Лабораторная работа №2.
Исследование схем разделения секрета

Цель работы: Ознакомить студентов с различными схемами разделения секретных ключей, которые используются в криптографических системах для предотвращения их несанкционированного использования.

Теоретические пояснения

Рассмотрим случай, когда руководитель банка или какой-либо другой организации не полностью доверяет своим сотрудникам и хочет подстраховаться при использовании секретного ключа. Он может разделить весь секретный ключ (двоичная или десятичная последовательность символов) на отдельные фрагменты и эти фрагменты раздать нескольким сотрудникам так, чтобы при общем числе сотрудников n полный ключ мог быть ими составлен, если соберутся вместе не менее h сотрудников.

1. Наиболее просто поставленная задача решается при h = n, т.е. когда ключ раздается n сотрудникам и требуется наличие всех n фрагментов ключа, чтобы собрать полностью секретный ключ S [1]. Выберем некоторое простое число p, и пусть секретный ключ представляется в виде набора $(s_1,s_2,s_3,\ldots,s_k)$, где все s_i являются элементами поля Галуа – GF(p) [4]. Разделим секретный ключ на n фрагментов следующим образом. Будем генерировать произвольные случайные числа:

$(a_{11}, a_{12}, a_{13},\ldots, a_{1k})$ - фрагмент секретного ключа 1-го сотрудника,

$(a_{21}, a_{22}, a_{23},\ldots, a_{2k})$ - фрагмент секретного ключа 2-го сотрудника,

……..

$(a_{n-11},a_{n-12},a_{n-13},\ldots, a_{n-1k})$ - фрагмент секретного ключа n-1 –го сотрудника.

А последнему n-му сотруднику вычислим элементы его фрагмента секретного ключа по следующему правилу:

$a_{n1} = (s_1 - a_{11} - a_{21} - a_{31} - \ldots - a_{n1}) \bmod p.$

$a_{n2} = (s_2 - a_{12} - a_{22} - a_{32} - \ldots - a_{n2}) \bmod p.$

……

$a_{nk} = (s_k - a_{1k} - a_{2k} - a_{3k} - \ldots - a_{nk}) \bmod p.$

В этом случае только при сложении всех фрагментов ключа по модулю p получим полный секретный ключ.

Пример. Пусть p = 29 и секретный ключ имеет вид: (26,13,21,8,0,18). Требуется разделить его на 5 фрагментов для раздачи 5 сотрудникам. Для первых четырех из них генератор случайных чисел по модулю 29 пусть выработал фрагменты:

(26, 0, 13, 11, 23, 25)

(2, 7, 15, 12, 27, 6)

(1, 3 , 24, 6, 0, 16)

(12, 2, 7, 0, 7, 0)

Для последнего, пятого сотрудника вычисленный фрагмент имеет вид:

(14, 1, 20, 8, 1, 0).

Легко проверяется, что сложение всех фрагментов (каждый элемент складывается по модулю 29) дает полный секретный ключ (26,13,21,8,0,18).

Следует заметить, что сложность подбора секретного ключа в рассмотренном случае зависит только от значения модуля p и числа элементов k и практически не зависит от количества сотрудников n.

2. Рассмотрим случай, когда h < n. Имеется несколько вариантов решения такой пороговой задачи. Приведем алгоритм, описанный в [2]. Он основан на модульной арифметике и китайской теореме об остатках.

Имеется n участников $A_1,A_2,A_3,\ldots,A_n$. Пусть m_i, i = 1,2,…n, целые числа, большие 1, такие, что $(m_i,m_j) = 1$ при $i \neq j$. В данном случае запись $(m_i,m_j) = 1$ означает, что числа m_i и m_j взаимно простые, т.е. не имеют общих множителей. Например, к взаимно простым числам относятся все простые числа [4].

Обозначим за M – произведение всех чисел m_i, т.е. $M = m_1m_2m_3\ldots,m_i,\ldots m_t$. Обозначим также M_i – произведение всех m_j (j = 1,2,…, i-1,i+1,…,n), кроме m_i, т.е.$M_i = M/m_i$. Вычислим значения N_i из условия: $M_iN_i \equiv 1 \bmod m_i$. Так как $(M_i,m_i) = 1$, то решение всегда существует, и все N_i будут найдены.

Если имеется n сравнений вида: $x \equiv a_i \bmod m_i$, i = 1,2,…,n, a_i – целые, то общее решение этих сравнений имеет вид: $x \equiv \sum_{i=1}^{n} a_i M_i N_i$

Кроме того, это решение единственное, т.е. любое другое решение y удовлетворяет сравнению: $y \equiv x \bmod M$.

