *открытый* текст - это конечная последовательность чисел $b_1, b_2, \ldots, b_r$.
8. *Алгоритм шифрования* чисел b_i: зная $\{e, n, b_i\}$, вычисляем

$$c_i \equiv b_i^e \, (mod\, n), \; c_i \in \mathbb{Z}_n.$$

Итак, *шифротекст* - это последовательность чисел $c_1, c_2, \ldots, c_r$.

[1] Такое число d обязательно найдется во множестве $\mathbb{Z}_m$ и притом только одно (см. Приложение).

[2] Например, каждой букве ставится в соответствие её номер в алфавите, начиная с нуля:

$$а \mapsto 0, \; б \mapsto 1, \; в \mapsto 2, \; \ldots, \; я \mapsto 32.$$

9. *Алгоритм расшифрования* чисел c_i: зная $\{d, n, c_i\}$, вычисляем

$$b_i \equiv c_i^d \,(mod\, n),\ b_i \in \mathbb{Z}_n.$$

Замечание. В дальнейшем, для простоты изложения, будем считать, что открытый текст, также как и шифротекст, состоит из одного блока.

Шифрование и расшифрование с помощью системы MATHEMATICA

Пример 1.1. *Провести шифрование в системе RSA при следующих значениях параметров:* $p = 7$, $q = 11$.

Решение. По условию $n = p \cdot q = 77$, а $m = 60$. Выберем открытый ключ $e = 37$, для которого выполняется условие взаимной простоты $(37, 60) = 1$. С помощью команды **5** (см. Приложение) вычисляем секретный ключ

PowerMod[37,-1,60]=13.

Таким образом,

$$d = 37^{-1} (mod 60) = 13.$$

Выберем открытый текст $b = 2$. С помощью команды **6** (см. Приложение) вычислим шифротекст на основе открытого ключа

PowerMod[2,37,77]=51,

т.е.

$$c = 2^{37}\,(mod\ 77) = 51.$$

Аналогичным образом происходит процесс расшифрования с помощью секретного ключа

PowerMod[51,13,77]=2,

или

$$b = 51^{13}\ (mod\ 77) = 2.\ \square$$

Пример 1.2. *Провести шифрование в системе RSA при следующих значениях параметров:* $p = 7703$, $q = 7919$.

Решение. С помощью команды разложения на простые множители **3** (см. Приложение) убедимся в простоте чисел $p = 7703$ и $q = 7919$:

FactorInteger[7703] $= \{\{7703, 1\}\}$, **FactorInteger[7919]** $= \{\{7919, 1\}\}$.

По условию

$$n = p \cdot q = 61000057, \quad m = (p-1)(q-1) = 60984436.$$

Выбран открытый ключ $e = 5743$. Используя команду **1** (см. Приложение) нетрудно убедиться во взаимной простоте чисел e и m:

$$\mathbf{GCD[5743,60984436]} = 1,$$

т.е.

$$(e, m) = (5743, 60984436) = 1.$$

Вычислим секретный ключ

$$\mathbf{PowerMod[5743,-1,60984436]=35753891}.$$

Таким образом,

$$d = 5743^{-1} (mod\ 60984436) = 35753891.$$

Выбран открытый текст $b = 1234567$. С помощью команды **6** (см. Приложение) вычислим шифротекст на основе открытого ключа

$$\mathbf{PowerMod[1234567,5743,61000057]}=53455492,$$

т.е.

$$c = 1234567^{5743} \, (mod\ 61000057) = 53455492.$$

Произведем процесс расшифрования с помощью секретного ключа

$$\mathbf{PowerMod[53455492,35753891,61000057]}=1234567,$$

или

$$b = 53455492^{35753891} \, (mod\ 61000057) = 1234567. \square$$

Вскрытие шифра RSA

Задача RSA. *Известны: модуль n, открытый ключ e и шифротекст c. Требуется восстановить открытый текст, т.е. найти такое число b, что*

$$c \equiv b^e \, (mod\, n).$$

Решение. Применяя алгоритм факторизации, разложим модуль n на простые множители:

$$n = p \cdot q.$$

Знание чисел p и q позволяет найти число $m = (p-1)\cdot(q-1)$. Далее находим секретный ключ d как элемент обратный e :

$$d \equiv e^{-1} \,(mod\, m).$$

Теперь, зная секретный ключ d, можно восстановить открытый текст

$$b = c^d \,(mod\, n).\square$$

Пример 1.3. *(Задача RSA.) Известны следующие параметры системы RSA:*

$$\textit{модуль}\quad n = 10471957439, \quad \textit{открытый ключ}\quad e = 10471753,$$

