МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2016 г.

РАЗДЕЛЕНИЕ СЕКРЕТА

Методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 004.056.55 (076.5)

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Разделение секрета: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 13 с. Библиогр.: с. 13.

Содержат основные теоретические и практические сведения о способе разделения секрета между n участниками с помощью схемы Шамира. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться использовать пороговую схему разделения секрета между n сторонами.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Ознакомиться с примерами решения. Выбрать свой вариант задания, рассчитать схему разделения секрета между n сторонами.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Выбрать значение секрета.
4. Рассчитать пороговую схему разделения секрета между n сторонами.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Расчет схемы разделения секрета.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В 1979 году израильский криптоаналитик Ади Шамир предложил пороговую схему разделения секрета между n сторонами, которая позволяет проводить разделение таким образом, что:

- Для восстановления секрета достаточно k и больше сторон.
- Никакие$(k-1)$ и меньше сторон не смогут получить никакой информации о секрете.

Схема интерполяционных полиномов Лагранжа (схема разделения секрета Шамира или схема Шамира) — схема разделения секрета, широко используемая в криптографии. Схема Шамира позволяет реализовать (t, n) — пороговое разделение секретного сообщения (секрета) между n сторонами так, чтобы только любые t и более сторон ($t \leq n$) могли восстановить секрет. При этом любые *t-1* и менее сторон не смогут восстановить секрет.

Для интерполяции многочлена степени $(k-1)$требуется k точек. К примеру, для задания прямой достаточно двух точек, для задания параболы - трех точек, и так далее.

Основная идея данной схемы состоит в том, что интерполяция невозможна, если известно меньшее число точек.

Если мы хотим разделить секрет между n людьми таким образом, чтобы восстановить его могли только k человек ($k \leq n$), мы «прячем» его в формулу многочлена степени $k-1$. Восстановить этот многочлен и исходный секрет можно только по k точкам. Количество же различных точек многочлена не ограничено (на практике оно ограничивается размером числового поля, в котором ведутся расчёты).

Пусть нужно разделить секрет M между n сторонами таким образом, чтобы любые k участников могли бы восстановить секрет (то есть нужно реализовать(k, n) -пороговую схему).

Выберем некоторое простое число $k > M$. Это число можно открыто сообщать всем участникам. Оно задаёт конечное поле

размера p. Над этим полем построим многочлен степени $(k-1)$ (то есть случайно выберем все коэффициенты многочлена, кроме M):

$$F(x) = (\, a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + M) \bmod p$$

В этом многочлене M — это разделяемый секрет, а остальные коэффициенты a_{k-1}, a_{k-2}.. — некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

Генерация долей секрета.

Теперь вычисляем «тени» — значения построенного выше многочлена, в nразличных точках, причём $(x \neq 0)$:

$k_1 = F(1) = (\, a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \cdots + a_1 \cdot 1 + M) \bmod p$

$k_2 = F(2) = (\, a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + \cdots + a_1 \cdot 2 + M) \bmod p$

$k_i = F(i) = (\, a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + \cdots + a_1 \cdot i + M) \bmod p$

$k_n = F(n) = (\, a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \cdots + a_1 \cdot n + M) \bmod p$

