Основні методичні вимоги до організації компетентнісно-орієнтованого змісту навчання інформатичних дисциплін майбутніх фахівців із документознавства – це спрямованість на формування науково-технічної, інформаційно-управлінської, інформаційно-комунікаційно-технологічної компетентностей всіх складових навчального процесу шляхом встановлення міждисциплінарних зв'язків; навчання перенесенню набутих теоретичних знань у простір їх безпосереднього використання з максимальним наближенням до реальної професійної діяльності та із застосуванням інформаційно-комунікаційних технологій і систем електронного документообігу; дотримання принципів розробки та використання завдань компетентнісного характеру з визначенням їх призначення та місця у навчальному процесі.

Література

1. Будапештсько-Віденська декларація про створення Європейського простору вищої освіти (від 12 березня 2010 року) [Електрон. ресурс]. – Режим доступу : http://22school.at.ua/news/budapeshtsko_videnska_deklaracija_pro_stvorennja_evropejskogo_prostoru_vishhoji_osviti/2010-03-17-6.
2. Державна національна програма «Освіта» (Україна XXI століття). – К. : Освіта, 1993. – 24 с.
3. Жалдак М.І. Модель системи соціально-професійних компетентностей вчителя інформатики / М. І. Жалдак // Науковий часопис НПУ ім. М. П. Драгоманова. Серія №2. Комп'ютерно-орієнтовані системи навчання : Зб. наук. праць / Редрада. – К. : НПУ ім. М. П. Драгоманова, 2009. – №14. – С. 5-12.
4. Коканова Р.А. Дидактическая модель формирования профессиональной компетентности специалиста в области электронного документооборота в современном вузе : дис. … кандидата пед. наук : 13.00.08 / Рауза Абдришевна Коканова. – Великий Новгород, 2008. – 189 с.
5. Матвієнко О.В. Документознавча освіта: проблеми та перспективи розвитку практики та наукових досліджень / О. В. Матвієнко // Бібліотекознавство. Документознавство. Інформологія. – 2009. – №4. – С. 17-21.
6. Морзе Н.В. Компетентнісні завдання як засіб формування інформатичної компетентності в умовах неперервної освіти / Н. В. Морзе, О. Г. Кузьмінська, В. П. Вембер, О. В. Барна // Інформаційні технології в освіті : Зб. наукових праць. – Херсон : Видавництво ХДУ. – 2010. – Вип. 6. – С. 23-31.
7. Сивак О.А. Формування професійних компетентностей майбутніх документознавців у процесі навчання інформатичних дисциплін : дис. ... на здоб. наук. ступ. канд. пед. наук : спец. 13.00.04 «Теорія і методика професійної освіти» / О.А. Сивак. – Бердянськ, 2014. – 172 с.

Загацька Н.О.
Житомирський державний університет імені Івана Франка

Застосування програмного засобу CrypTool 2 у підготовці фахівців з інформатики до вивчення класичних алгоритмів шифрування

Сучасні інформаційно-комунікаційні технології (ІКТ) інтенсивно впроваджуються в усі сфери людського життя. Інформаційні ресурси стають головною цінністю наукового, економічного та технічного розвитку суспільства, будь-якої галузі діяльності людей. При цьому великого значення набуває проблема захисту даних, що полягає у забезпеченні їх конфіденційності, цілісності та вірогідності під час зберігання, опрацювання та передавання. Постає стратегічно важливе питання якості підготовки вищими навчальними закладами майбутніх фахівців з інформатики, які б у своїй діяльності ефективно використовували різноманітні методи захисту повідомлень даних, зокрема криптографічних. Криптографія займається розробкою алгоритмів перетворення повідомлень, в тому числі шляхом шифрування з використанням спеціальних (ключових) даних. Дослідженням вразливих місць таких алгоритмів та розробкою методів зламу зашифрованих повідомлень займається криптоаналіз. Ці два наукових напрями тісно пов'язані між собою і разом складають науку криптологію.