а также шифротекст $c = 7820151105$. *Требуется восстановить открытый текст, т.е. найти число* b *такое, что*

$$c \equiv b^e \,(mod\, n).$$

Решение. С помощью команды факторизации 3 (см. Приложение) разложим модуль $n = 10471957439$ на простые множители

$$\mathbf{FactorInteger[10471957439]} \longmapsto 104729^1 \cdot 99991^1, \quad p = 104729, \quad q = 99991.$$

Отсюда $m = (p-1)\cdot(q-1) = 104728 \cdot 99990 = 10471752720;$

$$(m, e) = (10471752720, 10471753) =$$

$$= \mathbf{GCD[10471752720,10471753]} = 1;$$

$$d = e^{-1} \,(mod\, m) = 10471753^{-1} \,(mod\, 10471752720) =$$

$$= \mathbf{PowerMod[10471753,-1,10471752720]} = 9835967737;$$

$$b = c^d \,(mod\, n) =$$

$$= \mathbf{PowerMod[7820151105,9835967737,10471957439]} =$$

$$= 471957439.$$

Проверка шифрованием

$$b^e \,(mod\, n) = \mathbf{PowerMod[471957439,10471753,10471957439]} =$$

$$= 7820151105 = c.\square$$

Сложность вскрытия шифра RSA

Рассмотренное выше решение задачи RSA основано на решении трех задач: 1) задачи факторизации модуля n на простые множители, 2) задачи вычислении элемента обратного e по модулю m, 3) задачи возведении натуральных чисел в степень по модулю n.

Теорема 1.1. *С вычислительной точки зрения задача RSA не сложнее алгоритма факторизации натуральных чисел на простые множители.*

Набросок доказательства. Будем использовать приведенное выше решение задачи RSA. Применяя алгоритм факторизации, разложим модуль n на простые множители:

$$n = p \cdot q. \tag{1.1}$$

Затем, найдем число $m = (p-1) \cdot (q-1)$. Далее, решая сравнение

$$ex \equiv 1 \,(mod\, m) \tag{1.2}$$

с помощью алгоритма Евклида, найдем секретный ключ $d = x$. Теперь, зная секретный ключ d, можно восстановить открытый текст

$$b = c^d \,(mod\, n). \tag{1.3}$$

Заметим, что возведение в степень по модулю может быть выполнено методом повторного возведения в квадрат (см. [4], стр. 26). Для завершения доказательства осталось заметить (см. [3], стр. 191; [4], стр. 103, [5], стр. 89), что с вычислительной точки зрения решение задачи факторизации (1.1), существенно сложнее решения задач (1.2) и (1.3).□

Замечания. Приведем две цитаты из книги [3] (см. стр. 191 и 193).

"Существует гипотеза, подтвержденная некоторыми косвенными соображениями, что задача RSA на самом деле легче проблемы факторизации. В настоящее время проверка этой гипотезы является одним из главных открытых вопросов криптологии".

"Если проблема факторизации модуля системы окажется легкой, RSA будет взламываться. Самые большие числа, которые в настоящее время удается разложить на множители за разумное время, имеют 500 двоичных знаков. В связи с этим, для обеспечения стойкости систем среднего срока действия, рекомендуется брать модули шифрования порядка 1024 битов. Для систем большего срока действия следует выбирать модули, состоящие из 2048 битов".

Полезную информацию, относящуюся к обсуждаемой теме, можно найти в книге [2] на стр. 532-533.

Выберем натуральное число m (*модуль*) и три целых числа:

$$\textit{начальное значение } x_0 \in \mathbb{Z}_m \equiv \{0, 1, \ldots, m-1\};$$
$$\textit{множитель } a \in \mathbb{Z}_m; \quad \textit{приращение } c \in \mathbb{Z}_m.$$

Определение. *Последовательность целых чисел, получаемая с помощью соотношения*

$$x_{n+1} = ax_n + c \,(mod\, m), \quad n = 0, 1, 2, \ldots, \tag{2.1}$$

называется линейной конгруэнтной последовательностью (ЛКП). Само соотношение (2.1) называют линейным конгруэнтным генератором (ЛКГ).

