©Н.О.Загацька, 2012
ISSN 2076-8184. Інформаційні технології і засоби навчання. 2012. №5 (31).
Режим доступу до журналу: http://www.journal.iitta.gov.ua

УДК 378:004.056.55

Загацька Наталія Олександрівна, аспірантка кафедри прикладної математики та інформатики Житомирського державного університету імені Івана Франка, м. Житомир, e-mail: thalitana@gmail.com

ОГЛЯД РІЗНИХ ВЕРСІЙ ПАКЕТА CRYPTOOL ЯК ЗАСОБУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анотація

У статті описуються характерні особливості вільно поширюваного програмного забезпечення із захисту інформаційних ресурсів CrypTool, що поєднує у собі ефективну реалізацію відомих алгоритмів шифрування та їх візуальне подання. Приділено значну увагу застосуванню такого програмного забезпечення у процесі навчання дисципліни «Криптологія», що дає змогу оглянути широке коло питань із захисту інформаційних ресурсів. Проведено детальний огляд і порівняльний аналіз усіх наявних версій цього програмного засобу, серед яких виділено найефективніші щодо реалізацій алгоритмів шифрування та зручності інтерфейсу.

Ключові слова: криптологія, криптографія, криптоаналіз, програмний засіб, шифрування.

Постановка проблеми. В епоху розвитку інформаційно-комунікаційних технологій (ІКТ) основи криптографічного захисту інформації та застосування їх на практиці є дуже важливим питанням для вивчення у підготовці сучасного фахівця з інформатики.

Криптологія — наука, яка складається з двох напрямів: криптографії та криптоаналізу. Криптографія — наука про способи перетворення (шифрування) повідомлень з метою їх захисту від незаконних користувачів. Криптоаналіз — наука (і практика її застосування) про методи та способи зламування шифрів [1, с. 22].

У процесі навчання дисципліни «Криптологія» найчастіше перед студентами ставиться завдання зі створення програмної оболонки алгоритмів шифрування (дешифрування) або інструментів криптоаналізу. Складність програмування деяких криптоалгоритмів вимагає наявності значної кількості академічних годин, що обмежує час для вивчення багатьох інших важливих понять і питань курсу.

Для забезпечення кращої ефективності навчання пропонується використовувати вільно поширюване спеціалізоване програмне забезпечення із захисту інформаційних ресурсів, що забезпечує різнобічне і змістовне вивчення відповідної предметної галузі, формування у майбутніх фахівців з інформатики навчальної, пізнавальної, професійної, інформаційно-комунікаційної та інших компетентностей.

Аналіз наукових досліджень. Розгляд комплексу питань, пов'язаних із використанням сучасних ІКТ у навчальному процесі, присвячені праці В. Ю. Бикова, М. С. Голованя, О. Г. Глазунової, М. І. Жалдака, Н. В. Морзе, О. В. Співаковського, С. А. Ракова, Ю. С. Рамського та багатьох інших.

Принципи використання ІКТ під час навчання різних дисциплін досліджуються такими науковцями, як О. Ю. Афанасьєва, Л. С. Глоба, О. М. Джерджула, М. М. Козяр, Ю. В. Лук'яненко, С. В. Росоха. Активно працювали в цьому напрямі також зарубіжні вчені: Д. Кендау, Д. Доерті, Дж. Йост, Т. Барський, С. Бандерсон, Т. Ейджер, А. Лесгодс, Г. Кєдровіч, Й.-Л. Мартинанд, Ф. Янушкевич та інші.

Питанням захисту інформаційних ресурсів займались такі учені, як М. З. Згуровський, Й. У Мастяниця, О. В. Соснін, Л. Є. Шиманський та багато інших. Щодо теоретичних і методичних аспектів підготовки фахівців у галузі захисту інформаційних ресурсів, то вони висвітлені у роботах В. П. Бабака, О. М. Богданова, Г. Ю. Маклакова, В. В. Козловського, М. Г. Коляди [2], С. О. Охріменко, В. О. Хорошко, Д. В. Чиркова та інших. Існує також низка праць, присвячених інформаційній безпеці особистості, зокрема праці Г. В. Грачова, М. А. Котика, В. Н. Ковальчук [3], Г. В. Ложкіна та інших науковців. Шляхи захисту інформаційних ресурсів за допомогою прикладних програм розглядали В. Б Дудикевич, В. М. Стеренчук , Л. М. Ракобовчук, В. В. Хома.

Однак питання застосування спеціалізованого програмного забезпечення під час навчання дисципліни «Криптологія» лишається недостатньо висвітленим і потребує детального вивчення.

Метою статті є огляд і порівняльна характеристика наявних версій програмного пакета CrypTool для застосування цього програмного забезпечення у процесі навчання дисципліни «Криптологія» майбутніх фахівців з інформатики.

Виклад основного матеріалу. ***CrypTool*** (e-learning software for cryptography and cryptanalysis [4]) — найпоширеніший в галузі криптології безкоштовний програмний засіб з відкритим вихідним кодом. Розробка CrypTool почалася у 1998 році за співробітництва «Дойче банк» (нім. Deutsche Bank), найбільшого фінансового конгломерату Німеччини, та декількох німецьких університетів (університет Дармштадта, університет Дуйсбург-Ессен, університет Зіген). Проект CrypTool був запущений з метою підвищення кваліфікації співробітників банку в галузях IT-безпеки та криптографії. Далі CrypTool було презентовано як безкоштовне програмне забезпечення з відкритим кодом для залучення до проекту інших додаткових розробників. Нині багато людей працюють по всьому світу над удосконаленням і технічним обслуговуванням цього програмного продукту.

CrypTool складається з п’яти незалежних складових (CT1, CT2, JCT, CTO, MTC3), що пов'язані між собою, але мають відмінні принципи роботи й використовуються в різних аспектах [5].

