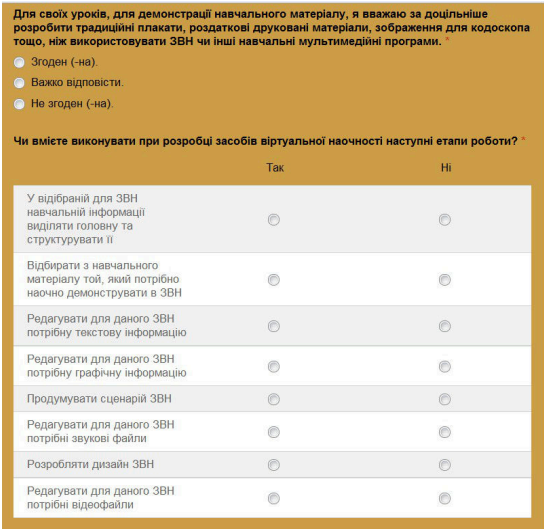
Для своїх уроків, для демонстрації навчального матеріалу, я вважаю за доцільніше розробити традиційні плакати, роздаткові друковані матеріали, зображення для кодоскопа тощо, ніж використовувати ЗВН чи інші навчальні мультимедійні програми. *

- Згоден (-на).
- Важко відповісти.
- Не згоден (-на).

Чи вмієте виконувати при розробці засобів віртуальної наочності наступні етапи роботи? *

	Так	Ні
У відібраній для ЗВН навчальній інформації виділяти головну та структурувати її		
Відбирати з навчального матеріалу той, який потрібно наочно демонструвати в ЗВН		
Редагувати для даного ЗВН потрібну текстову інформацію		
Редагувати для даного ЗВН потрібну графічну інформацію		
Продумувати сценарій ЗВН		
Редагувати для даного ЗВН потрібні звукові файли		
Розробляти дизайн ЗВН		
Редагувати для даного ЗВН потрібні відеофайли		

Таким чином, нами розроблено платформу для наукової та навчальної діяльності з використанням хмарних технологій, основні ознаки та властивості яких нами описані в [1], і ми вбачаємо значні перспективи у подальшому її використанні у організації дистанційного навчання [2].

Джерела

1. Войтович І.С. Перспективи використання «cloud computing» у навчальній діяльності педагогічних університетів / Сергієнко В.П., Войтович І.С. // Науковий часопис НПУ імені М.П.Драгоманова. Серія 2. Комп'ютерно–орієнтовані системи навчання: зб.наук.праць / Редрада. – К.: НПУ імені М.П. Драгоманова, 2011. – № 10 (17). – С. 58 – 63.
2. Войтович І.С. Створення навчальних ресурсів у середовищі moodle на основі технології «cloud computing» / Сергієнко В.П., Войтович І.С. // Інформаційні технології і засоби навчання. / Том 24, № 4 (2011). – Режим доступу: http://journal.iitta.gov.ua/index.php /itlt/article/view/518.

Навчання криптології з використанням вільно поширюваного програмного абезпечення

Загацька Н. О.

Житомирський державний університет імені Івана Франка, thalitana@gmail.com

The paper describes the open source and e-learning software for information resources security. The considerable attention is given to using CrypTool and GNU Privacy Guard in the course of Cryptology training. It can be used as a teaching tool to demonstrate the working principles of cryptographic algorithms related to data encryption, digital signature, hash functions and other.

Навчання дисципліни «Криптологія» має на меті формування професійних компетентностей у майбутніх фахівців в галузі інформатики через їх ознайомлення із загальними принципами побудови та використання криптографічних алгоритмів захисту даних, а також розвиток у них навичок розв'язання практичних завдань із застосуванням сучасних криптографічних методів. Такі методи передбачають перетворення даних, при якому ті стають доступними для прочитання лише власникові деякого секретного параметра (ключа).

Для забезпечення кращої ефективності навчання студентів спеціальності «Інформатика» пропонується використовувати вільно поширюване програмне забезпечення із захисту інформаційних ресурсів, що сприятиме різнобічному і змістовному вивченню відповідної предметної галузі, відкриє нові пізнавальні можливості та перспективи для підвищення рівня знань студентів, допоможе їм легко засвоїти складні принципи та технології криптографічних перетворень на практиці.

Метою дослідження є огляд вільно поширюваних засобів для навчання дисципліни «Криптологія» майбутніх фахівців з інформатики.