Нетрудно видеть, что такая ЛКП периодична и её период не превышает m. Действительно, ввиду того, что для любого натурального n

$$x_n \in \mathbb{Z}_m,$$

то среди первых $m+1$ членов этой последовательности обязательно найдутся по крайней мере два одинаковых, а это, ввиду равенства (2.1), влечет за собой периодичность ЛКП с периодом не превышающим m.

Поскольку длинный период необходим для псевдослучайных последовательностей, которые в криптографии используются в качестве случайных, то представляет интерес подбор параметров $\{a, c, m\}$, при котором период ЛКП достигает максимального значения равного модулю m.

Теорема 2.1. *Линейная конгруэнтная последовательность (2.1) определенная числами $\{a, c, m\}$ имеет при любом начальном значении x_0 максимальный период m тогда и только тогда, когда*

1. *числа c и m взаимно просты, т.е. $(c, m) = 1$;*
2. *число $b = a - 1$ кратно p для каждого простого $p < m$, являющегося делителем числа m;*
3. *число b кратно 4, если m кратно 4.*

Доказательство. Смотри [7], стр. 28.

Примеры ЛКГ, имеющих максимальный период

2.1. $\{a = 106, c = 1283, m = 6075\}$.
(1283,6075)=GCD[1283,6075]=1;

b=a-1=105,
FactorInteger[105]={{3, 1}, {5, 1}, {7, 1}},
$105 = 3 \cdot 5 \cdot 7$,
FactorInteger[6075]={{3, 5}, {5, 2}},
$6075 = 3^5 \cdot 5^2$;

2.2. $\{a = 141,\ c = 28411,\ m = 134456\}$.
(28411,134456)=**GCD[28411, 134456]**=1;
b=a-1=140,
FactorInteger[140]={{2, 2}, {5, 1}, {7, 1}},
$140 = 4 \cdot 5 \cdot 7$.
FactorInteger[134456]={{2, 3}, {7, 5}},
$134456 = 4 \cdot 2 \cdot 7^5$.

В книге ([8], стр. 416-417) приведено большое число примеров ЛКГ, имеющих максимальный период.

Взлом линейного конгруэнтного генератора

Рассмотрим ситуацию, когда некоторое число элементов линейной конгруэнтной последовательности (2.1)

$$x_k, x_{k+1}, \ldots, x_{k+n} \tag{2.2}$$

доступны для наблюдений, но параметры ЛКГ $\{m, a, c\}$ наблюдателю неизвестны.

Нахождение модуля.

В следующей лемме устанавливается, как по известным членам линейной конгруэнтной последовательности можно найти числа целочисленно кратные модулю m.

Лемма 2.1, (см. [9]). *Для определителей*

$$\delta_k = \begin{vmatrix} x_{k+1} - x_k & x_{k+2} - x_{k+1} \\ x_{k+2} - x_k & x_{k+3} - x_{k+1} \end{vmatrix}, \quad \Delta_k = \begin{vmatrix} x_{k+2} - x_k & x_{k+3} - x_{k+1} \\ x_{k+4} - x_k & x_{k+5} - x_{k+1} \end{vmatrix}, \tag{2.3}$$

которые построены на основе членов линейной конгруэнтной последовательности (2.2), справедливы соотношения

$$\delta_k = 0\,(mod\, m), \quad \Delta_k = 0\,(mod\, m).$$

Доказательство. Вначале выразим члены последовательности (2.2) через x_k. Так как

$$x_{k+1} = ax_k + c\,(mod\, m),$$

то существует число $r_1 \in \mathbb{Z}$ такое, что

$$x_{k+1} = ax_k + c + r_1 m.$$

Аналогично рассуждая, для некоторого $\widetilde{r}_2 \in \mathbb{Z}$ получаем равенство

$$x_{k+2} = ax_{k+1} + c + \widetilde{r}_2 m = a^2 x_k + c(a+1) + (r_1 + \widetilde{r}_2)m.$$