CrypTool 1 (CT1) є першим найповнішим і досконалим варіантом реалізації майже усіх наявних криптографічних алгоритмів та функцій. CT1 написаний на мові програмування C++ під операційну систему Windows. Програмне забезпечення доступне англійською, німецькою, польською, іспанською та сербською мовами. Нещодавно розпочався процес локалізації CT1 грецькою та російською мовами [6]. Певним недоліком є відсутність українського інтерфейсу, проте в майбутньому є ймовірність появи версії і цією мовою. CT1 має простий графічний інтерфейс та зручне меню, за допомогою якого користувач може створювати нові або відкривати вже існуючі текстові повідомлення, здійснювати їх редагування, зберігання, видалення тощо.

Шифрування повідомлень відбувається у робочій області програми з використанням симетричних [7, с. 15–16] класичних алгоритмів (шифри Цезаря [8, с. 25], Віженера [9, с. 18–19], Хілла [10, с. 18–20], Атбаш [8, с. 41–42] , Плейфера [9, с. 113–115], ADFGVX [4, с. 416–417], Вернама [11, с. 26–28], гомофонної заміни [8, с. 70–72], маршрутної перестановки [5, с. 35], Солітер [12, с. 81–85], Сцитала [8, с. 22–23]) і сучасних алгоритмів (IDEA [11, с. 238–243], RC2 [11, с. 237–238], RC4 [12, с. 34–36], RC6 [13, с. 82], DES [11, с. 200–208], AES[13, с. 75–78; 7, с.30–35], MARS [13, с. 82], Serpent [13, с. 78–79], Twofish [13, с. 79–81]). Асиметричні [7, с. 62–69]

алгоритми представлені шифром RSA [11, с. 346–347], а змішані (гібридні) [11, с. 38–39] — шифрами RSA-AES та ECC [14]–AES.

Для прикладу можна запропонувати студентам під час вивчення теми «Класичні шифри» дисципліни «Криптологія» розглянути перетворення повідомлення в середовищі CT1. Створимо повідомлення з текстом «WELL BEGUN IS HALF DONE» і зашифруємо його, використовуючи алгоритм Плейфера. Для цього оберемо у меню команду Encrypt/Decrypt ⇒ Symmetric (classic) ⇒ Playfair. У діалоговому вікні, що відкриється, потрібно вказати символи, які будуть розділяти біграми (пари символів) з однаковими літерами й увести ключ, у даному випадку ми вибрали «PLAYFAIREXEMPLE» (див. рис. 1). Програма автоматично створить ключову матрицю, за якою відбуватиметься перетворення, після чого натискаємо кнопку Encrypt. У головному вікні програми з’явиться два вікна, одне з яких міститиме розбите на біграми початкове повідомлення, а друге — шифротекст (див. рис. 2).

Даний приклад забезпечує детальне наочне представлення процесу шифрування, сприяє кращому розумінню студентами навчального матеріалу теми.

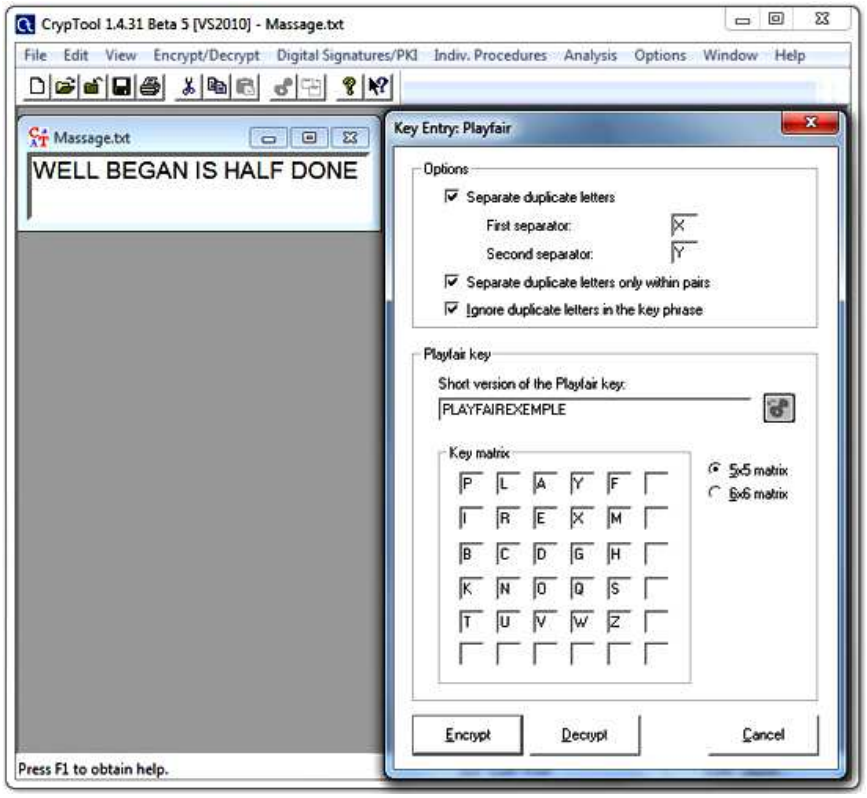

Рис. 1. Введення повідомлення та визначення параметрів перетворення у шифрі Плейфера

Рис. 2. Розбите на біграми початкове повідомлення та зашифроване повідомлення

Пакет CT1 забезпечує процедури створення і перевірки електронного цифрового підпису [15] на основі декількох алгоритмів (RSA [11, с. 351], DSA [11, с. 358–362] та ін.), генерування, експортування та імпортування ключів [11, с. 33].

Обчислення хеш-значення документа у програмі відбувається з використанням хеш-функцій MD2 [11, с. 328], MD4 [11, с. 324], MD5 [11, с. 324–328], SHA [11, с. 328–331], SHA-1 [13, с. 109–100], SHA-256 [13, с. 109–100], SHA-512 [13, с. 109–100], RIPEMD-160 [11, с. 331].

Потужний математичний апарат програми сприяє поглибленому вивченню асиметричних алгоритмів, зокрема RSA, та дозволяє визначити, чи є число простим, здійснювати генерацію простих чисел у заданому діапазоні, факторизацію числа (розклад числа на прості множники) [9, с. 174–197].

CT1 передбачає вивчення криптографічних протоколів [11, с. 31–35], таких як протоколи обміну ключами Діффі-Хелмана [11, с. 78–379], мережевої автентифікації [11, с. 380] тощо.