Пусть теперь k фиксированный порог, $1 < k \leq n$. Обозначим через min(k) – наименьшее из k произведений m_i, а max(k-1) – наибольшее из k-1 произведений m_i. Если выполнены условия:

$$\min(k) - \max(k-1) \geq 3 \max(k-1) \quad (2)$$

$$\text{и } \max(k-1) < c < \min(k), \quad (3)$$

то множество $\{a_1,a_2,\ldots,a_t\}$, где $a_i \equiv c \bmod m_i$, образует (k,n) пороговую схему для c [2]. Это означает, что если c – некоторый секретный ключ, а a_i – фрагменты ключа, розданные n участникам, то любые k из участников смогут восстановить значение c по его фрагментам, а любые k-1 участников сделать это не смогут (без перебора вариантов). При этом, чем больше в (2) разность, тем труднее k-1 участникам подобрать секретный ключ по своим фрагментам.

Пример. Пусть n = 5 и $m_1 = 97$; $m_2 = 98$, $m_3 = 99$, $m_4 = 101$, $m_5 = 103$. Возьмем k = 3 и вычислим min(3) = (97*98*99) = 941094; max(2) = (101*103) = 10403. Неравенство (2) примет вид: 941094 – 10403 = 930691 > 3*10403 = 31209.

Секретное число c должно лежать в пределах (3). Пусть оно известно некоторому сотруднику, разделяющему секрет, который вычислил значения a_i (i = 1,2,…,5) из условий $a_i \equiv c \bmod m_i$ и раздал фрагменты секрета пяти участникам: $a_1 = 62$, $a_2 = 4$, $a_3 = 50$, $a_4 = 50$, $a_5 = 38$. Пусть теперь трое из пяти участников, например, A_2,A_3 и A_4 пытаются восстановить секретный ключ c по своим фрагментам. Поскольку каждый участник знает только свое значение m_i, то они вычисляют: $M_2' = m_3 m_4 = 9999$; $M_3' = m_2 m_4 = 9898$; $M_4' = m_2 m_3 = 9702$, а затем соответствующие значения N_i: $N_2 = 33$, $N_3 = 49$, $N_4 = 17$. После чего находят значение x = 4*9999*33 + 50*9898*49 + 50*9702*17 = 33816668. Секретный ключ вычисляется из сравнения: $c \equiv x \bmod (m_2 m_3 m_4)$, т.е. $c \equiv 33816668 \bmod (98*99*101) \equiv 500000 \bmod 979902$.

Если взять любую другую тройку клиентов, например, A_1,A_4,A_5, то они вычислят тот же секретный ключ c = 500000.

Пусть теперь двое клиентов, например, A_2 и A_5 пытаются найти секретный ключ c. Они вычисляют значения y = 4*103*59 + 38*98*41 = 176992 ≡ 5394 ≡ c mod 10094. Они понимают, что истинный секретный ключ находится из условий: 5394 + i 10094, но значения i не знают. Количество значений i определяется как целая часть дроби: $\left[\frac{\min(k) - \max(k-1) - 1}{\max(k-1)}\right]$

Для рассматриваемого примера целая часть дроби равна 89, т.е. двум участникам потребуется перебрать 89 вариантов ключа. В реальных условиях количество вариантов может быть сделано существенно большим.

3. Рассмотрим еще один пример разделения секретного ключа, описанный в [4]. Пусть к приему сообщения допущено n сотрудников, из которых не все могут оказаться на месте во время приема. Фрагменты ключа распределяются между сотрудниками по

определенному правилу, причем так, что ни один сотрудник не имеет полного набора фрагментов ключа. Сообщение может быть расшифровано, если соберутся h или более сотрудников (т.е. h сотрудников должны иметь полный набор фрагментов), при этом $1 \le h \le n$. В дальнейшем слова “фрагмент ключа” будем заменять на слово “фрагмент, имея в виду, что это фрагмент общего секретного ключа.

Требуется по заданным параметрам n и h определить число фрагментов k и дать правило распределения этих фрагментов между сотрудниками.

Сначала рассмотрим случай, когда n – нечетное число и $h = (n+1)/2$.

1. Мажоритарный принцип.

Замечание 1. Известно, что n - разрядными равновесными кодами веса q называют двоичные n- разрядные комбинации, содержащие ровно q единиц и n - q нулей. Полным равновесным кодом длины n веса q будем называть набор всех кодов, отвечающих данным условиям и обозначать R(n,q).