Или, обозначая $r_1 + \widetilde{r}_2$ через r_2,

$$x_{k+2} = a^2 x_k + c(a+1) + r_2 m, \quad r_2 \in \mathbb{Z}.$$

Повторяя рассуждения, будем иметь

$$x_{k+3} = a^3 x_k + c(a^2 + a + 1) + r_3 m, \quad r_3 \in \mathbb{Z}.$$

$$x_{k+4} = a^4 x_k + c(a^3 + a^2 + a + 1) + r_4 m, \quad r_4 \in \mathbb{Z},$$

$$x_{k+5} = a^5 x_k + c(a^4 + a^3 + a^2 + a + 1) + r_5 m, \quad r_5 \in \mathbb{Z},$$

Наконец,

$$x_{k+n} = a^n x_k + c\frac{a^n - 1}{a - 1} + r_n m, \quad r_n \in \mathbb{Z}, \quad n = 0, 1, 2, \ldots,$$

$$\text{т.е.} \quad x_{k+n} = a^n x_k + c\frac{a^n - 1}{a - 1} \,(mod\, m).$$

Используя найденные выражения, нетрудно вычислить определитель[3]

$$\delta_k = (x_{k+1} - x_k)(x_{k+3} - x_{k+1}) - (x_{k+2} - x_{k+1})(x_{k+2} - x_k) =$$

$$= [(a-1)x_k + c + r_1 m][a(a^2-1)x_k + c\,a(a+1) + (r_3 - r_1)m] -$$

$$-[a(a-1)x_k + c\,a + (r_2 - r_1)m][(a^2-1)x_k + c(a+1) + r_2 m] =$$

$$= m^2 C_1 + mC_2 = m(mC_1 + C_2);$$

где

$$mC_1 + C_2 \in \mathbb{Z}, \quad \text{так как} \quad C_1 = -r_1^2 + r_1 r_2 - r_2^2 + r_1 r_3 \in \mathbb{Z},$$

$$\text{и} \quad C_2 = a^2 c r_1 + 2ac(r_1 - r_2) + c(r_3 - r_2) +$$

$$+ \left[a^3 r_1 + a^2(r_1 - 2r_2) + + a(-2r_1 + r_2 + r_3) + r_2 - r_3\right] x_k \in \mathbb{Z}.$$

Аналогично рассуждая, будем иметь

$$\Delta_k = (x_{k+2} - x_k)(x_{k+5} - x_{k+1}) - (x_{k+4} - x_k)(x_{k+3} - x_{k+1}) =$$

[3]Вычисления можно провести с помощью команды 7 (см. Приложение).

$$= [(a^2-1)x_k+c(a+1)+r_2m][a(a^4-1)x_k+ca(a^3+a^2+a+1)+(r_5-r_1)m]-$$
$$-[(a^4-1)x_k+c(a^3+a^2+a+1)+r_4m][a(a^2-1)x_k+ca(a+1)+(r_3-r_1)m] = mC,$$

где

$$C = r_2[a(a^4-1)x_k + ca(a^3+a^2+a+1) + (r_5-r_1)m]-$$
$$-r_4[a(a^2-1)x_k + ca(a+1) + (r_3-r_1)m] \in \mathbb{Z}. \square$$

При практическом нахождении модуля m на основе конечного числа членов

$$x_k, x_{k+1}, \ldots, x_{k+n}$$

линейной конгруэнтной последовательности (2.1), рассматривают несколько подряд идущих "четверок"

$$\{x_k, x_{k+1}, x_{k+2}, x_{k+3}\}, \{x_{k+1}, x_{k+2}, x_{k+3}, x_{k+4}\}, \ldots, \{x_{k+s}, x_{k+s+1}, x_{k+s+2}, x_{k+s+3}\},$$

а также "шестерок"

$$\{x_k, x_{k+1}, x_{k+2}, x_{k+3}, x_{k+4}, x_{k+5}\}, \{x_{k+1}, x_{k+2}, x_{k+3}, x_{k+4}, , x_{k+5}, x_{k+6}\}, \ldots,$$

$$\{x_{k+s}, x_{k+s+1}, x_{k+s+2}, x_{k+s+3}, x_{k+s+4}, x_{k+s+5}\}.$$

Для каждой "четвертки" и "шестерки" по формулам (2.3) вычисляют определители

$$\delta_k, \ldots, \delta_{k+s}, \ \Delta_k, \ldots, \Delta_{k+s}.$$

Затем, используя лемму 2.1, в качестве оценки модуля m берут наибольший общий делитель этих определителей

$$\widetilde{m} = (\delta_k, \ldots, \delta_{k+s}, \ \Delta_k, \ldots, \Delta_{k+s}).$$