Різноманітні методи криптоаналізу реалізовано у CT1 — атака на основі шифротексту, атака на основі відкритого тексту та відповідного шифротексу на деякі симетричні алгоритми [11, с. 20], атака сторонніми каналами на RSA і на основі факторизації числа, атака на хеш-значення цифрового підпису [11, с. 348–351]. Існує можливість застосування аналітичних методів вимірювання, таких як обчислення ентропії [9, с. 179] й автокореляції, підрахунок частоти появи символу (послідовності двох, трьох, N символів) у тексті, представлення частоти у вигляді гістограми, визначення періодичності появи окремих фрагментів шифротексту.

Значною перевагою першої версії CrypTool є широкий діапазон анімації і

демонстрації шифрів Цезаря, Віженера, Енігми [8, с. 149], DES, AES, RSA, цифрового підпису, алгоритму шифрування на основі еліптичних кривих тощо. Наочне представлення та візуалізація криптографічних перетворень забезпечують ефективне сприйняття навчального матеріалу студентами спеціальності «Інформатика» під час вивчення дисципліни «Криптологія».

Під час вивчення теми «Симетричні шифри» дисципліни «Криптологія» пропонується розглянути один із найскладніших для вивчення симетричний блоковий алгоритм — DES (державний стандарт шифрування США), який доцільно продемонструвати студентам покроково, пояснивши кожен крок детально (див. рис. 3).

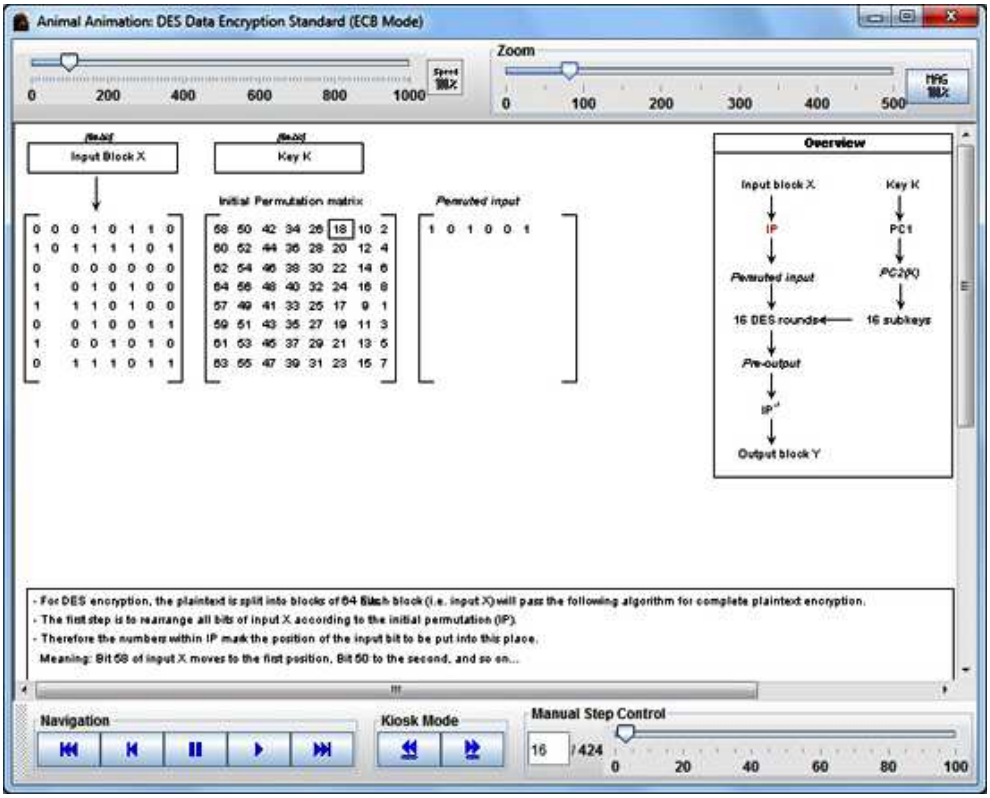

Рис. 3. Демонстрація початкової перестановки бітів вхідного 64-бітового блоку у шифрі DES

Щодо ***CrypTool 2 (CT2),*** то це сучасний наступник CT1, який реалізує концепцію візуального програмування та виконання каскадів криптографічних процедур [16]. Отже, криптографічний алгоритм з усіма складовими (наприклад, відкритий текст, ключ, шифротекст тощо) є єдиним проектом. Програма має зручний сучасний графічний інтерфейс, завдяки чому володіє яскравою наочністю й отримала широке розповсюдження (див. рис. 4). CT2 в даний час доступна німецькою й англійською мовами.

Унікальною особливістю CT2 є модульна конструкція, яка пропонує набір інструментів, котрі можуть бути об'єднані в нові проекти для реалізації криптографічних алгоритмів. Викладач має можливість використовувати це для підготовки практичних завдань для студентів. Також засобами CT2 можна забезпечити творчу роботу, пізнавальну активність студентів, яка полягає у власному створенні криптографічних алгоритмів.

Для зручності користувачів, яким важко працювати з проектами, що є набором модулів, розроблено компонент Wizard для візуалізації та кращого розуміння більшості криптографічних алгоритмів та процедур.

За винятком вищезгаданих шифрів, представлених у першій версії пакета CrypTool, у CT2 додатково реалізовані такі симетричні класичні алгоритми шифрування M-209 [17, с. 107–112], шифр Нігілістів [18, с. 34]; симетричні сучасні — шифри PRESENT, TEA; асиметричні алгоритми — шифр Paillier [19].

Зазначимо, що у CT2, на відміну від усіх інших версій, є можливість задавати алфавіт повідомлення, яке підлягатиме перетворенню. Це означає, що відкритий текст може бути українською або російською мовами, на відміну від CT1.