CrypTool [1] – найпоширеніший в області криптології безкоштовний програмний засіб з відкритим вихідним кодом. Його розробка почалася у 1998 році за співробітництва «Дойче банк» (нім. Deutsche Bank) та декількох німецьких університетів. CrypTool має простий графічний інтерфейс та зручне меню, за допомогою якого користувач може у робочій області програми шифрувати повідомлення з використанням симетричних, асиметричних та змішаних алгоритмів, виконувати процедури створення та перевірки електронного цифрового підпису, обчислювати хеш-значення документу тощо. CrypTool передбачає вивчення математичного апарату криптології, оскільки більшість криптографічних алгоритмів ґрунтуються на математичних поняттях та обчисленнях.

Значною перевагою CrypTool є також широкий діапазон анімації криптографічних перетворень. Під час проведення лекції на тему «Симетричні шифри» пропонується розглянути найпопулярніший симетричний блоковий алгоритм AES (Rijndael) [2, с. 75], що з 2002 року є державним стандартом шифрування США і складається з 10 раундів. За допомогою CrypTool студентам можна детально продемонструвати етапи кожного раунду: підстановку байтів, зсув рядків, перемішування стовпців (у 10-му раунді пропускається), додавання з раундовим ключем (рис. 1). Зауважимо, що схема утворення вхідних блоків шифрування та ключових елементів є досить складною, тому наочне представлення та покрокова візуалізація алгоритму AES забезпечить ефективне сприйняття студентами навчального матеріалу теми.

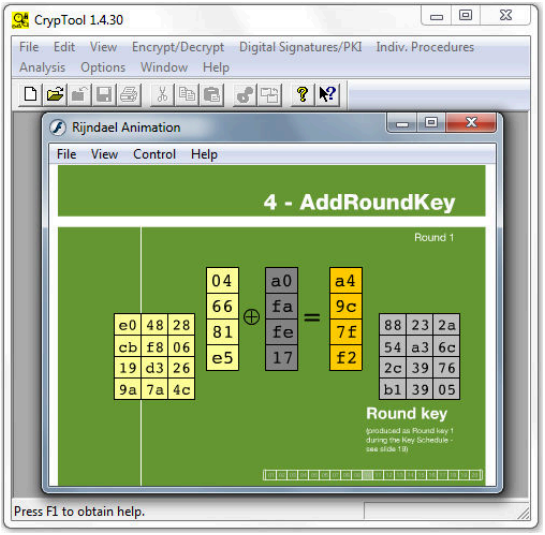

Рис.1. CrypTool-анімація етапу додавання бітів вхідного блоку з раундовим ключем у шифрі AES

GNU Privacy Guard, **GnuPG** [3] – вільно поширюване програмне забезпечення, що використовує криптографію з відкритим ключем. Перша версія проекту, створена Вернером Кохом (нім. Werner Koch) та профінансована німецьким урядом, вийшла в світ у 1999 році під ліцензією GNU General Public. Шифрування повідомлень проводиться шляхом використання пари ключів – закритого (секретного) та відкритого (публічного), які математично пов'язані один з одним. Відкритий ключ генерується із закритого ключа і може бути доступним будь-якому учаснику процесу інформаційного обміну. Повідомлення зашифровується за допомогою відкритого ключа, що доступний усім бажаючим, а дешифрується за допомогою закритого ключа, відомого тільки одержувачу. Також можливості GnuPG дають змогу підписувати повідомлення за допомогою електронного цифрового підпису з метою перевірки цілісності даних та достовірності авторства.

Звичним інтерфейсом для GnuPG є командний рядок, проте на сьогоднішній день існують різні зовнішні оболонки, які роблять доступною функціональність цієї програми через графічний інтерфейс користувача, наприклад GPGShell для Windows або GNU Privacy Assistant (GPA) для Linux.

Під час проведення заняття у вигляді лабораторної роботи на тему «Асиметричні та комбіновані алгоритми шифрування» для кращого розуміння досить складного поєднання симетричних та асиметричних алгоритмів студентам пропонується виконати ряд завдань за допомогою програмного забезпечення GnuPG.