Впрочем, нередко возникает ситуация (см. примеры, рассмотренные ниже), когда

$$m \neq \widetilde{m}.$$

В таком случае для нахождения периода m следует рассматривать делители числа $\widetilde{m}$ превосходящие $\max\limits_{1\le i\le s} x_{k+i}$.

Нахождение множителя и приращения.

Будем считать, что модуль m ЛКП (2.1) нам уже известен, а множитель a и приращение c нет. Рассмотрим четыре члена ЛКП

$$x_1, \ x_2, \ x_3, \ x_4.$$

Тогда неизвестные числа a и c удовлетворяют системе сравнений.

$$\begin{cases} x_2 = ax_1 + c\,(mod\, m) \\ x_4 = ax_3 + c\,(mod\, m). \end{cases}$$

Отсюда, используя свойства сравнений, получим сравнение первой степени относительно неизвестного a :

$$(x_3 - x_1)\, a = (x_4 - x_2)\,(mod\, m). \tag{2.6}$$

Для решения этого сравнения будем использовать способ, основанный на теории непрерывных дробей (см. [10], стр. 54-56.).

Ограничимся случаем, когда

$$(x_3 - x_1, m) = 1.$$

Запишем разложение рационального числа $\frac{m}{x_3 - x_1}$ в непрерывную дробь

$$\frac{m}{x_3 - x_1} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

и рассмотрим подходящие дроби $\frac{P_k}{Q_k}$:

$$\frac{P_1}{Q_1} = q_1, \quad \frac{P_2}{Q_2} = q_1 + \frac{1}{q_2}, \quad \frac{P_3}{Q_3} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}},$$

$$\frac{P_4}{Q_4} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}}, \quad \ldots, \quad \frac{P_n}{Q_n} = \frac{m}{x_3 - x_1}.$$

Лемма 2.2. (См. [10].) *Если* $(x_3 - x_1, m) = 1$, *то решение сравнения (2.6) имеет вид*

$$a = (-1)^{n-1}(x_4 - x_2)P_{n-1}(mod\, m),$$

где P_{n-1} *- числитель предпоследней подходящей дроби.*

При известном модуле m и множителе a нетрудно найти приращение

$$c = (x_2 - ax_1)\,(mod\, m).$$

Пример 2.3. (см. [9]). Линейный конгруэнтный генератор с неизвестными параметрами m, a, c вырабатывает последовательность

308, 785, 930, 695, 864, 237, 1006, 819, 204, 777, 378, 495, 376, 357, 70, 356.

Найти параметры m, a, c. Будет ли заданная ЛКП иметь максимальный период?

Решение. $x_1 = 308$, $x_2 = 785$, $x_3 = 930$, $x_4 = 695$, $x_5 = 864$, $x_6 = 237$, $x_7 = 1006$, $x_8 = 819$, $x_9 = 204$, $x_{10} = 777$.

Вначале найдем модуль m заданной ЛКП[4].

$$\Delta_1 = \begin{vmatrix} x_3 - x_1 & x_4 - x_2 \\ x_5 - x_1 & x_6 - x_2 \end{vmatrix} = \begin{vmatrix} 622 & -90 \\ 556 & -548 \end{vmatrix} = -290816,$$

$$\Delta_2 = \begin{vmatrix} x_4 - x_2 & x_5 - x_3 \\ x_6 - x_2 & x_7 - x_3 \end{vmatrix} = \begin{vmatrix} -90 & -66 \\ -548 & 76 \end{vmatrix} = -43008,$$

$$\Delta_3 = \begin{vmatrix} x_5 - x_3 & x_6 - x_4 \\ x_7 - x_3 & x_8 - x_4 \end{vmatrix} = \begin{vmatrix} -66 & -458 \\ 76 & 124 \end{vmatrix} = 26624,$$

$$\Delta_4 = \begin{vmatrix} x_6 - x_4 & x_7 - x_5 \\ x_8 - x_4 & x_9 - x_5 \end{vmatrix} = \begin{vmatrix} -458 & 142 \\ 124 & -660 \end{vmatrix} = 1024.$$

$$(-290816, -43008, 26624, 1024) =$$

GCD[-290816,-43008,26624,1024]=1024.

