Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра сетей и устройств телекоммуникаций

КРИПТОГРАФИЧЕСКОЕ КОДИРОВАНИЕ ИНФОРМАЦИИ

Методические указания
к лабораторной работе
по дисциплинам «Основы защиты информации»
и «Криптографическая защита информации в телекоммуникациях»
для студентов специальности «Сети телекоммуникаций»
дневной, вечерней и заочной форм обучения

В 3-х частях

Часть 3

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Минск 2003

УДК 621.391.2(075.8)
ББК 32.811 я 73
К 82

Составители:
В.Ф. Голиков, А.В. Курилович

Криптографическое кодирование информации: Метод. указания к К 82 лабораторной работе по дисциплинам «Основы защиты информации» и «Криптографическая защита информации в телекоммуникациях» для студентов специальности «Сети телекоммуникаций» дневной, вечерней и заочной форм обучения. В 3 ч. Ч. 3: Электронная цифровая подпись / Сост. В.Ф. Голиков, А.В. Курилович. — Мн.: БГУИР, 2003. — 8 с.

Методические указания составлены в соответствии с рабочей программой курса и включают основные теоретические положения и контрольные вопросы для осмысления прочитанного материала. Часть 3 посвящена изучению национального стандарта электронной цифровой подписи СТБ-1176.02-99.

УДК 621.391.2(075.8)
ББК 32.811 я 73

Части 1 и 2 настоящих методических указаний изданы в БГУИР в 2003 г.

1. ЦЕЛЬ РАБОТЫ

Закрепление теоретических знаний по национальному стандарту электронной цифровой подписи СТБ-1176.02-99.

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.1. Введение

Белорусские стандарты, регламентирующие использование электронной цифровой подписи, официальные названия которых «Процедура выработки и проверки ЭЦП» и «Функция хэширования», были разработаны группой белорусских специалистов в 1999 г. и официально приняты в 2000 г.

В данной лабораторной работе реализован стандарт «Процедура выработки и проверки ЭЦП», а стандарт «Функция хэширования» реализован в упрощенном виде.

В этих стандартах наряду с элементами классических процедур ЭЦП используются современные идеи, позволяющие увеличить криптостойкость и быстродействие. Так, открытый ключ и секретный ключ связаны известным соотношением

$$\mathrm{K_O} = \left(a^{\mathrm{K_C}}\right) \bmod \mathrm{P},$$

которое позволяет легко вычислить $\mathrm{K_O}$ по $\mathrm{K_C}$, но очень сложно решение обратной задачи — вычисления $\mathrm{K_C}$ по $\mathrm{K_O}$. К подписываемому сообщению добавляется случайная компонента t, что усложняет возможный подбор хэш-значения злоумышленником по известному тексту сообщения.

2.2. Обозначения, принятые в стандарте СТБ-1176.02-99

- B_p — множество, состоящее из чисел $1, 2, \ldots, p-1$;
- $c := d$ — присвоение параметру c значения d;
- $c \bmod d$ — остаток от деления c на d, где c — натуральное число или ноль, d — натуральное число;
- $c^{-1} \bmod d$ — натуральное число b, такое, что $b < d$ и $(cb) \bmod d = 1$, где c и d — взаимно простые числа;
- $\lceil c \rceil$ — наименьшее целое число, не меньшее, чем c;
- $\lfloor c \rfloor$ — наибольшее целое число, не большее, чем c;
- $c = \sum_{i=0}^{k-1} c_i (2^b)^i$ — разложение неотрицательного целого числа c по основанию 2^b, где k и b — натуральные числа,
- c_i — целое число, $0 \le c_i < 2^b$;

• $\oplus$бинарная операция, определенная на множестве неотрицательных целых чисел по формуле $d \oplus b = \sum_{i=0}^{k-1} \left((d_i + b_i) \bmod 2 \right) 2^i$, где $d = \sum_{i=0}^{k-1} d_i 2^i$, $b = \sum_{i=0}^{k-1} b_i 2^i$, $d_0, \ldots, d_{k-1}, b_0, \ldots, b_{k-1} \in \{0,1\}$;

• $\circ$ — операция $\circ : B_p \times B_p \to B_p$ определяется для любых $c \in B_p$ и $d \in B_p$ по формуле $c \circ d = (cd(2^{l+2})^{-1}) \bmod p$;

• $c^{(k)}$ — степень числа на основе операции $\circ$, определяется индуктивно по формуле $c^{(k)} = \begin{cases} c, & k = 1, \\ c^{(k-1)} \circ c, & k > 1. \end{cases}$, где k - натуральное число;

• h — функция хэширования, процедура вычисления значений которой соответствует СТБ.