Замечание 2. P(a,b) - обозначают количество перестановок из a объектов 1-го вида и b объектов второго, это число равно:

$$P(a,b) = \frac{(a+b)!}{a!b!} = C^{a}_{(a+b)} = C^{b}_{(a+b)} \qquad (4)$$

Для R(n,q) число комбинаций равно P(n-q,q).

Рассмотрим поставленную задачу в случае, когда n - нечетное число, а порог $h = (n+1)/2$.

Теорема 1: Если n - нечетное число и порог $h = (n+1)/2$, тогда количество фрагментов ключа k равно числу n разрядных двоичных кодов веса h, а именно

$$k = P\left(\frac{n+1}{2}, \frac{n-1}{2}\right) = \frac{n!}{((n+1)/2)!((n-1)/2)!},$$

а правило распределения ключей между сотрудниками соответствует столбцам полного равновесного кода R(n,q).

Доказательство необходимости и достаточности приведено ниже.

Пример 1. Пусть $n = 5$ и $h = 3$. Построим таблицу равновесных 5 -и разрядных кодов веса 3 , т.е. R (5,3)

Таблица 1

	1	2	3	4	5
1)	1	1	1	0	0
2)	1	1	0	1	0
3)	1	1	0	0	1
4)	1	0	1	1	0
5)	1	0	1	0	1
6)	1	0	0	1	1
7)	0	1	1	1	0
8)	0	1	1	0	1
9)	0	1	0	1	1
10)	0	0	1	1	1

В таблице цифрами 1,2,3,4,5 обозначены члены приемной команды, а 1),2),3),... обозначены номера фрагментов. Возьмем для примера 3-го члена команды. Он имеет фрагменты с номерами 1),4),5),7),8),10). Любая тройка членов приемной команды имеет полный набор фрагментов и может составить полный секретный ключ S. При этом никакие пары членов приемной команды не имеют полного набора. Количество фрагментов в данном примере равно 10. Единицы в вертикальном коде соответствуют номерам фрагментов, которые имеет данный член команды.

2.Принцип с произвольным порогом

В некоторых случаях может оказаться более удобным принцип, основанный на произвольном пороге h. Для этого сформулируем и докажем следующую теорему.

Теорема 2: Если максимальное число людей, имеющих ключи равно n (здесь уже n - любое целое положительное число) и требуется обеспечить решение при пороге h, то количество фрагментов равно числу кодовых комбинаций в R(n, n-h+1)

$$k = P(h-1, n-h+1) = \frac{n!}{(h-1)!(n-h+1)!}.$$

Пример 2. Пусть n = 6, h = 2. Построим равновесный двоичный код R(6,5)

Таблица 2.

	1	2	3	4	5	6
1)	1	1	1	1	1	0
2)	1	1	1	1	0	1
3)	1	1	1	0	1	1
4)	1	1	0	1	1	1
5)	1	0	1	1	1	1
6)	0	1	1	1	1	1

Дизъюнкция любых двух столбцов дает код, содержащий все единицы. Доказательство необходимости и достаточности приведено ниже.

Теорема 2 является обобщением теоремы 1. Действительно, если положить в теореме 2 значение h = (n +1)/2, то получим R(n,(n +1)/2).

Обе теоремы являются конструктивными, так как дают правило распределения ключей между членами принимающей команды.

Доказательство. Возьмем i -й столбец из R(n,h) и обозначим его r(i). Его вес будем определять как число единиц в коде и обозначать $|r(i)|$ Определим операцию дизъюнкции столбцов r(i) и r(j) в виде результирующего вектора той же размерности, все компоненты которого получены путем дизъюнкции соответствующих компонентов векторов r(i) и r(j).Аналогично введем операцию дизъюнкции "v" над s векторами: $r(i_1)$ v $r(i_2)$ v $r(i_3)$ v...v $r(i_s)$.

Возьмем полную таблицу кодов длины n веса q, которую мы обозначали R(n,q). Из этой таблицы выберем произвольный столбец с номером i, т.е. r(i). Определим его вес. Легко видеть, что при любом i. $|r(i)| = P(n-q, q-1) = C_{n-q}^{q-1}$.