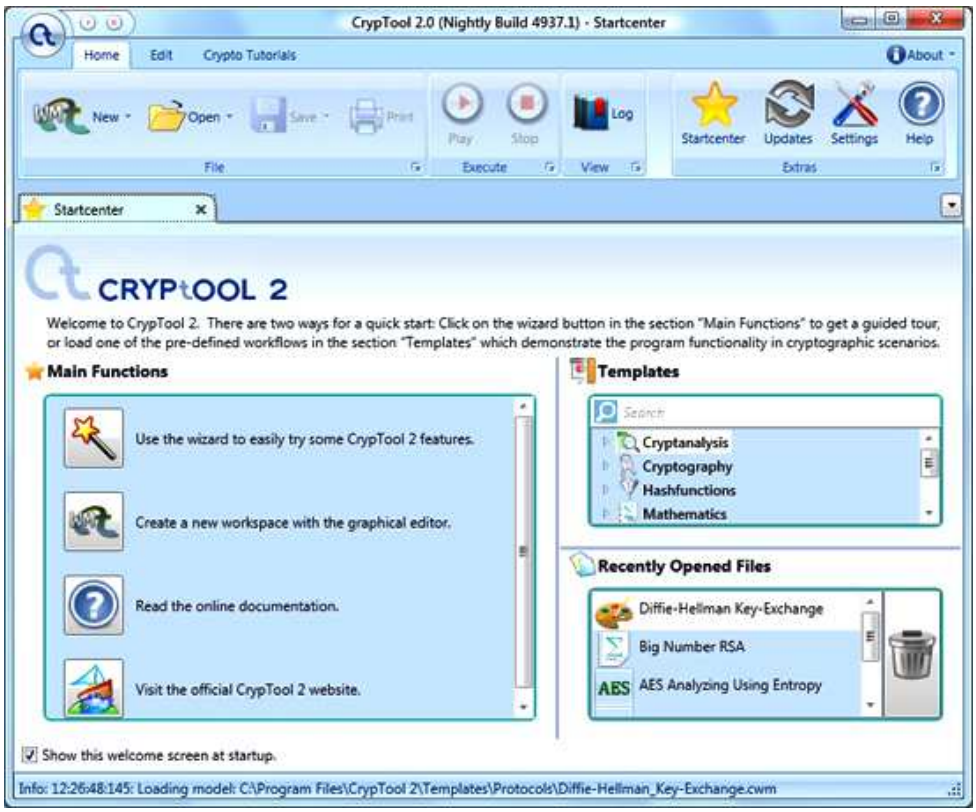

Рис. 4. Вікно завантаження CrypTool 2

Для прикладу пропонується під час навчання теми «Класичні шифри» дисципліни «Криптологія» розглянути шифр Віженера.

Повідомлення «З ВИДИМОГО ПІЗНАВАЙ НЕВИДИМЕ» та ключ «ВІЖЕНЕР» записуємо у відповідні текстові поля (Massage, Key). Далі визначаємо параметри перетворень, використовуючи наступні дві комірки (Vigenere), що реалізують алгоритми шифрування та дешифрування. На панелі інструментів натискаємо кнопку Play. У текстових полях (Encrypted, Result) одночасно з'являться зашифроване повідомлення та результат його дешифрування (див. рис. 5).

Цей приклад забезпечує наочність представлення процесу шифрування та дешифрування одночасно, що значно сприяє розумінню студентами навчального матеріалу даної теми.

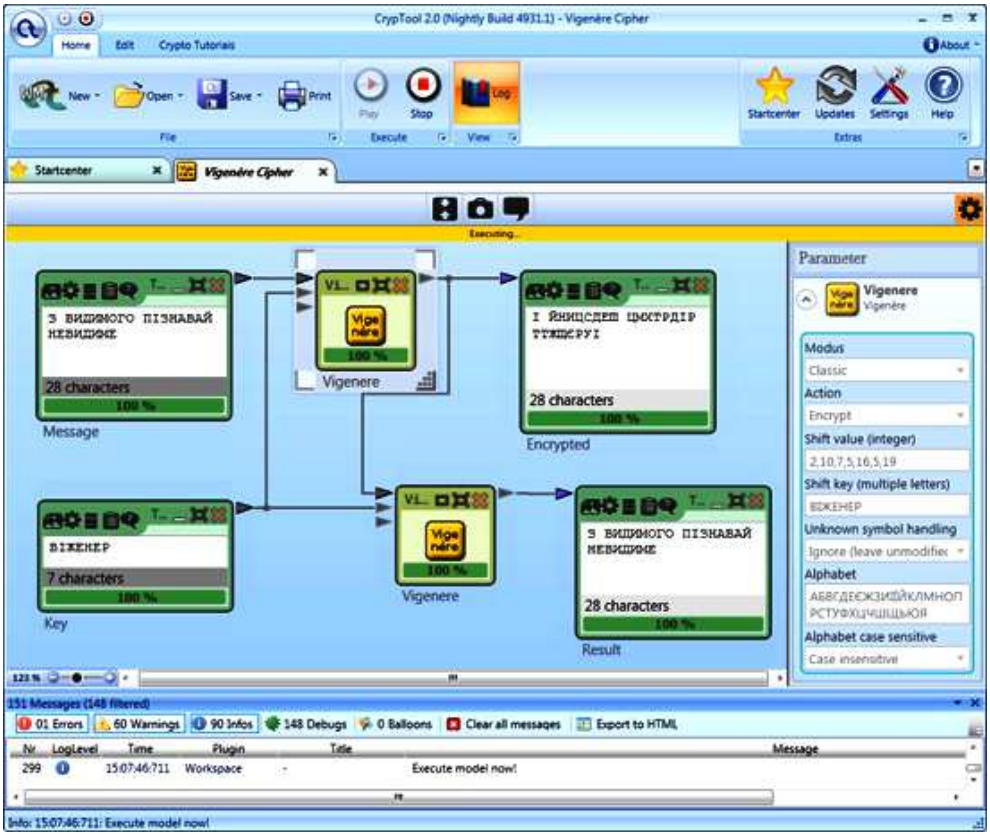

Рис. 5. Перетворення повідомлення за допомогою шифру Віженера у CT2

У програмному забезпеченні CT2 відсутня схема створення та перевірки електронного цифрового підпису, проте автоматизовано більшість відомих криптографічних хеш-функції (починаючи з MD5 і закінчуючи Whirlpool [20]).

