13. https://www.didactic.ro/revista-cadrelor-didactice/metoda-studiului-de-caz (accesat: 24.08.2018)

ПРОЕКТИРОВАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ ПО ПО ТЕМЕ “АЛГОРИТМЫ ХЕШИРОВАНИЯ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ” ДЛЯ СТУДЕНТОВ ГУМАНИТАРНОГО ПРОФИЛЯ

Виолета Богданова, дрд., ТГУ
Любомир Кирияк, др. хаб., проф.
Тираспольский Государственный Университет

Rezumat. În articol respectiv este prezentat un model de desfăşurare a unei lecţii practice la tema ”Algoritmi de hashing şi semnătura digitală electronică” care ţine de disciplina ”Securitatea sistemelor informaţionale” pentru studenţii de la profilul economic. Sunt examinate diverse aplicaţii practice in economie ale algoritmul de criptare El Gamal. Sunt analizate aspecte didactice privind desfăşurarea lecţiilor practice.

Summary. In this article is presented the structure of a practical lesson on the discipline "Protection of computer information" on the topic "Algorithms of hashing and electronic digital signature" for students of the economic profile of training. Different practical applications in the economy of the El Gamal encryption algorithm are examined. Didactical aspects of the practical lessons are analyzed.

1. Введение

Национальная стратегия «Электронная Молдова» гласит: «Информационное общество является новой, более совершенной формой человеческой цивилизации, в которой равноправный и универсальный доступ к информации, связанный с развитием информационно-коммуникационной инфраструктуры, способствует стабильному социально-экономическому развитию, снижению уровня бедности, повышению качества жизни» [1].

Важными категориями цифровой экономики являются электронный документ и электронно-цифровая подпись (ЭЦП). Целостность и достоверность данных, наряду с конфиденциальностью, являются важнейшими составляющих ИБ в современном цифровом мире. Для решения этих задач служит криптография.

Как передать по открытому каналу связи сообщение с подтвержденной подлинностью авторства и неизмененное злоумышленником, имеющее юридическую силу? Такая задача возникает в банковской и налоговой сферах, торговле, таможенном декларировании и т.п.

В рамках дисциплины «Защита компьютерной информации» студенты экономического профиля подготовки знакомятся с основами криптографии, алгоритмами хеширования и электронно-цифровой подписи.

Применение ЭЦП позволяет:

– подтвердить подлинность электронного документа;

– повысить эффективность организационных процессов, т.к. снижаются затраты на ведение работ и услуг;

– повысить интенсивность юридически значимого документооборота (2013, Ермоленко) и т.д.

Главным отличием электронной подписи от обычной является ее зависимость от подписываемого документа [3, стр.151]

Требования к ЭЦП [5, 54 с.] представлены на рисунке.

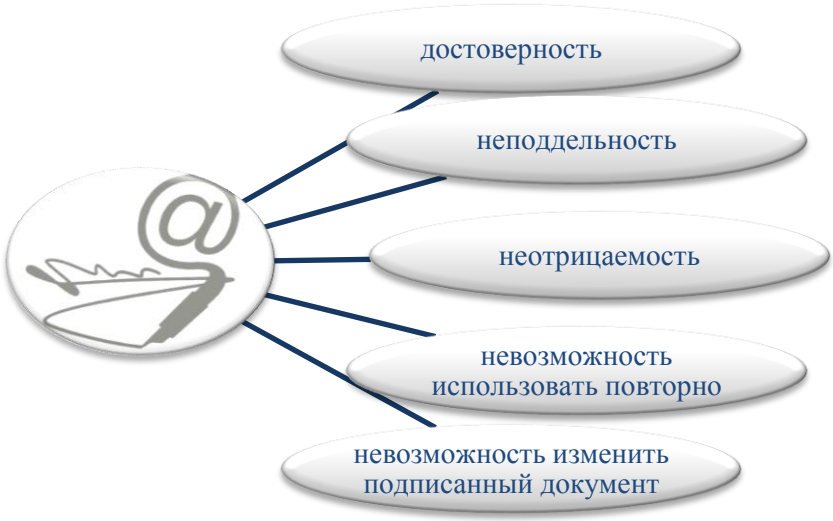

Рисунок. Требования к ЭЦП

Различные алгоритмы цифровой подписи рассматриваются на теоретическом занятии и при самостоятельной работе. На практическом занятии рассматривается процесс создания и проверки цифровой подписи по схеме Эль-Гамаля [7].