Актуальність використання ІКТ у процесі навчання криптології, обумовлена тим, що збільшується обсяг і змінюється зміст знань, умінь і навичок, якими повинні володіти майбутні фахівці з інформатики. У ході підготовки студентів виникає необхідність реформування освітнього процесу вищої школи, що полягає у перегляді методів, форм та засобів навчання фахових дисциплін. Типовий лекційний курс з криптології включає в себе теоретичні та математичні аспекти криптографічних алгоритмів. Практичні роботи переважно присвячені розв'язуванню вправ з теорії чисел, оскільки багато понять цього розділу математики лежать в основі науки про шифри. Завдання до лабораторних робіт часто полягають у програмній реалізації алгоритмів шифрування або методів їх криптоаналізу. Однак поглиблене вивчення математичних основ криптології та вдосконалення

навичок програміста не достатньо відповідає вимогам до висококваліфікованого фахівця з інформатики. До того ж складність програмування деяких сучасних криптоалгоритмів вимагає наявності значної кількості академічних годин, що обмежує час для вивчення багатьох інших важливих понять курсу. Застосування ІКТ у процесі навчання криптології та поєднання їх з традиційними методами навчання по-перше, дасть можливість викладачеві під час пояснення нового матеріалу на лекційних заняттях демонструвати студентам покрокову візуалізацію роботи криптографічних алгоритмів; по-друге, допоможе значно розширити діапазон завдань до практичних та лабораторних робіт; по-третє, сприятиме збільшенню обсягу навчального матеріалу за рахунок економії часу.

Розгляду комплексу питань, пов'язаних із використанням сучасних ІКТ у навчальному процесі середньої та вищої школи присвячені праці В. Ю. Бикова, М. І. Жалдака [1], Н. В. Морзе, О. М. Спіріна, Ю. В. Триуса та багатьох інших. Теоретичні та методичні аспекти підготовки фахівців у галузі захисту інформаційних ресурсів висвітлені у дослідженнях В. П. Бабака, О. Л. Голубенка, Г. Ю. Маклакова, В. В. Козловського, М. Г. Коляди [2], В. М. Полякова, В. О. Хорошко та інших дослідників. Проблеми захисту інформаційних ресурсів за допомогою криптографічних методів розглядали І. Д. Горбенко [3], В. К. Задірака, І. І. Маракова , А. І. Рибак, Ю. С. Ямпольський та інші. Однак значно менше уваги приділено питанням застосування спеціалізованого програмного забезпечення, зокрема засобу CrypTool 2, у процесі навчання криптології.

В даній статті розглядаються питання, що стосуються дослідження основних засад застосування програмного засобу CrypTool 2 у підготовці фахівців з інформатики до вивчення класичних алгоритмів шифрування, розробки та опису методики проведення лабораторних робіт з дисципліни «Криптологія» на тему «Класичні шифри та їх криптоаналіз».

Аналіз досвіду провідних країн Європи із використання ІКТ у процесі навчання криптології показав, що ефективним у підготовці майбутніх фахівців з інформатики є середовище CrypTool 2 [4, 5]. CrypTool 2 – безкоштовне програмне забезпечення з відкритим вихідним кодом, де реалізується концепція візуального програмування та виконання каскадів криптографічних процедур [6]. CrypTool 2 є однією із складових великого проекту CrypTool [7], призначеного в першу чергу для навчання криптографії та криптоаналізу. Програмний засіб CrypTool 2 (рис. 1) на даний час доступний німецькою та англійською мовами, оснащений інтуїтивно зрозумілим сучасним графічним інтерфейсом та зручним меню, за допомогою якого користувач у робочому полі програми може перетворювати повідомлення з використанням найвідоміших криптографічних алгоритмів.