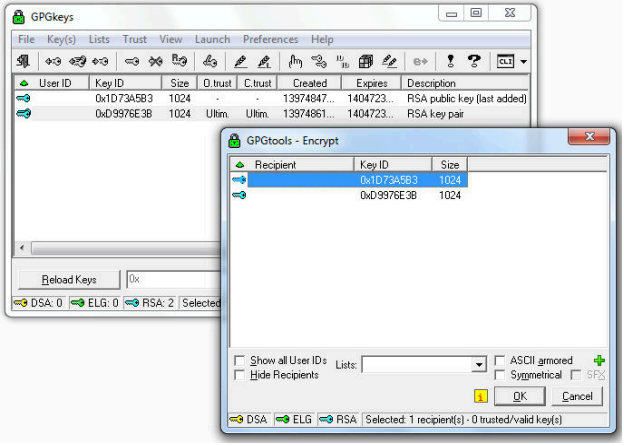

Рис.2. Зашифрування повідомлення за допомогою GnuPG

Студент та викладач окремо один від одного можуть створити власну пару ключів у діалоговому вікні GPGkeys за допомогою меню Key(s)⇒New. Закритий ключ та відкритий ключ – це два великі числа, обчислені на основі деякого асиметричного алгоритму, наприклад RSA [4, с.351]. Студент та викладач обмінюються один з одним відкритими ключами та додають їх до середовища GnuPG. Для цього у вікні GPGkeys за допомогою меню Key(s) потрібно обрати команди Import або Export.

Перед студентами постає завдання зашифрувати деякий документ, використовуючи відкритий ключ викладача. Для виконання цього завдання, у контекстному меню документа потрібно обрати пункт GPGShell та підпункт Encrypt (рис. 2).

Крім того, невидимо для ока користувача, GnuPG створює ще один так званий сеансовий ключ – це псевдовипадкове число, яке генерується на основі випадкових рухів миші, натискань клавіш клавіатури. Такий ключ використовується лише один раз для шифрування повідомлення з використанням деякого надійного та швидкого симетричного алгоритму. Сеансовий ключ зашифровується відкритим ключем одержувача та додається до шифротексту.

Зашифрований документ студент відправляє викладачу. У разі правильного виконання студентом вище описаного завдання, викладач успішно прочитає зашифроване повідомлення. Під час дешифрування усі дії будуть виконуватися у зворотному порядку. За допомогою свого закритого ключа викладач дешифрує сеансовий ключ, який в свою чергу використовується для дешифрування отриманого повідомлення. Повна схема комбінованого алгоритму шифрування з використанням GnuPG представлена на рис. 3.

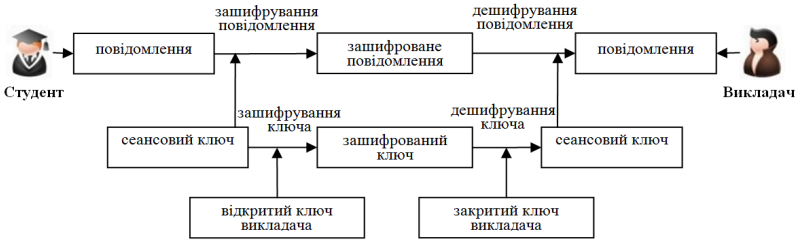

Рис.3. Схема комбінованого алгоритму шифрування

Отже, використання вільно поширюваного програмного забезпечення із захисту інформаційних ресурсів у процесі навчання криптології може використовуватись з метою ознайомлення студентів з додатковими теоретичними відомостями, закріплення набутих знань та умінь, проведення лабораторних робіт, поглиблення міжпредметних зв'язків, підготовки студентів до проектування та розробки власного криптографічного програмного забезпечення.

Література

1. Огляд різних версій пакету CrypTool як засобу захисту інформаційних ресурсів./ Н. О. Загацька // Інформаційні технології і засоби навчання: електронне наукове фахове видання [Електронний ресурс] / Ін-т інформ. технологій і засобів навчання АПН України, Ун-т менеджменту освіти АПН України; гол. ред.: В. Ю. Биков. – 2012. – № 5(31). – Режим доступу : http://journal.iitta.gov.ua/index.php/itlt/article/view/744/548
2. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер; [пер. с англ. Н.Н. Селиной]. – М.: «Диалектика», 2004. – 432 с.
3. GnuPG [Електронний ресурс]. – Режим доступу: http://www.gnupg.org
Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М.: Триумф, 2002. – 816 с.

Zabbix — система моніторингу IT-інфраструктури

Сало М, Жгута В.
"Uk2Group", michaels@uk2group.com, vitaliyz@uk2group.com

Zabbix is the ultimate enterprise-level software designed for monitoring availability and performance of IT infrastructure components. Zabbix is open source and comes at no cost.

IT-інфраструктура сучасного підприємства чи компанії є складною інформаційною системою. Дуже важливо не допустити збоїв та простоїв у роботі суттєвих для бізнесу сервісів, тому що це може спричинити зниження прибутку та погіршення рівня обслуговування клієнтів.

Як відомо, клієнт зацікавлений в якісному і безперебійному сервісі, і його мало хвилюють технічні деталі, які виникають. Забезпечуючи мінімальну кількість збоїв в роботі, або їх повну відсутність за