Значно розширено математичну базу, яка застосовується у багатьох алгоритмах криптографії: задача дискретного логарифмування [9, с. 195], розклад числа на прості множники за різними алгоритмами [11, с. 190–191], генератор простих чисел, методи генерації псевдовипадкових чисел (лінійний конгруентний метод [9, с. 275–277],

регістр зсуву з лінійним зворотним зв'язком [9, с. 277–282], регістр зсуву з нелінійним зворотним зв'язком [9, с. 306–307]).

Програмний засіб CT2 оснащений численними інструментами криптоаналізу повідомлень, де представлені частотний аналіз (див. рис. 6) і метод прямого перебору шифрів заміни. Що стосується шифрів перестановки, то можливе застосування наступних атак: на основі відкритого тексту та відповідного шифротексту, на основі поєднання літер у тексті, на основі нейронних мережевих шифрувальних пристроїв (генетичної). Криптоаналіз сучасних шифрів у програмі відбувається з використанням ентропії, атаки на основі відкритого тексту, кубічної атаки.

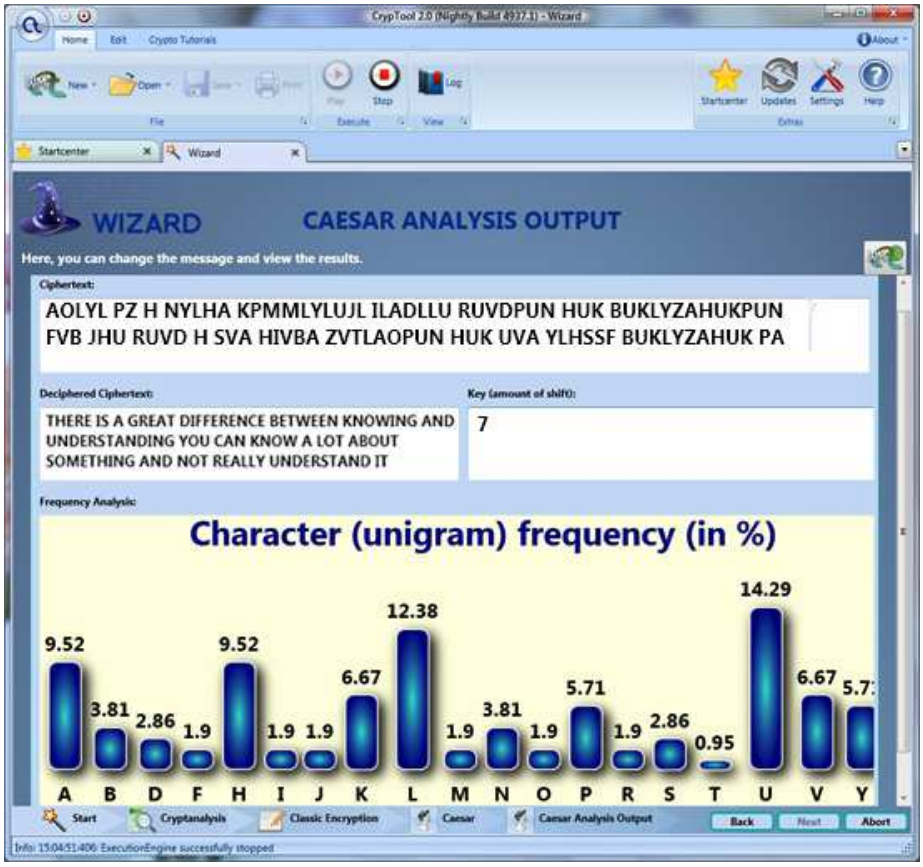

Рис. 6. Wizard-візуалізація частотного криптоаналізу шифру Цезаря

У другій версії CrypTool представлено роботу протоколу обміну ключами Діффі-Хелмана та протоколу смарт-карти. Також тут показано, як можна зламати протокол WEP [12, с. 212], який використовується для забезпечення безпеки мереж Wi-Fi.

Новизною у CT2 є використання стеганографії, яку використовують спільно з методами криптографії. Під стеганографією найчастіше розуміють приховування інформації в текстових, графічних або аудіофайлах шляхом використання спеціального програмного забезпечення.

JCrypTool (JCT) — незалежний від платформи програмний засіб, сумісний з операційними системами MAC, Windows і Linux, а також обов'язково для роботи потребує встановлення Java 1.6 або новіше. JCrypTool має сучасний користувацький інтерфейс та підтримує англійську, німецьку або іспанську мови [21].

Перш за все, файли, що підлягатимуть перетворенню, мають бути відкритті у середовищі програми. Вони можуть бути як текстовими, так і представлені у шістнадцятковій системі числення [22] (для перегляду в потрібному вигляді існує команда Edit ⇒ Open with…).

Крім алгоритмів шифрування присутніх у двох попередніх версіях CrypTool, ця версія передбачає використання класичних шифрів Bifid, Double Box [17, с. 95–96]. Сучасні симетричні шифри представлені, зокрема, такими відомими алгоритмами як SAFER+, SAFER++ [7, с. 41–46]. З асиметричних шифрів реалізовано шифри ElGamal [11, с. 353], McEliece [9, с. 355–356] та інші.

JCrypTool має два режими роботи:

- основний (за замовчуванням) Default — документо-орієнтований (див. рис. 7), забезпечує доступ до криптографічних функцій через головне меню та CryptoExplorer (провідник у правій частині вікна).