Вес кода дизъюнкции любых s столбцов с номерами $i_1,i_2,i_3,...i_s$ при $1 < s < n-q+1$

$$\left|r(i_1) \vee r(i_2) \vee r(i_3) \vee ... \vee r(i_s)\right| = C_{n-1}^{q-1} + C_{n-2}^{q-1} + C_{n-3}^{q-1} + ... + C_{n-s}^{q-1} \qquad (5)$$

Если s = n-q+1, то сумма (5) точно равна количеству кодов в R(n,q), $C_n^q = \frac{n!}{q!(n-q)!}$

Действительно, последний член в (5) равен 1.

Если число членов s ряда (5) меньше n-q+1, то сумма (5) меньше значения (4), что доказывает теорему, так как никакие члены команды, если их меньше, чем n-q+1 не имеют полного набора ключей. В частном случае, если q = (n+1)/2, имеем, что при s = (n+1)/2 в совокупности имеется полный набор ключей для расшифровки сообщения.

Приведенный алгоритм распределения фрагментов общего секретного ключа достаточно прост и позволяет найти распределения секрета при любых значениях n и любых h ($1 \le h \le n$). Это является достоинством приведенного алгоритма. Этот алгоритм

имеет существенный недостаток, если общий ключ просто разделять на отдельные участки: чем больше соберется сотрудников (хотя их может быть и меньше h), тем легче им будет подобрать значения недостающих фрагментов. Например, если общий ключ представлял собой 20 разрядное десятичное число и его разделить на фрагменты по 2 разряда, то когда соберутся любые 2 сотрудника, им достаточно будет подобрать значения двух недостающих разрядов, т.е. проверить всего 10^2 вариантов.

Секретность приведенного алгоритма можно существенно усилить, если формировать фрагменты также как формировались фрагменты в первом примере (при h = n).

Пример 3. Пусть секретный ключ S (S_1,S_2,S_3) имеет вид S = (23,8,11), т.е. представляет собой совокупность трех элементов, где каждый элемент – произвольное положительное целое меньшее некоторого простого числа p.

Девять из десяти фрагментов получим с помощью генератора случайных чисел, при этом совершенно необязательно, чтобы элементы находились в пределах 0 – p-1. Например,

1) (5,32,18)
2) (0,19,3)
3) (36,7,16)
4) (9,11,35)
5) (16,1,28)
6) (25,39,46)
7) (3,0,21)
8) (15,14,2)
9) (35,20,20)

А десятый фрагмент (a_{10},b_{10},c_{10}) получим по следующему правилу:

$a_{10} = (S_1 - a_1 - a_2 - \ldots - a_{9)} \bmod p$

$b_{10} = (S_2 - b_1 - b_2 - \ldots - b_{9)} \bmod p$

$c_{10} = (S_3 - c_1 - c_2 - \ldots - c_{9)} \bmod p$

Для рассматриваемого примера получаем:

10) (24,10,25)

Если соберутся вместе любые три или больше сотрудников, то ключ S легко восстанавливается сложением соответствующих элементов всех десяти фрагментов по модулю 29. Если соберется вместе менее трех сотрудников, то на подбор ключа S им потребуется столько же усилий, сколько требуется любому одному сотруднику.

В общем случае при заданных n и h число фрагментов ключей равно

$$P(h-1, n-h+1) = \frac{n!}{(h-1)!(n-h+1)!}$$

Криптостойкость ключа не зависит от числа сотрудников, если их меньше h и ключ легко собирается, если число сотрудников равно или больше h.

Приведенный метод позволяет производить разделение секрета при различных степенях доверия к сотрудникам. Так, если разделяющий секрет доверяет какому-то лицу больше, чем остальным, он может выделить ему две или даже три “квоты” ключа. Порог, как и ранее можно выбирать любой (но не менее, чем число “квот”, выданных наиболее доверенному сотруднику). Естественно, число сотрудников в такой схеме соответственно уменьшается.

Использованные источники

1. Arto Salomaa Public-Key Criptography. Springer-Verlag. 1990. Berlin Heidelberg New York London Paris Tokyo Hong Kong Barselona.(Перевод на русский).
2. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М. Высшая школа. 1999, 110 стр.
3. Шеннон К. Работы по теории информации и кибернетике, М, ИЛ, 1963.
4. Ерош И.Л. Дискретная математика. Математические вопросы криптографии. Учебное пособие. СПбГУАП. 2001 г.