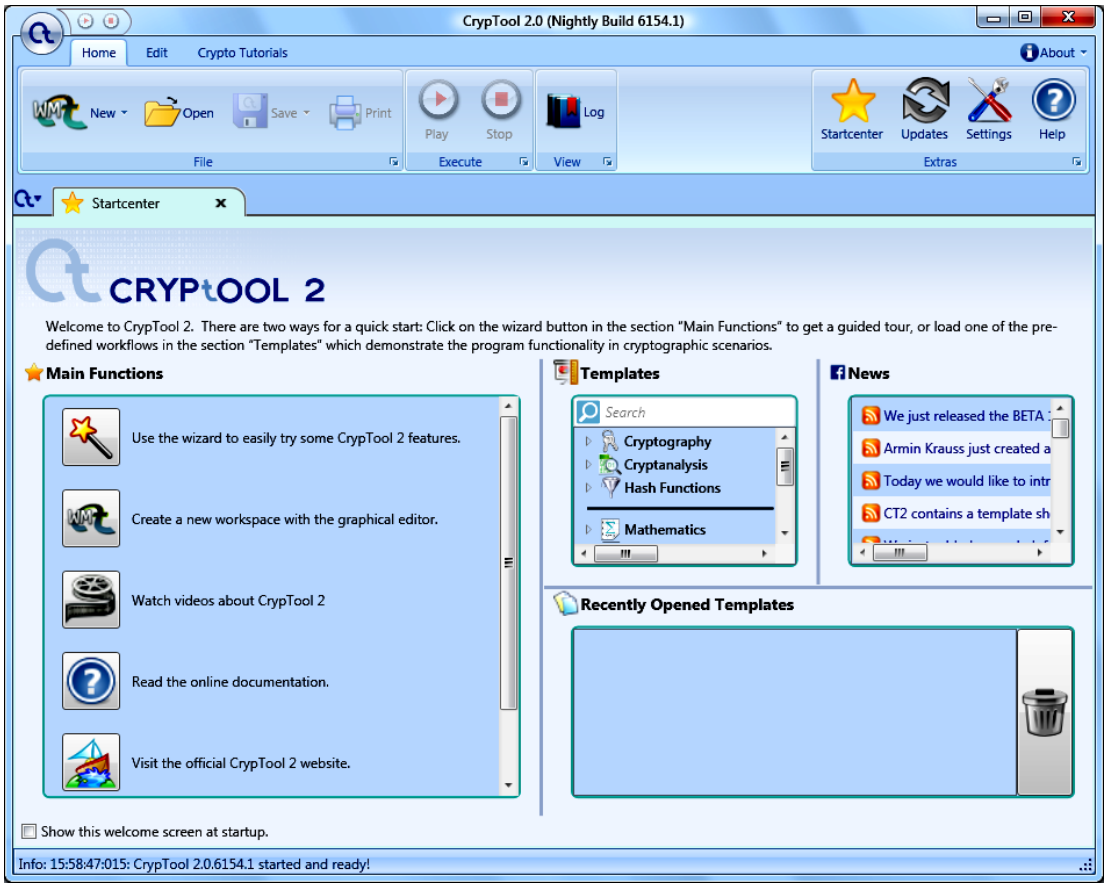

Рис. 1

Особливістю CrypTool2 є модульна конструкція, в якій пропонується набір інструментів, які можуть бути об'єднані в нові проекти для реалізації роботи криптографічних алгоритмів. Це дає змогу викладачеві реалізовувати індивідуальний підхід в навчанні, готувати завдання, виконання яких на практичних та лабораторних заняттях найкраще сприятиме досягненню цілей навчання.

CrypTool2 відповідає усім дидактичним та методичним вимогам, оскільки створювався в першу чергу як навчальний засіб, що призначений для більш широкого, наочного і доступного подання навчального матеріалу з криптології; використання якого дозволяє підвищити пізнавальну активність студентів за рахунок комп'ютерного моделювання процесу шифрування; розвинути мотивацію до навчання під час розв'язування професійних завдань; розширити можливості для творчої діяльності, особливо під час дослідження і систематизації навчального матеріалу; забезпечити активну взаємодію викладача зі студентами та студентів між собою; посилити міжпредметні зв'язки криптології з такими дисциплінами як алгебра та теорія чисел, теорія ймовірності та математична статистика, комп'ютерні мережі, захист повідомлень в телекомунікаційних системах, математична теорія телекомунікацій та кодування повідомлень.

Розглянемо приклад лабораторної роботи з криптології на тему *«Класичні шифри та їх криптоаналіз»*. Метою цієї роботи є вивчення студентами принципів побудови класичних алгоритмів шифрування та методів частотного криптоаналізу, набуття вмінь та навичок із зашифрування, дешифрування, зламу кодів повідомлень на прикладі шифру моноалфавітної заміни, зокрема алгоритму Цезаря. Зміст лабораторного заняття полягає у створенні проектів із окремих модульних компонентів, за допомогою яких реалізують роботу відповідних криптоалгоритмів та методів у середовищі CrypTool 2. Кінцевим результатом навчання повинні стати сформовані на основі здобутих знань, вмінь і навичок, пізнавальні, навчальні, професійні, інформаційно-комунікаційні та інші компетентності.