2. Структура практического занятия

2.1. Организационный этап

Студентам сообщается тема и цель практического занятия.

Тема практического занятия по дисциплине «Защита компьютерной информации» для бакалавров по направлению подготовки «Экономика»: Алгоритмы хеширования и электронной цифровой подписи.

Место занятия: компьютерный класс.

Цель занятия: закрепить и углубить полученные теоретические знания о криптографии, изложенные в лекционной части курса; реализовать практически алгоритмы создания и проверки цифровой подписи.

2.2. Этап актуализации знаний

На лекционном занятии студенты прослушали теоретический материал и получили информацию в виде презентации. Студентам предлагается ответить на контрольные вопросы по пройденному на лекции материалу:

1) Что такое идентификация пользователя?

2) В чем состоит суть алгоритма хеширования?

3) Чем отличается цифровая подпись от обычной?

4) Где применятся ЭЦП?

5) Какие требования предъявляются к ЭЦП?

6) Сформулируйте экономические преимущества электронно-цифровой подписи.

2.3. Этап постановки задачи

После актуализации знаний студентам предлагается ознакомиться на практике с алгоритмом создания и проверки ЭЦП по схеме Эль-Гамаля.

В связи с тем, что использование криптографии с открытыми ключами (подписывание, проверка подписей и т. д.), процесс очень медленный, более того, если подписывать всё сообщение целиком, то размеры этой подписи будут сопоставимы с размером сообщения; подписывают не сообщение, а хеш-функцию от сообщения. И далее получатель, когда расшифровывает подпись, получает хеш-функцию. Далее он сравнивает хеш-функцию от того сообщения, которое он получил, и хеш-функцию, которая была получена в результате расшифровки. За счет того, что хеш-функция имеет фиксированную длину, она меньше, чем само сообщение. Это позволяет быстро вычислить электронную цифровую подпись. Размер этой подписи будет мал по сравнению с размером сообщения.[5]

Пример: Создать и проверить ЭЦП для сообщения «ZKI» по схеме Эль-Гамаля.

Этап I: Создание дайджеста (свертки) сообщения, т.е. преобразование в числовой эквивалент (1):

$$m\,("ZKI") \;=>\; 25 + 10 + 8 \;=>\; 2 + 5 + 1 + 0 + 8 = 16 \;=>\; 1 + 6 = 7 \quad (1)$$

m=7

Этап II: Создание цифровой подписи:

1) Выбираем простые числа число p, g, x – секретное значение, при соблюдении условия $g < p$, $x < p$:

Пусть ***p=11, g=7, x=5***.

2) Вычисляем значение y по формуле 2:

$$y \;=\; g^x \bmod p \quad (2)$$

$$y \;=\; 7^5 \bmod 11 = 10$$

3) Получаем открытый ключ ***(p,g,y) = (11,7,10).***

4) Выбираем секретное число k из условия *НОД*(k, p -1) =1:

Пусть ***k=5***.