2.3. Процедура выработки ЭЦП

1. Выбираются параметры l и r, которые определяют уровень криптографической стойкости ЭЦП. Число l является длиной записи числа p в системе счисления по основанию 2, r является длиной записи числа q в системе счисления по основанию 2.

2. В соответствии с выбранными l и r генерируются простые числа p и q, такие, что q делит $p-1$ нацело.

3. Генерируется случайное число d, $0 < d < p$.

4. Вычисляется $a = d^{\left(\frac{p-1}{q}\right)}$. Если $a \equiv 2^{l+2} \bmod p$, то перейти к пункту 3.

5. Генерируется случайное число x, $0 < x < q$, которое является секретным ключом.

6. Вычисляется число $y = a^{(x)}$, которое является открытым ключом.

7. Генерируется случайное число k, $0 < k < q$.

8. Вычисляется $t = a^{(k)}$. Далее число t разлагается по основанию 2^8, т.е. $t = \sum_{i=0}^{n-1} t_i (2^8)^i$. Таким образом, получаются коэффициенты $t_0, t_1, \ldots, t_{n-1}$.

9. Формируется последовательность $\mathrm{M}_t = (t_0, t_1, \ldots, t_{n-1}, m_1, m_2, \ldots, m_z)$, состоящая из коэффициентов $t_0, t_1, \ldots, t_{n-1}$ и блоков открытого текста $m_1, m_2, \ldots, m_z$.

10. Вычисляется значение хэш-функции $\mathrm{U} = h(\mathrm{M}_t)$. Если $\mathrm{U} = 0$, то перейти к пункту 6.

11. Вычисляется $\mathrm{V} = (k - x\mathrm{U}) \bmod q$. Если $\mathrm{V} = 0$, то перейти к пункту 6.

12.Вычисляется $\mathrm{S} = \mathrm{U} \cdot 2^r + \mathrm{V}$. ЭЦП последовательности M_t есть число S.

13.Отправляется M_t, S.

2.4. Процедура проверки ЭЦП

1. Вычисляется $\mathrm{V} = \mathrm{S} \bmod 2^r$.
2. Вычисляется $\mathrm{U} = \left(\mathrm{S} - \mathrm{V}\right) / 2^r$.
3. Если хотя бы одно из условий $0 < \mathrm{U} < 2^r$ и $0 < \mathrm{V} < q$ не выполнено, то ЭЦП считается недействительной и работа алгоритма завершается.
4. Вычисляется $t' = a^{(\mathrm{V})} \circ y^{(\mathrm{U})}$.
5. Число t' разлагается по основанию 2^8, т.е. $t' = \sum_{i=0}^{n-1} t'_i (2^8)^i$. Таким образом, получаются коэффициенты $t'_0, t'_1, \ldots, t'_{n-1}$.
6. Формируется последовательность $\mathrm{M}'_t = \left(t'_0, t'_1, \ldots, t'_{n-1}, m_1, m_2, \ldots, m_z\right)$, состоящая из коэффициентов $t'_0, t'_1, \ldots, t'_{n-1}$ и блоков открытого текста $m_1, m_2, \ldots, m_z$.
7. Вычисляется хэш-функция $\mathrm{W} = h\left(\mathrm{M}'_t\right)$.
8. Проверяется условие $\mathrm{W} = \mathrm{U}$. При совпадении W и U принимается решение о том, что ЭЦП была создана при помощи личного ключа подписи x, связанного с открытым ключом проверки подписи y, а также ЭЦП и последовательность M_t не были изменены с момента их создания. В противном случае подпись считается недействительной.

Стандарт «Процедура выработки и проверки ЭЦП» содержит алгоритмы и процедуры выработки и проверки электронной цифровой подписи, а также подробные инструкции по:

- выбору величин r и l (размер p и q);
- генерации p и q;
- генерации a.