Попередня підготовка до лабораторної роботи полягає у ознайомленні студентів із теоретичними відомостями з метою поглиблення, розширення та уточнення знань, здобутих на лекціях та в процесі самостійної роботи. Студенти повинні володіти такими поняттями як шифр моноалфавітної заміни, знати алгоритм перетворення повідомлень за шифром Цезаря.

Шифр заміни – це шифр, у якому символи тексту замінюються символами того самого або іншого алфавіту згідно із заздалегідь встановленим правилом. У шифрі моноалфавітної заміни кожній конкретній літері повідомлення відповідає єдина, завжди одна і та сама, літера шифротексту. Цей алгоритм шифрування на сьогоднішній день є нестійким до зламу і не використовується на практиці, проте є важливим для вивчення. Оскільки відомо, що навіть дуже складні сучасні криптосистеми в якості типових складових використовують прості шифри заміни.

Одним з найдавніших та найбільш поширених шифрів моноалфавітної заміни є шифр Цезаря [8, с. 12]. У цьому шифрі кожна літера повідомлення зсувається в алфавіті на K позицій вперед від символу, що замінюється. При досягненні кінця алфавіту виконується циклічний перехід до його початку. За необхідності розділові знаки та пробіли ігноруються. Отже, ключем шифрування є деяке фіксоване секретне число K – від 1 до 25 для англійського (латинського) алфавіту та K – від 1 до 33 для українського. Сам Цезар використовував ключ K=3, тобто відбувався зсув символів повідомлення на три позиції вперед у латинському алфавіті (рис. 2). Під час дешифрування літера зашифрованого тексту замінюється на літеру, розташовану в алфавіті на K позицій раніше.

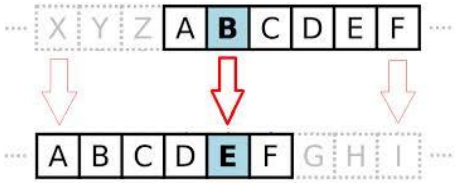

Рис. 2

Водночас із вмінням шифрувати повідомлення студентам необхідно опанувати навички зламу шифрів повідомлень з використанням методів криптографічного аналізу. Криптоаналіз шифру Цезаря ґрунтується на частотному аналізі появ окремих символів природньої мови у тексті. Частота символу у повідомленні дорівнює кількості його появи у тексті, поділеній на загальну кількість літер тексту. Для кожної мови виявляється, що у досить довгих текстах кожна літера зустрічається із приблизно однаковою частотою, залежно від самої літери і незалежно від конкретного тексту [9, с. 20]. Тобто імовірність появи окремих літер, а також їх порядок у словах і фразах природної мови підпорядковуються статистичним закономірностям. Так, наприклад, відомо, що в українській, російській та англійській мовах частоти появи літер розподілені наступним чином (табл. 1):

Таблиця 1

Українська мова						Російська мова						Англійська мова					
А	0,072	Ї	0,006	У	0,04	А	0,062	Л	0,035	Ц	0,004	A	0,081	J	0,001	S	0,066
Б	0,017	Й	0,008	Ф	0,001	Б	0,014	М	0,026	Ч	0,012	B	0,016	K	0,005	T	0,096
В	0,052	К	0,035	Х	0,012	В	0,038	Н	0,053	Ш	0,006	C	0,032	L	0,040	U	0,031
Г, Ґ	0,016	Л	0,036	Ц	0,006	Г	0,013	**О**	**0,09**	Щ	0,003	D	0,036	M	0,022	V	0,009
Д	0,035	М	0,031	Ч	0,018	Д	0,025	П	0,023	Ь, Ъ	0,014	**E**	**0,123**	N	0,072	W	0,020
Е	0,017	Н	0,065	Ш	0,012	Е, Ё	0,072	Р	0,04	Ы	0,016	F	0,023	O	0,079	X	0,002
Є	0,008	**О**	**0,094**	Щ	0,001	Ж	0,007	С	0,045	Э	0,003	G	0,016	P	0,023	Y	0,019
Ж	0,009	П	0,029	Ь	0,029	З	0,016	Т	0,053	Ю	0,006	H	0,051	Q	0,002	Z	0,001
З	0,023	Р	0,047	Ю	0,004	И	0,062	У	0,021	Я	0,018	I	0,071	R	0,0060		
И	0,061	С	0,041	Я	0,029	Й	0,021	Ф	0,002								
І	0,057	Т	0,055			К	0,028	Х	0,009								

Отже, літера з найбільшою частотою в шифротексті буде замінюватися на літеру з найбільшою частотою у мові. А кількість позицій між ними буде визначати довжину ключа. Однак, якщо текст не дуже великий, то закономірності будь-якої природної мови можуть проявлятися в ньому не обов'язково в строгій відповідності з таблицею частот. В такому випадку розглядається відношення наступної літери за частотою появи у зашифрованому тексті та найчастішою літерою мови.