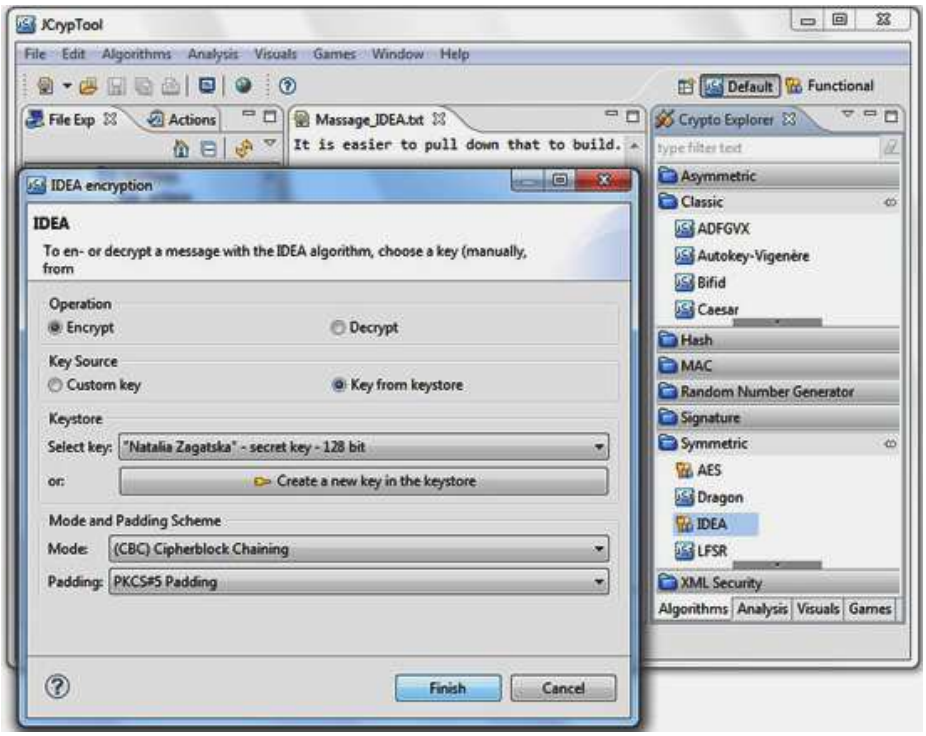

Рис. 7. Застосування шифру IDEA у режимі Default

- функціональний Functional — функціонально-орієнтований (рис. 8), забезпечує доступ до сховища ключів, роботу з бібліотекою FlexiProvider, містить

розширений перелік алгоритмів і дозволяє вибір всіх можливих параметрів перетворення.

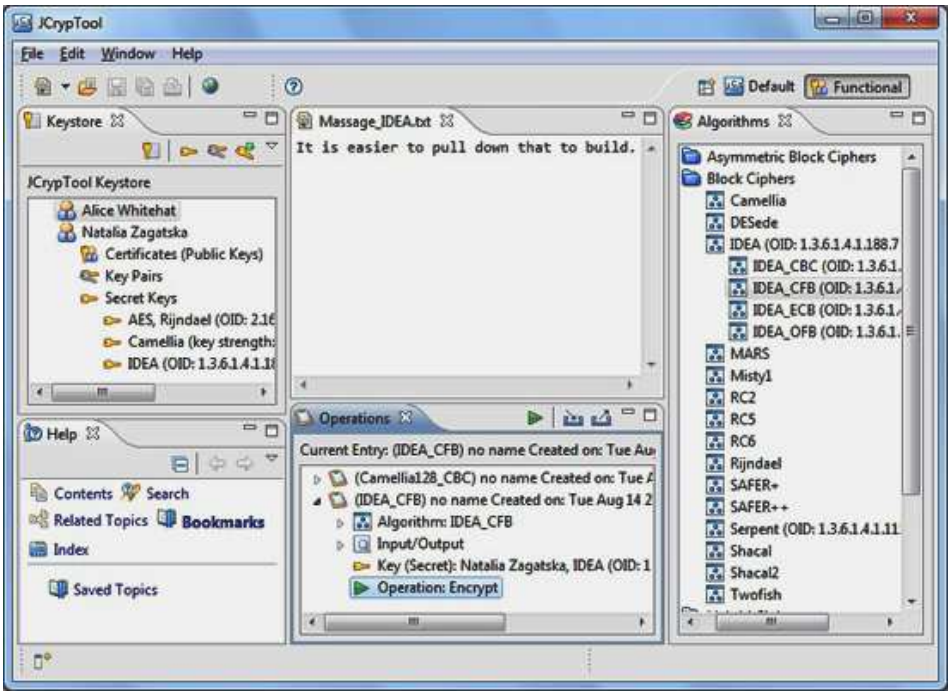

Рис. 8. Застосування шифру IDEA у режимі Functional

JCT містить багато функцій для обчислення хешу документа та створення імітовставки (CBC MACs, CMAC, Two-Track-MAC [11, с. 339]).

Поточна версія програмного засобу, на відміну від попередніх, не забезпечує користувача достатньою кількістю методів криптоаналізу, крім того, не акцентується увага на математичних поняттях криптології. А ось алгоритми генерації випадкових чисел реалізовані досить добре.

Особливістю JCT є використання процедур шифрування й електронного підпису вмісту XML-документів. Візуалізація алгоритмів містить значний перелік криптографічних алгоритмів і процедур (див. рис. 9).

CrypTool-Online — це он-лайн-версія програми електронного навчання CrypTool, яка, у першу чергу, призначена для вивчення класичних шифрів. Криптографічні перетворення відбуваються безпосередньо у браузері комп’ютера або смартфону [23].

Крім великого різноманіття класичних шифрів, CrypTool-Online пропонує такі методи кодування: ASCII, код Бекона, генератор штрих-кодів, код Хаффмана [24], код Морзе.

Криптоаналіз в он-лайн режимі забезпечується на основі автокореляції, підрахунку частот символів у тексті, побудови N-грам.