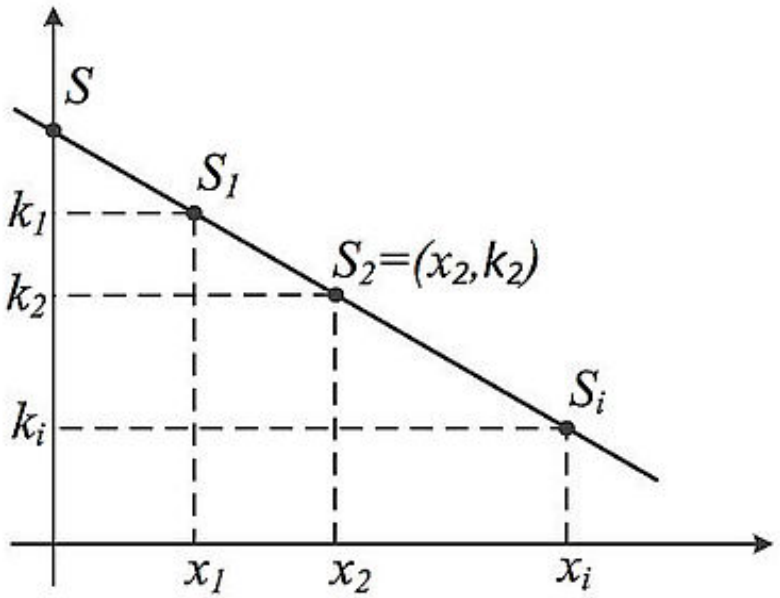

Рисунок 1 - Случай, когда для восстановления секрета необходимо две тени

Рассмотрим простой случай, когда для восстановления секрета необходимо две тени. Многочлен, в этом случае, будет задавать прямую, пересекающуюся с осью k в точке S (секрет). Каждая тень — точка на прямой. Секрет может быть восстановлен по двум произвольным теням. Однако, в случае задания лишь одной тени в качестве искомого секрета может быть выбрана любая точка на оси k, так как через одну точку можно провести множество различных прямых, пересекающихся с осью k в произвольных точках.

Аргументы многочлена (номера секретов) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдаётся доля секрета — тень k_i вместе с номером i. Помимо этого, всем сторонам сообщается степень многочлена k-1 и размер поля p. Случайные коэффициенты a_{k-1}, a_{k-2}.. и сам секрет M «забываются».

Восстановление секрета.

Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет[3].

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных $k-1$теней оценивается как p^{-1} . То есть в результате интерполяции по $k-1$ точке секретом может быть любой элемент поля с равной вероятностью. При этом попытка полного перебора всех возможных теней не позволит злоумышленникам получить дополнительную информацию о секрете.

Прямолинейное восстановление коэффициентов многочлена через решение системы уравнений можно заменить на вычисление интерполяционного многочлена Лагранжа (отсюда одно из

названий метода). Формула многочлена будет выглядеть следующим образом[3]:

$$F(x) = \sum_i l_i(x) y_i \ mod\ p$$

$$l_i(x) = \prod_{i \neq j} \frac{x - x_y}{x_i - x_j} \ mod\ p$$

где x_i, y_i — координаты точек многочлена.

Все операции выполняются также в конечном поле p.

К достоинствам данной схемы разделения секрета относят:

1. Идеальность: отсутствует избыточность — размер каждой из теней равен размеру секрета.

2. Масштабируемость: в условиях схемы (k, n) число владельцев части секрета n может дополнительно увеличиться вплоть до p, где p— размер поля, в котором ведутся вычисления. При этом количество теней k, необходимых для получения секрета, останется неизменным.

3. Динамичность: в случае, если были скомпрометированы k теней (либо утрачены $(n - k + 1)$ теней), то доверенный центр может быстро создать новую надёжную схему разделения секрета, сохранив при это сам секрет (свободный коэффициент многочлена) неизменным.

4. Гибкость: в тех случаях, когда стороны не являются равными между собой схема позволяет это учесть путём выдачи сразу нескольких теней одной стороне. Например, пусковой код баллистической ракеты может быть разделён по схеме (3,6) так, чтобы ракету могли запустить лишь три генерала, которые соберутся вместе, либо один президент, которому при разделении секрета было выдано сразу три тени.

Недостатки:

1. Ненадёжность дилера: по умолчанию в схеме предполагается, что тот, кто генерирует и раздаёт тени, надёжен, что не всегда верно.

2. Нет проверки корректности теней сторон: участвующая в разделении сторона не может с уверенностью сказать, что её тень подлинна — при подстановке в исходный многочлен получается верное равенство.

Данная схема нашла применение в аппаратных криптографических модулях. Где она используется для многопользовательской авторизации в инфраструктуре открытых ключей.

Также схема используется в цифровой стеганографии для скрытой передачи информации в цифровых изображениях, для противодействия атакам по сторонним каналам при реализации алгоритма AES.

Помимо этого, с помощью схемы Шамира может осуществляться нанесение цифрового водяного знака при передаче цифрового видео и генерация персонального криптографического ключа, используемого в биометрических системах аутентификации.

6. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Пусть нужно разделить секрет «11» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. То есть нужно реализовать (3,5) - пороговую схему.

Возьмём простое число $p = 13$.