Матеріально-технічне забезпечення до лабораторної роботи складається з: комп'ютер зі встановленим програмним забезпеченням CrypTool 2, інструкції до лабораторної роботи, текстові повідомлення для шифрування згідно варіанту, контрольно-тестові програми.

Виконання лабораторної роботи відбувається за такими етапами:

1. Доцільно поділити студентів на ротаційні групи з трьох чоловік: СТУДЕНТ-ВІДПРАВНИК, СТУДЕНТ-ОТРИМУВАЧ, СТУДЕНТ-КРИПТОАНАЛІТИК, та організувати обмін повідомленнями між учасниками за схемою (рис. 3), в основі якої лежить секретна система зв'язку, описана Клодом Шеноном (*Claude Shannon*) [10, с. 18]. Слід звернути увагу студентів на те, що у середовищі CrypTool 2 не потрібно використовувати вже готові шаблони криптографічних алгоритмів, а необхідно створювати свої власні проекти із окремих компонентів.

Рис. 3

2. СТУДЕНТ-ВІДПРАВНИК за допомогою шифру Цезаря у середовищі CrypTool 2 повинен зашифрувати текст, отриманий згідно відповідного варіанту. Для цього він створює проект під назвою *Ceasar_enc.cwm* з модульних компонентів «Text Input», «Caesar», «Text Output» та «File Output», встановлює між ними зв'язки, налаштовує їх параметри (вхідний алфавіт, довжину ключа, режим шифрування тощо). Після виконання проекту, зашифрований текст із середовища CrypTool 2 необхідно вивести до текстового файлу та відправити його адресату – СТУДЕНТУ-ОТРИМУВАЧУ.

Наприклад, зашифруємо повідомлення *«Шукаємо щастя в країнах, століттях, а воно скрізь і завжди з нами; як риба в воді, так і ми в ньому, і воно біля нас шукає нас самих. Нема його ніде від того, що воно скрізь. Григорій Сковорода»*, використовуючи шифр Цезаря з ключем 10. Для цього у середовищі CrypTool 2, на панелі компонентів «Components» у розділі «Tools» обираємо поле «Text Input» для введення тексту повідомлення з клавіатури. Далі визначимо, потрібний алгоритм шифрування, виконавши послідовність дій «Components»⇒«Classic Ciphers»⇒«Caesar». Налаштуємо параметри перетворення вікна «Caesar»: дія – шифрувати, ключ – 10, алфавіт – А, Б,…, Я (український), ігноруємо розділові знаки та пробіли. Забезпечимо виведення зашифрованого тексту до поля «Text Output» та до текстового файлу «File Output». Встановимо за допомогою стрілок зв'язки між кожним компонентом програми. Збережемо проект, використовуючи опцію «Save». Для отримання зашифрованого тексту (рис. 4) натиснемо «Play».

Рис. 4

3. СТУДЕНТ-ОТРИМУВАЧ, який одержав файл із зашифрованим текстом та заздалегідь таємно узгодив із СТУДЕНТОМ-ВІДПРАВНИКОМ довжину ключа шифрування, у середовищі CrypTool 2, аналогічно до попереднього завдання, із окремих компонентів «Text Input», «Caesar», «Text Output» створює проект *Ceasar_dec.cwm* для дешифрування повідомлення. Результатом правильного виконання роботи буде коректно дешифроване повідомлення від СТУДЕНТА-ВІДПРАВНИКА.

Дешифруємо повідомлення із вище описаного прикладу. Створимо проект із компонентів, де передбачається введення тексту, шифрування за алгоритмом Цезаря та виведення розшифрованого тексту, налаштуємо зв'язки між ними (рис. 5). У параметрах налаштування алгоритму Цезаря оберемо: дію – дешифрувати, ключ – 10, український алфавіт. Скопіюємо текст повідомлення до поля «Text Input». Після натискання «Play» шифротекст із розглянутого вище прикладу перетвориться до початкового вигляду.