5) Вычислим первую часть цифровой подписи по формуле 3:

$$a \;=\; g^k \bmod p \quad (3)$$

$$a \;=\; 7^3 \bmod 11 = 2$$

6) Вычислим вторую часть цифровой подписи по формуле 4:

$$\mathrm{m} = (\mathrm{x} * \mathrm{a} + \mathrm{k} * \mathrm{b}) \bmod (\mathrm{p} - 1) \quad (4)$$

$$7 = (5 * 2 + 3 * b) mod\ 10$$

b=9

7) Получим цифровую подпись для сообщения m= “ZKI”: ***(m,a,b) = (7,2,9).***

Этап III: Проверка цифровой подписи с помощью открытого ключа:

1) Вычислим c_1 по формуле (5):

$$c_1 = y^a * a^b \bmod p \quad (5)$$

$$c_1 = 10^2 * 2^9 \bmod 11 = 6$$

2) Вычислим c_2 по формуле (6):

$$c_2 = g^m \bmod p \quad (6)$$

$$c_2 = 7^7 \bmod 11 = 6$$

3) Если $c_1 = c_2$, то подпись верна. Т.к. 6=6, то это значит, что цифровая подпись в сообщения m=7 верна.

Вывод: проверка показала идентичность подписи и сообщения. [4]

Задание. *«Сверните» свое имя до 1 цифры (вместо букв использовать порядковый номер буквы) и создайте цифровую подпись по схеме Эль-Гамаля. Поверьте сообщение и подпись коллеги.*

2.4. Этап текущего контроля знаний

Данный этап призван получить обратную связь о том, насколько качественно усвоен студентами теоретический материал по теме «Основы криптография» для студентов экономического профиля подготовки в рамках дисциплины «Защита компьютерной информации». Проведение текущего контроля осуществляется с помощью теста по теме «Алгоритмы хеширования и электронной цифровой подписи», созданного в он-лайн конструкторе testmoz.com/1802092.

Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:

a) логарифмической функция

b) сжимающая функцией

c) хэш- функция

d) электронно-цифровая подпись

Отметьте правильные высказывания: «Цифровая подпись:»

a) зависит от подписываемого документа, разная для различных текстов

b) неотделима от носителя (бумаги), поэтому отдельно подписывается каждый экземпляр

c) имеет ограничения по сроку действия

d) легко отделима от документа, поэтому верна для всех его копий

Каким требованиям должна удовлетворять цифровая подпись:

a) ЭЦП однозначно связана с лицом, подписавшим данные

b) с ее помощью можно подтвердить подлинность лица, подписавшего данные

c) подпись связана с данными, которым она соответствует

d) ее можно использовать повторно

2.6. Домашнее задание

Составить схему создания и проверки ЭЦП. Уточнтте требования, касающиеся цифровой подписи

3. Заключение

Практическое занятие «Защита компьютерной информации» по теме «Алгоритмы хеширования и электронной цифровой подписи» позволяет развить у студентов экономического профиля подготовки не только информационную культуру в области информационной безопасности, но и математическую компетенцию. Развитие математической компетенции у студентов гуманитарного профиля подготовки способствует повышению продуктивности мышления и качества аргументации, развития умственных способностей и предметной речи [6].

Библиография

1. Постановление Правительства Республики Молдова №255 от 09.03.2005 о Национальной стратегии создания информационного общества. «Электронная Молдова».–[URL:lex.justice.md/document_rus.php?id=50B7955B:0183B7ED].
2. Лапонина О.Р. Криптографические основы безопасности. М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2004. С. 320. ISBN 5-9556-00020-5.
3. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. М.: ФОРУМ, 2012. – 240 с.
4. Спиридонова И.А. Основы криптографии : методические указания к практическим занятиям, лабораторным работам и самостоятельной работе студента / Южно-Российский государственный политехнический университет (НПИ) имени М. И. Платова. – Новочеркасск: ЮРГПУ (НПИ), 2016. 28 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.:ТРИУМФ, 2003. 816 с.
6. Яшин Б.Л. Математика в контексте философских проблем: Уч. пособие. М.:МПГУ, 2012. 110 с. –С.100.
7. Gamal T. El. A public key cryptosystem and a signature scheme based on discrete algorithms. IEEE Transactions on Information, Theory, 31 (1985), pp. 469-472.