Построим многочлен степени $k - 1 = 3 - 1 = 2$:

$$F(x) = (7x^2 + 8x + 11) mod\ 13$$

В этом многочлене 11 — это разделяемый секрет, а остальные коэффициенты 7 и 8 — некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

Теперь вычисляем координаты 5 различных точек:

$$k_1 = F(1) = (7 \cdot 1^2 + 8 \cdot 1 + 11) mod\ 13 = 0$$
$$k_2 = F(2) = (7 \cdot 2^2 + 8 \cdot 2 + 11) mod\ 13 = 3$$
$$k_3 = F(3) = (7 \cdot 3^2 + 8 \cdot 3 + 11) mod\ 13 = 7$$
$$k_4 = F(4) = (7 \cdot 4^2 + 8 \cdot 4 + 11) mod\ 13 = 12$$
$$k_5 = F(5) = (7 \cdot 5^2 + 8 \cdot 5 + 11) mod\ 13 = 5$$

После этого ключи (вместе с их номером, числом $p = 13$ и степенью многочлена ($k - 1 = 2$) раздаются сторонам. Случайные коэффициенты 7,8 и сам секрет M=11 «забываются».

Теперь любые 3 участника смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделённый секрет. Например, чтобы восстановить многочлен по трём долям k_2, k_3, k_5 им нужно будет решить систему:

$$\begin{cases} (a_2 \cdot 2^2 + a_1 \cdot 2 + M)\ mod\ 13 = 3 \\ (a_2 \cdot 3^2 + a_1 \cdot 3 + M)\ mod\ 13 = 7 \\ (a_2 \cdot 5^2 + a_1 \cdot 5 + M)\ mod\ 13 = 5 \end{cases}$$

Очевидно, что с меньшим числом известных секретов получится меньше уравнений и систему решить будет нельзя (даже полным перебором решений).

Построим интерполяционный многочлен Лагранжа:

$$F(x) = \sum_i l_i(x) y_i \ mod\ p$$

$$l_i(x) = \prod_{i \neq j} \frac{x - x_y}{x_i - x_j} \ mod\ p$$

$$l_1(x) = \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = \frac{1}{3}(x^2 - 8x + 15)$$
$$= 9(x^2 + 5x + 2) = 9x^2 + 6x + 5 \ \ mod\ 13$$

$$l_1(x) = \frac{x - x_{12}}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = \frac{1}{11}(x^2 - 7x + 10)$$
$$= 6(x^2 + 6x + 10) = 6x^2 + 10x + 8 \ \ mod\ 13$$

$$l_1(x) = \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = \frac{1}{6}(x^2 - 5x + 6)$$
$$= 11(x^2 + 8x + 6) = 11x^2 + 10x + 1 \ \ mod\ 13$$

Получим исходный многочлен:

$$F(x) = 3 \cdot l_1(x) + 7 \cdot l_2(x) + 5 \cdot l_3(x) \ \mathrm{mod}\ p$$
$$a_2 = 9 \cdot 3 + 6 \cdot 7 + 11 \cdot 5 = 7\ mod\ 13$$
$$a_1 = 6 \cdot 3 + 10 \cdot 7 + 10 \cdot 5 = 8\ mod\ 13$$
$$M = 5 \cdot 3 + 8 \cdot 7 + 1 \cdot 5 = 11 \ mod\ 13$$
$$F(x) = 7x^2 + 8x + 11 \ mod\ 13$$

Последний коэффициент многочлена *M=11* и является секретом.

7. ВАРИАНТЫ ЗАДАНИЙ

Необходимо рассчитать (4,5) -пороговую схему.

№ вар.	*M*	*P*
1	57	61
2	48	53
3	45	59
4	36	47
5	52	59
6	29	41
7	23	37
8	47	53
9	49	59
10	31	43
11	43	53
12	30	41
13	37	47
14	26	37
15	32	41
16	35	43
17	27	41
18	40	53
19	34	41
20	33	43
21	24	37
22	44	53
23	50	59
24	42	47
25	41	53
26	46	59
27	51	53
28	38	47
29	46	53
30	39	47

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Виноградов И.М. Основы теории чисел. М.: Наука,1995.
2. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.
3. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение,1970.
4. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.
5. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999
6. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993
7. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003