4. У криптології передбачається, що стійкість зашифрованого повідомлення забезпечується в першу чергу через ключ. Припускається, що сам алгоритм шифрування та шифротекст є відомими зловмиснику. Тому СТУДЕНТ-КРИПТОАНАЛІТИК, маючи доступ до зашифрованого повідомлення, повинен зламати його, використовуючи частотний криптоаналіз. Для цього за допомогою CrypTool 2, у своєму проекті *Ceasar_analisys.cwm* СТУДЕНТУ-КРИПТОАНАЛІТИКУ потрібно використати компонент «Frequency Test». На основі частоти появи літер у шифротексті обчислюється ключ шифрування. При правильному налаштуванні роботи усіх компонентів проекту та зв'язків між ними, із використанням дібраного ключа СТУДЕНТ-КРИПТОАНАЛІТИК відновлює повідомлення.

Наприклад, нехай вдалося перехопити, на перший погляд, незрозумілу послідовність символів «*Еафінцш єіюяи щш фьітчів, юяшхсяяив, і йшчш юфьспж с пійолр п чіцр; иф ьрії й йшлс, яіф с цр й чжшца, с йшчш їсхи чію еафін чію юіцрв. Чмці ушкш чслм йсл яшкш, єш йшчш юфьспж. Кьркшьсу Юфшйшьшлі*». У середовищі CrypTool 2 створимо поле «Text Input» та додамо до нього отримані дані.