Порядок выполнения лабораторной работы

1. Прочитайте теоретическую часть и запустите программу на компьютере.
2. Для схемы разделение секрета среди n участников при пороге также равном n. Введите число участников - n, сам разделяемый секрет из 3-х произвольных чисел и модуль P – некоторое простое число. Автоматически для n-1 участника получите произвольные фрагменты секрета, а для n-го участника - вычисленные по методике, описанной в теоретической части. Напишите код и сравните результат, который выдаст компьютер, с исходным ключом и в случае неверного ответа найти свою ошибку. Повторите операцию для других фрагментов ключа.
3. Разделение секрета среди n участников при произвольном пороге k, основанное на китайской «Теореме об остатках». Введите число участников, необходимых для сборки ключа – k (общее число участников – n = 5). Для каждого участника выберите и введите числа m_i (i= 1,…,5), автоматически получите ограничения на значения ключа. В соответствии с ними выберите и введите ключ. Для каждого участника автоматически получите число a_i, вычисленное по методике, описанной в теоретической части. Выберите k произвольных участников (укажите их номера «галочкой») и убедитесь в том, что секретный ключ будет собран правильно. Повторите последнее действие при всех возможных сочетаниях участников по k из n.Выберите число участников больше k, укажите их номера и убедитесь в том, что ключ собран правильно. Выберите число участников меньше k и укажите их номера. Проанализируйте составленный в этом случае ключ. Изменяя значения чисел m_i, получите ограничения ключа. Проанализируйте защищенность.
4. Разделение секрета среди n участников при пороге k, основанное на свойствах равновесных кодов. Выберите и введите число участников n и порог k. Выберите секретный ключ и получите его компоненты по методике, изложенной выше. Для каждого участника сформируйте и введите распределение фрагментов ключа. Выберите номера участников, собирающих ключ, укажите их номера и убедитесь в том, что ключ собран правильно. Повторите последнее действие при всех возможных сочетаниях участников по k из n.Убедиться в том, что если число участников больше или равно k, то ключ собирается правильно, а если меньше, то ключ вообще не может быть собран.
5. Оформите отчет. Отчет должен содержать:
   a) Титульный лист с указанием университета, кафедры, дисциплины, названия лабораторной работы, № группы, фамилии студента и преподавателя.
   b) Все решения, выполненные вручную.
   c) Комментарии при проверке решений на компьютере.

Порядок выполнения лабораторной работы

6. Прочитайте теоретическую часть и запустите программу на компьютере.
7. Для схемы разделение секрета среди n участников при пороге также равном n. Введите число участников - n, сам разделяемый секрет из 3-х произвольных чисел и модуль P – некоторое простое число. Автоматически для n-1 участника получите произвольные фрагменты секрета, а для n-го участника - вычисленные по методике, описанной в теоретической части. Нажмите кнопку «Собрать», сравните результат, который выдаст компьютер, с исходным ключом и в случае неверного ответа найти свою ошибку. Повторите операцию для других фрагментов ключа.
8. Разделение секрета среди n участников при произвольном пороге k, основанное на китайской «Теореме об остатках». Введите число участников, необходимых для сборки ключа – k (общее число участников – n = 5). Для каждого участника выберите и введите числа m_i (i= 1,…,5), автоматически получите ограничения на значения ключа. В соответствии с ними выберите и введите ключ. Для каждого участника автоматически получите число a_i, вычисленное по методике, описанной в теоретической части. Выберите k произвольных участников (укажите их номера «галочкой») и убедитесь в том, что секретный ключ будет собран правильно. Повторите последнее действие при всех возможных сочетаниях участников по k из n.Выберите число участников больше k, укажите их номера и убедитесь в том, что ключ собран правильно. Выберите число участников меньше k и укажите их номера. Проанализируйте составленный в этом случае ключ. Изменяя значения чисел m_i, получите ограничения ключа. Проанализируйте защищенность.
9. Разделение секрета среди n участников при пороге k, основанное на свойствах равновесных кодов. Выберите и введите число участников n и порог k. Выберите секретный ключ и получите его компоненты по методике, изложенной выше. Для каждого участника сформируйте и введите распределение фрагментов ключа. Выберите номера участников, собирающих ключ, укажите их номера и убедитесь в том, что ключ собран правильно. Повторите последнее действие при всех возможных сочетаниях участников по k из n.Убедиться в том, что если число участников больше или равно k, то ключ собирается правильно, а если меньше, то ключ вообще не может быть собран.
10. Оформите отчет. Отчет должен содержать:
    a) Титульный лист с указанием университета, кафедры, дисциплины, названия лабораторной работы, № группы, фамилии студента и преподавателя.
    b) Все решения, выполненные вручную.
    c) Комментарии при проверке решений на компьютере.