3. ПРЕДВАРИТЕЛЬНОЕ ЗАДАНИЕ

3.1. Изучите теоретическую часть.

3.2. Определите число $b = a \bmod n$, где $a = 241$, $n = 101$ и $a = -547$, $n = 99$.

3.3. Сколько существует различных пар простых чисел p и q, находящихся в диапазоне $20 < p,\ q < 100$, и таких, что q делит $p - 1$ нацело?

3.4. Определите с помощью расширенного алгоритма Евклида число x, обратное числу $a = 5$ (т.е. $\left(xa\right) \bmod n = 1$) по модулю $n = 307$.

3.5. Разложите число $a = \text{B25DE2A1}_{16}$ по основанию 10, т.е. необходимо найти коэффициенты $t_0, t_1, \ldots, t_{n-1}$ ряда $a = \sum_{i=0}^{n-1} t_i 10^i$.

3.6. Разложите число $a = 218168065_{10}$ по основанию 2^8, т.е. необходимо найти коэффициенты $t_0, t_1, \ldots, t_{n-1}$ ряда $a = \sum_{i=0}^{n-1} t_i (2^8)^i$.

4. ЛАБОРАТОРНОЕ ЗАДАНИЕ

4.1. Включите ПЭВМ.

4.2. Запустите программу eds.exe на выполнение. Данная программа реализует национальный стандарт СТБ-1176.02-99 «Процедура выработки и проверки ЭЦП».

4.3. Нажмите кнопку «Начать выполнение работы». Выполнение работы состоит в том, что вы должны вручную найти значения в контрольных точках работы алгоритма. Для этого необходимо ввести полученное значение в соответствующее поле рабочего окна программы и нажать кнопку «Проверить». Если расчет выполнен правильно, происходит переход к следующей контрольной точке.

4.4. Руководствуйтесь инструкциями в рабочем окне программы.

5. СОДЕРЖАНИЕ ОТЧЕТА

5.1. Решение задач предварительного задания.

5.2. Результаты выполнения работы.

5.3. Анализ результатов и выводы.

6. КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. Какие числа называются простыми, взаимно простыми?

6.2. Много ли простых чисел?

6.3. Какие вы знаете способы поиска простых чисел?

6.4. На каком типе криптосистем основана ЭЦП?

6.5. Какие плюсы и минусы у криптосистем данного типа?

6.6. Поясните использование операции «$\circ$«.

6.7. Какое число называется обратным к числу a по модулю n?

6.8. Всегда ли существует обратное число в модулярной арифметике?

6.9. Какую информацию несет положительное решение при проверке ЭЦП?

6.10. Где можно получить открытый ключ y для проведения процедуры проверки ЭЦП?

6.11. Что должен знать злоумышленник, чтобы подделать ЭЦП?

ЛИТЕРАТУРА

Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.

Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.

Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. Мн.: БГУ, 1999.

Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МГИФИ, 1997.

Леонов А.П., Леонов К.П., Фролов Г.В. Безопасность автоматизированных банковских и офисных технологий. Мн.: Нац. кн. палата Беларуси, 1996.

Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. СПб.: СпбГУ, 1998.

Св. план 2003, поз. 91

Учебное издание

КРИПТОГРАФИЧЕСКОЕ КОДИРОВАНИЕ ИНФОРМАЦИИ

Методические указания
к лабораторной работе
по дисциплинам «Основы защиты информации»
и «Криптографическая защита информации в телекоммуникациях»
для студентов специальности «Сети телекоммуникаций»
дневной, вечерней и заочной форм обучения

В 3-х частях

Часть 3

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Составители:
Голиков Владимир Федорович,
Курилович Андрей Владимирович

Редактор Н.А. Бебель
Корректор Е.Н. Батурчик

Подписано в печать 26.12.2002. Формат 60×84 1/16.
Бумага офсетная. Печать ризографическая. Гарнитура «Таймс». Усл. печ. л. 0,58.
Уч.-изд. л. 0,4. Тираж 100 экз. Заказ 607.

Издатель и полиграфическое исполнение:
Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия ЛП № 156 от 30.12. 2002.
Лицензия ЛВ № 509 от 03.08. 2001.
220013, Минск, П. Бровки, 6.