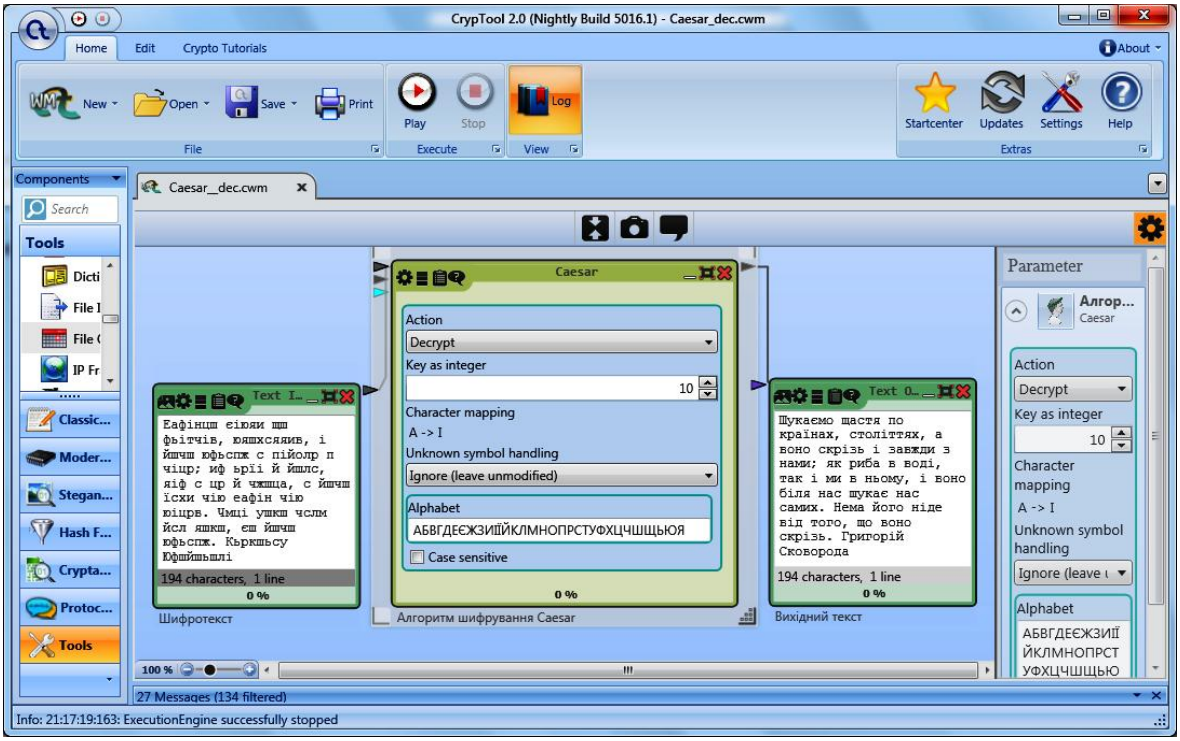

Рис. 5

Обчислимо частоти появи літер в шифротексті за допомогою інструменту «Frequency Test», що знаходиться на панелі компонентів «Components» у розділі «Cryptanalysis». Бачимо, що найчастіше у тексті з'являється літера «Ш» – 12,7 % (рис. 6). З табл. 1 видно, що найчастіше в текстах українською мовою зустрічається літера «О». Тому можемо припустити, що літері «Ш» в шифротексті, ймовірно, відповідає літера «О» у початковому тексті. Якщо впорядкований набір літер А, Б,…, О,…, Ш,…, Я ототожнити із впорядкованим набором їх позицій в алфавіті 0, 1,…, 17,…, 27,…, 33, то можна обчислити ключ K: 27–17=10. Тепер можна дешифрувати текст, використавши компонент «Caesar» і отримати початкове повідомлення: «Шукаємо щастя в країнах, століттях, а воно скрізь і завжди з нами; як риба в воді, так і ми в ньому, і воно біля нас шукає нас самих. Нема його ніде від того, що воно скрізь».

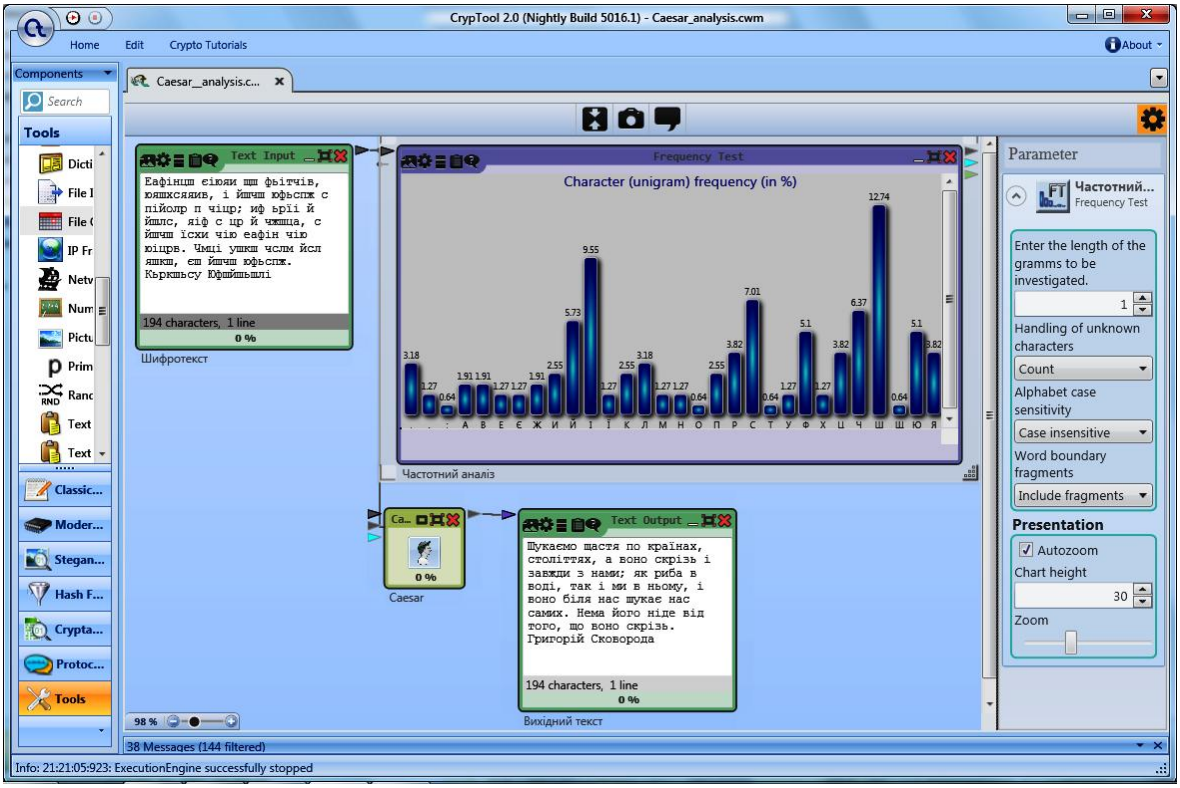

Рис. 6

Таким чином кожен студент повинен виконати всі три завдання, подати викладачеві для оцінювання проекти *Ceasar_enc.cwm, Ceasar_dec.cwm* та *Ceasar_analisys.cwm*, проаналізувати отримані результати, зробити висновки про взаємодію учасників інформаційного обміну, усвідомити особливості криптографічних методів шифрування та аналізу зашифрованих повідомлень, встановити відношення між поняттями, що вивчаються, на основі використовуваних модульних компонентів середовища CrypTool 2.