В качестве модуля будем рассматривать число $m = 1024$.

Далее

$$x_3 - x_1 = 622, \quad x_4 - x_3 = -90.$$

Поэтому сравнение (2.6) принимает вид

$$622\, a = -90\,(mod\, 1024). \tag{2.10}$$

Заметим, что наибольший общий делитель

$$(622, -90, 1024) = 2.$$

[4]При вычислении определителей с помощью пакета MATHEMATICA, используются команда **7**

Так как обе части сравнения и модуль можно разделить на любой их общий делитель, то сравнение (2.10) принимает вид

$$311\,a = -45\,(mod 512). \qquad (2.11)$$

С помощью команды 8 получим список подходящих дробей, соответствующих представлению рационального числа числа $\frac{512}{311}$ в виде непрерывной дроби.

$$\mathbf{Convergents[512/311]} =$$
$$= \{1,\ 2,\ 3/2,\ 5/3,\ 23/14,\ 28/17,\ 107/65,\ 135/82,\ 512/311\}.$$

Используя лемму 2.2, и команду 4 получим решение сравнения (2.11):

$$n = 9,\quad P_8 = 135,$$

$$a = (-1)^8 \cdot (-45) \cdot 135\,(mod 512) =$$
$$= \mathbf{Mod[(-45)\cdot 135,512]} = 69,$$

$$c = (785 - 69 \cdot 308)\,(mod 1024) =$$
$$= \mathbf{Mod[785 - 69\cdot 308,\ 1024]} = 13.$$

Таким образом, уравнение линейного конгруэнтного генератора имеет вид

$$x_{n+1} = 69x_n + 13\,(mod 1024), \quad n = 0,\ 1,\ 2,\ \ldots. \qquad (2.12)$$

Проверка. Используя формулу (2.12) для вычисление элементов линейной конгруэнтной последовательности с начальным элементом $x_1 = 308$, получаем исходную последовательность

308, 785, 930, 695, 864, 237, 1006, 819, 204, 777, 378, 495, 376, 357, 70, 356.

Проверим выполнение условий теоремы 2.1.
(c,m)=(13,1024)=1;
b=a-1=68, $\mathbf{FactorInteger[68]=\{\{2,\ 2\},\ \{17,\ 1\}\}}$, $68 = 4 \cdot 17$,
$\mathbf{FactorInteger[1024]=\{\{2,\ 10\}\}}$, $1024 = 2^{10}$.
Все условия теоремы 2.1 выполняются. ЛКГ, определяемый соотношением (2.12), имеет максимальный период $m = 1024$. □

Пример 2.4. (см. [9]). Линейный конгруэнтный генератор с неизвестными параметрами m, a, c вырабатывает последовательность

768, 54, 747, 221, 321, 48, 225, 669, 414, 163, 260, 723, 127, 119, 420, 685.

Найти параметры m, a, c. Будет ли заданная ЛКП иметь максимальный период?

Приложение

А. Необходимые определения и утверждения из теории чисел[5].

1. Сравнения.

Имея дело с натуральными числами, будем использовать стандартные обозначения:

- $a|b$ - *a делит b*, $a \nmid b$ - *a не делит b*,
- (a, b) - *наибольший общий делитель чисел a и b*,
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Определение. *Если два целых числа a и b при делении на целое число (модуль) n дают одинаковые остатки, то эти числа называют сравнимыми по модулю n и пишут*

$$a \equiv b \,(mod\, n).$$

Нетрудно убедиться в справедливости утверждения

$a \equiv b \,(mod\, n)$ тогда и только тогда, когда $n|(a-b)$.

2. Алгоритм Евклида.

Для нахождения наибольшего общего делителя (a, b) двух натуральных чисел (с помощью последовательного деления с остатком) прменяют алгоритм Евклида.