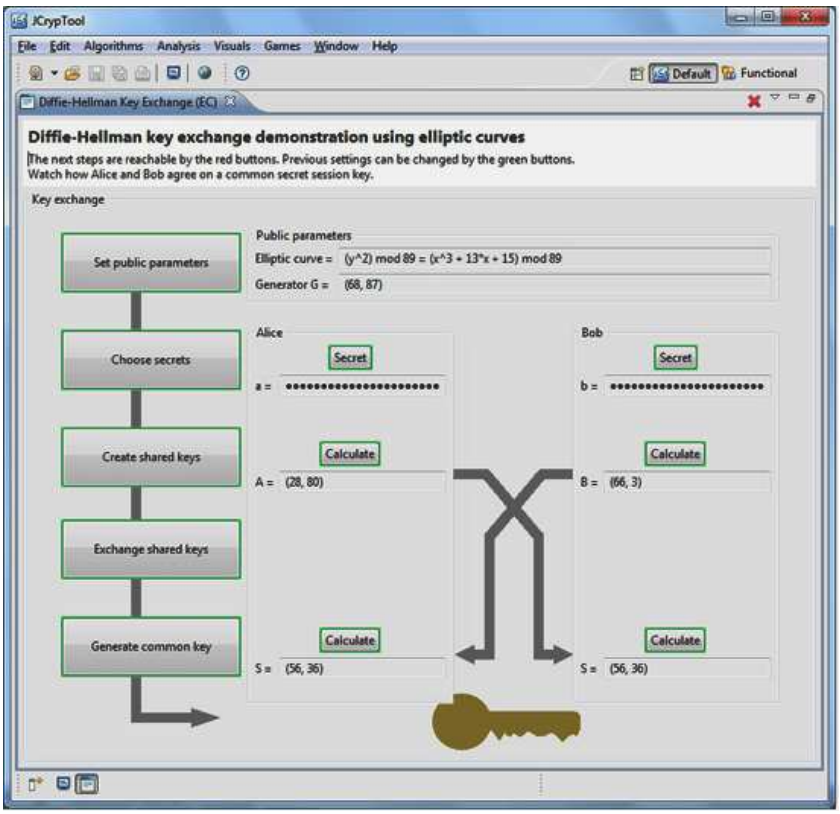

Рис. 9. Візуалізація протоколу обміну ключами Діффі-Хелмана на основі еліптичних кривих

У CrypTool-Online представлено шифр AES, генератор паролів, також є можливість вивчення теорії чисел на основі навчальної гри Taxman (збирач податків). Варто зазначити, що практично всі наведені на сайті методи мають детальне теоретичне пояснення, підкріплені прикладами та ілюстраціями.

MisteryTwister C3 (MTC3) — це міжнародні змагання в галузі криптографії [25]. Різноманітні завдання та загадки пропонуються на чотирьох рівнях складності. Теми, що охоплюються в MTC3, будуть цікавими, як для студентів-початківців, які бажають дізнатися більше про криптографію, так і для фахівців з багаторічним досвідом роботи.

Отже, підсумовуючи вищесказане, наведемо порівняльну характеристику технічних вимог і вихідних характеристик (див. табл. 1) та деяких основних криптографічних функцій та алгоритмів різних версій пакета CrypTool (див. табл. 2).

Таблиця 1

Технічні вимоги та вихідні характеристики

	CT1	**CT2**	**JCT**	**CTO**
Системні вимоги	Windows (32 Bit)	Windows (32, 64 Bit)	Windows, Linux, MacOS (32, 64 Bit)	Windows, Linux, MacOS (32, 64 Bit)
Додатково вимагає встановлення	JRE 1.6 (Java Runtime Environment)	Microsoft .NET Framework 4.0	JRE 1.6 або JDK 7 (Java Development Kit)	Adobe Flash Player
Поточна стабільна версія	CrypTool 1.4.30 (серпень 2010)	CrypTool 2.0.48 05.1 (травень 2012)	Jcryptool-1.0.0-RC6 (червень 2012)	CrypTool-Online (з березня 2009)
Адреса домашньої сторінки	http://www.cryptool.org/en/cryptool1	http://www.cryptool.org/en/cryptool2	http://www.cryptool.org/en/jcryptool	http://www.cryptool-online.org
Тип відкритої ліцензії	Apache Open Source Licence 2.0	Apache Open Source Licence 2.0	Eclipse Public Licence 1.0	GNU General Public License 3.0
Мови інтерфейсу	англійська, німецька, іспанська, польська, сербська (грецька та російська у стадії розробки)	англійська, німецька	англійська, німецька, іспанська	англійська, німецька
Реалізовано на мові програмування	C++	C#, .NET, WPF (Windows Presentation Foundation)	Java, Eclipse RCP (Rich Client Platform)	Joomla!, JavaScript

Таблиця 2

Деякі основні криптографічні функції та алгоритми

	Криптографічна функція	**CT1**	**CT2**	**JCT**	**CTO**
Класичні шифри	ADFGVX	+	+	+	+
	Альберті				+
	Атбаш	+			
	Віженер	+	+	+	+
	Вернам	+			
	Енігма		+		+
	Плейфер	+	+	+	+
	Полібій				+

	Криптографічна функція	CT1	CT2	JCT	CTO
	Сцитала	+	+		+
	Цезар	+	+	+	+
	Хілл	+			+
Сучасні шифри	AES	+	+	+	+
	DES	+	+		
	ElGamal			+	
	IDEA	+		+	
	RSA	+	+	+	
	Twofish	+	+	+	
Хеш-функції	MD2	+			
	MD4	+		+	
	MD5	+	+	+	
	RIPEMD	+	+	+	
	SHA family	+	+	+	
	Whirlpool		+		
ЕЦП	DSA	+		+	
	ECDSA	+		+	
	GMSS			+	
	RSA	+		+	
Криптоаналіз	Злам шифру ADFGVX	+	+		
	Атака повним перебором на AES	+	+		
	Атака на основі автокореляції	+			
	Атака повним перебором на шифр Цезаря	+	+		
	Атака повним перебором на DES	+	+		
	Злам Енігми		+		
	Злам на основі ентропії	+		+	
	Злам на основі факторизації	+	+		
	Частотний криптоаналіз	+	+	+	+
	Злам шифру Хілла	+			
	Атака повним перебором на IDEA	+			
	Тест Казіскі		+		
	Злам шифру Плейфера	+			
	Атака на RSA	+			
	Аналіз шифру Вернама	+			
	Злам шифру Віженера	+	+	+	+

Висновки. Пакет CrypTool забезпечує комплексну та всебічну підтримку навчально-методичних матеріалів і програм для навчання дисципліни «Криптологія».

З проведеного порівняльного аналізу всіх версій CrypTool можна зробити висновок, що CrypTool1 та CrypTool2 можуть бути рекомендовані до застосування у процесі навчання дисципліни «Криптологія» майбутніх фахівців з інформатики, як найбільш доцільні, оскільки вони вдало реалізують алгоритми шифрування, мають простий і зручний інтерфейс. Ці програмні засоби можна використовувати для демонстрації принципів роботи криптографічних алгоритмів і протоколів на лекціях, а також для проведення лабораторних досліджень та вправ.