Під час підрахунку балів оцінювання підлягають: рівень знань, необхідний для виконання лабораторної роботи, повнота, якість та вчасність її виконання. Також з метою контролю засвоєння знань та вмінь студентами наприкінці лабораторної роботи доцільно провести співбесіду або комп'ютерне тестування для з'ясування рівня засвоєння знань теоретичного матеріалу та основних понять класичної криптології.

Отже, як свідчить практика, впровадження та застосування у процес навчання криптології програмного засобу CrypTool 2 сприятиме підвищенню ефективності навчального процесу, забезпечить можливості розв'язування широкого кола задач з криптології, в тому числі за створеною студентом комп'ютерною моделлю. Очевидно, що дії шифрування та зламу шифру можна виконати вручну, проте це значно збільшить витрати часу на розв'язування задач. До того ж результати ручного шифрування або зламу шифру довгого тексту можуть містити багато неточностей і помилок.

Перспективи дослідження полягають у детальному розгляді можливих шляхів впровадження спеціалізованого програмного забезпечення у процес навчання криптології, розробці та описі методів, прийомів та засобів його застосування при підготовці фахівців з інформатики до захисту інформаційних ресурсів, що сприятиме підвищенню пізнавального інтересу студентів до дисципліни, формуванню їх готовності до подальшої навчальної та професійної діяльності.

Література

1. Жалдак М. І. Проблеми інформатизації навчального процесу в середніх і вищих навчальних закладах/ М. І. Жалдак // Комп'ютер у школі та сім'ї. – 2013. – №3. – С. 8-15.
2. Коляда М. Г. Концептуальні методологічні підходи в професійній підготовці майбутніх фахівців в галузі інформаційної безпеки. [Електронний ресурс] / М. Г. Коляда // Інформаційні технології в освіті. – 2009. – № 3. – Режим доступу: http://ite.kspu.edu/webfm_send/507
3. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І. Д. Горбенко, Ю. І. Горбенко; Харк. нац. ун-т радіоелектрон., Приват. АТ «Ін-т інформ. Технологій». – Х.: Форт, 2012. – 868 с.
4. Sibylle Hick. Reducing the complexity of understanding cryptology using CrypTool [Електронний ресурс] / Sibylle Hick, Bernhard Esslinger, Arno Wacker. – Режим доступу: http://www.iiis.org/CDs2012/CD2012SCI/EISTA_2012/PapersPdf/EA678TR.pdf
5. Kulwinder Kaur. Performance evaluation of ciphers using CrypTool 2.0 [Електронний ресурс] / Kulwinder Kaur // International journal of computers & technology. – Режим доступу: http://cirworld.org/journals/index.php/ijct/article/view/426/78
6. About CrypTool 2 [Електронний ресурс]. – Режим доступу: http://www.cryptool.org/en/cryptool2
7. Загацька Н. О. Огляд різних версій пакету CrypTool як засобу захисту інформаційних ресурсів. [Електронний ресурс] / Н. О. Загацька // Інформаційні технології і засоби навчання. – 2012. – № 5(31). – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/article/view/744/548
8. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. – М. : Солон-Пресс, 2002. – 511 с.
9. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький – Л.: ВНТЛ, 1998. – 247 с.
10. Аграновский А. В. Практическая криптографія: алгоритмы и их програмирование / А. В. Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2009. – 256 с.

Твердохліб І.А.
Національний педагогічний університет імені М.П. Драгоманова

Навчання фізико-технічних дисциплін майбутніх вчителів інформатики з використанням комп'ютерного моделювання

Розвиток інформаційно-комунікаційних технологій і масове їх впровадження в навчальний процес школи та ВНЗ стимулюють активний розвиток щодо нового методу пізнання – комп'ютерного моделювання. Його використання в навчальному процесі дає змогу виконувати моделювання реальних технічних пристроїв, не вимагає значних затрат часу та матеріальних ресурсів, а в деяких випадках дає змогу змоделювати роботу технічних пристроїв, розробка чи дослідження яких в реальних навчальних лабораторіях взагалі неможлива.