Теорема. *Для любых натуральных a и b таких, что $b \nmid a$ при некотором s существуют натуральные числа*

$$q_0, q_1, \ldots, q_s, \quad u \quad r_1, \ldots, r_s,$$

для которых выполняются соотношения $b > r_1 > r_2 > \ldots > r_s > 0$,

$$\begin{array}{lcl} a & = & q_0 b + r_1, \\ b & = & q_1 r_1 + r_2, \\ r_1 & = & q_2 r_2 + r_3, \\ \ldots & \ldots & \ldots\ldots\ldots \\ r_{s-2} & = & q_{s-1} r_{s-1} + r_s, \\ r_{s-1} & = & q_s r_s, \\ (a, b) & = & r_s. \end{array}$$

[5]Эту информацию можно найти в книге [10].

3. Обратимые элементы в $\mathbb{Z}_m$

Определение. *Элемент $c \in \mathbb{Z}_m$ называется* обратимым по умножению, *если найдется элемент $d \in \mathbb{Z}_m$, такой что*

$$c \cdot d \equiv 1 \,(mod\, m). \qquad (*)$$

Если для элементов c и d выполняется равенство $(*)$, то d называют обратным *элементом по отношению к c и обозначают через c^{-1}.*

Итак, для обратимого элемента c выполняется равенство

$$c \cdot c^{-1} \equiv 1 \,(mod\, m).$$

Теорема 3. *Обратимыми по умножению являются те и только те элементы из $\mathbb{Z}_m$, которые взаимно просты с модулем m. Для каждого обратимого элемента $c \in \mathbb{Z}_m$ существует только один обратный элемент.*

Б. Список использованных команд системы MATHEMATICA[6]

1. Команда вычисления наибольшего общего делителя двух натуральных чисел (a, b) :

GCD[a,b].

2. Команда вычисления наибольшего общего делителя нескольких натуральных чисел $a, b, ..., f$:

GCD[a, b, ... , f].

3. Команда разложения натурального числа n на простые множители с указанием показателей степеней этих множителей:

FactorInteger[n].

4. Команда вычисления остатка от деления числа a на модуль n :

$$a \,(mod\, n) = \textbf{Mod[a,n]}.$$

5. Команда вычисление обратного элемента в $\mathbb{Z}_m$:

$$a^{-1} \,(mod\, m) = \textbf{PowerMod[a,-1,m]}, \quad \text{если } (a, m) = 1.$$

[6]Необходимый перечень команд вместе с примерами их применения можно найти в самой системе MATHEMATICA.

6. Команда вычисления натуральной степени элемента в $\mathbb{Z}_n$:

$$u^v \,(mod\, n) = \textbf{PowerMod[u,v,n]}.$$

7. Команда вычисления определителя квадратной матрицы:

Det[matrix].

8. Команда вычисления подходящих дробей, соответствующих представлению рационального числа **a** в виде непрерывной дроби:

Convergents[a].

Библиографический список

1. Rivest R.L., Shamir A., Adelman L. *A method for obtaining digital signatures and public-key cryptosystems.* Comm. ACM, 21(2):120-126,1978.
2. van Tilborg H. (ed.) *Encyclopedia of cryptography and sequrity.* Springer, 2005. 684 p.
3. Смарт Н. *Криптография.* М.: Техносфера, 2005. 525 с.
4. Коблиц Н. *Курс теории чисел и криптографии.* М.: ТВП, 2001. 260 с.
5. Ященко В.В. (ред.) *Введение в криптографию.* СПб., МЦНМО, 2001. 271 с .
6. Черемушкин А.В. *Лекции по арифметическим алгоритмам в криптографии.* М.: МЦНМО, 2002. 103 с.
7. Кнут Д. *Искусство программирования*, т. 2, 2001. 795 с.
8. Шнайер Б. *Прикладная криптография*, М.: ТРИУМФ, 2003, 816 с.
9. Marsaglia G. *Random Number Generators*, Journal of Modern Applied Statistical Methods. May, 2003, Vol.2, No.1, 2-13.
10. Виноградов И.М. *Основы теории чисел*, М.:НАУКА, 1965. 172 с.

Оглавление

Введение 3

Глава 1. Система шифрования RSA 3

Глава 2. Линейный конгруэнтный генератор 8

Приложение 15

Библиографический список 18