Список використаних джерел

1. Дориченко С. А. 25 этюдов о шифрах: Популярно о современной криптографии / С. А. Дориченко, В. В Ященко. — М. : Теис, 1994. —72 с.
2. Коляда М. Г. Проблеми професійної підготовки фахівців з інформаційної безпеки у Російській Федерації [Електронний ресурс] / М. Г. Коляда // Інформаційні технології і засоби навчання. — 2009. — № 4 (12). — Режим доступу : http://journal.iitta.gov.ua/index.php/itlt/article/view/75, 20.09.2012.
3. Ковальчук В. Н. Розробка моделі системи захисту інформації навчального комп’ютерного комплексу [Електронний ресурс] / В. Н. Ковальчук // Інформаційні технології і засоби навчання. — 2008. — № 3 (7). — Режим доступу : http://journal.iitta.gov.ua/index.php/itlt/article/view/119, 20.09.2012.
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. The CrypTool Portal [Електронний ресурс]. — Режим доступу : http://www.cryptool.org/en.
6. CrypTool 1 [Електронний ресурс]. — Режим доступу : http://www.cryptool.org/en/download-ct1-en/215-ct1-downloads-eng.
7. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, Р. Е Серов. — М. : Горячая линия – Телеком, 2002. — 152 с.
8. Сингх С. Книга шифров: тайная история шифров и их расшифровки / Саймон Сингх; [пер. с англ. А. Галыгина]. — М. : АСТ: Астрель, 2007. — 447 с.
9. Основы криптографии : [учеб. пособ. 2-е изд., исп. и доп.] / [А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин]. — М : Гелиос АРВ, 2002. — 480 с.

10. Саломаа А. Криптография с открытым ключом. / Арто Саломаа; [пер. с англ. И. А. Вихлянцева]. — М. : Мир, 1995. — 318 с.

11. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. — М. : Триумф, 2002. — 816 с.

12. Поточные шифры / [Асосков А. В., Иванов М. А., Мирский А. А. и др.]. — М. : КУДИЦ-ОБРАЗ, 2003. — 336 с.

13. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер; [пер. с англ. Н. Н. Селиной]. — М. : «Диалектика», 2004. — 432 с.

14. Болотов А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / Болотов А. А., Гашков С. Б., Фролов А. Б. — М. : КомКнига, 2006. — 280 с.

15. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV [Електронний ресурс] / Верховна Рада України. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/852-15.

16. About CrypTool 2 [Електронний ресурс]. — Режим доступу http://www.cryptool.org/en/cryptool2.

17. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. — М. : Солон-Пресс, 2002. — 511 с.

18. Синельников А. В. Шифры и революционеры России. [Електронний ресурс]. — Режим доступу : http://www.e-reading.org.ua/bookreader.php/136568/Sinel'nikov_-_Shifry_i_revolyucionery_Rossii.pdf.

19. Варновский Н. П. Гомоморфное шифрование [Електронний ресурс] / Н. П. Варновский, А. В. Шокуров // Труды Института системного программирования РАН. — 2007. — Т. 12. — Режим доступу : http://www.ispras.ru/ru/proceedings/docs/2007/12/isp_12_2007_27.

20. The Whirlpool Hash Function [Електронний ресурс]. — Режим доступу : http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html.

21. JCrypTool — The cryptography e-learning platform [Електронний ресурс]. — Режим доступу : http://www.cryptool.org/en/jct-documentation-en/jct-resources-en.

22. Шауцукова Л. З. Информатика 10–11. [Електронний ресурс]. — М. : Просвещение, 2000. — Режим доступу : http://book.kbsu.ru/theory/chapter4/1_4.html.

23. CrypTool-Online [Електронний ресурс]. — Режим доступу : http://www.cryptool-online.org.

24. Симаков. А. Код Хаффмана. [Електронний ресурс] / А. Симаков. — Режим доступу : http://entropyware.info/HuffmanCode/huffcode.html.

25. MisteryTwister C3 [Електронний ресурс]. — Режим доступу : http://www.mysterytwisterc3.org.

ОБЗОР РАЗНЫХ ВЕРСИЙ ПАКЕТА CRYPTOOL КАК СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Загацкая Наталия Александровна, аспирантка кафедры прикладной математики и информатики Житомирского государственного университета имени Ивана Франка, г. Житомир, e-mail: thalitana@gmail.com

Аннотация

В статье описываются характерные особенности свободно распространяемого программного обеспечения по защите информационных ресурсов CrypTool, которое сочетает в себе эффективную реализацию известных алгоритмов шифрования и их визуальное представление. Уделено значительное внимание применению такого программного обеспечения в процессе обучения дисциплины «Криптология», что позволяет рассмотреть широкий круг вопросов по защите информационных ресурсов. Проведен детальный обзор и сравнительный анализ всех имеющихся версий этого программного средства, среди которых выделены наиболее эффективные относительно реализаций алгоритмов шифрования и удобства интерфейса.

Ключевые слова: криптология, криптография, криптоанализ, программное средство, шифрование.

REVIEW OF DIFFERENT RELEASES OF CRYPTOOL PACKAGE AS TOOL FOR INFORMATION RESOURCES SECURITY

Natalia O. Zagatska, graduate student of the Academic Chair of Applied Mathematics and Informatics, Zhytomyr Ivan Franko State University, Zhytomyr, e-mail: thalitana@gmail.com

Resume

The article describes the characteristic features of free software for information resources security CrypTool that combines effective realization of known encryption algorithms and their visual presentation. The considerable attention is given to using such software in the course of Cryptology training that allows considering a wide range of questions for information resources security. Conducted a detailed review and comparative analysis of all available releases of the software among them allocated the most effective concerning realization of encryption algorithms and convenience interface.

Keywords: cryptology cryptography, cryptanalysis, software, encryption.

Матеріал надійшов до редакції 22.10.2012 р.