УДК 378:004.056.55

Загацька Н.О.,
асистент кафедри прикладної математики та інформатики,
Житомирський державний університет імені Івана Франка, м. Житомир

НАВЧАННЯ МАТЕМАТИЧНИХ ОСНОВ КРИПТОЛОГІЇ З ВИКОРИСТАННЯМ ІНСТРУМЕНТАРІЮ CRYPTOOL

Важливу роль у процесі підготовки фахівців з інформатики відіграє вивчення як суто математичних дисциплін, так і дисциплін, тісно пов'язаних з математикою. Проте досить часто виникають випадки, коли викладачі відзначають недостатній рівень володіння студентами ВНЗ математичним апаратом, необхідним для вирішення прикладних завдань.

Методи та результати різних розділів математики, таких як алгебра та теорія чисел, дискретна математика, теорія складності, теорія ймовірностей та математична статистика лежать в основі криптології – науки про шифри. Тому розуміння студентами принципів роботи деяких сучасних криптографічних алгоритмів вимагає серйозної математичної підготовки. Знання математичних основ криптології дозволяє вирішувати задачі, на яких базуються сучасні симетричні і асиметричні криптосистеми, виконувати елементарний криптоаналіз шифрів, будувати алгоритми, що реалізують генератори випадкових послідовностей тощо.

Одним із шляхів подолання труднощів із сприйняттям та розумінням математичних основ криптографічних алгоритмів є застосування наочності. Перспективним напрямом реалізації дидактичного принципу наочності є використання у процесі навчання криптології програмного засобу CrypTool, що дає змогу демонструвати студентам абстрактні математичні об'єкти та явища, за рахунок чого підвищується рівень доступності складного навчального матеріалу, забезпечується його оптимальне засвоєння та запам'ятовування.

Програмний засіб CrypTool оснащений численним схемами, прикладами, ілюстраціями, анімаціями, які допомагають ознайомити студентів з основними математичними положеннями, на яких ґрунтується робота сучасних криптосистем (Рис. 1). Зокрема, це

операції з цілими числами за модулем *n*, поняття відображення, групи, кільця, поля, Алгоритм Евкліда, теорема Ферма та інші.

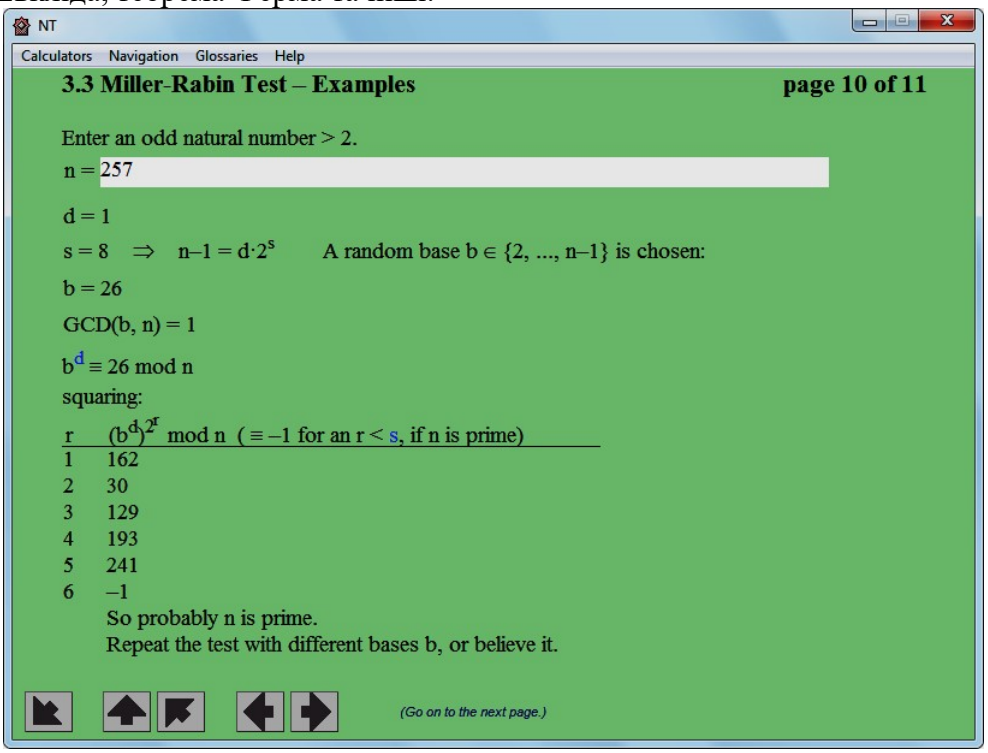

Рис. 1 Демонстрація тесту простоти Міллера–Рабіна у середовищі CrypTool

Цікавою є демонстрація криптографії на еліптичних кривих, що має інтерактивний характер та забезпечує діалог користувача з програмним засобом (Рис. 2). Користувач визначає параметри еліптичної кривої, таким чином переходячи від пасивного сприйняття інформації до активного дослідження характеристик об'єкта, що вивчається.

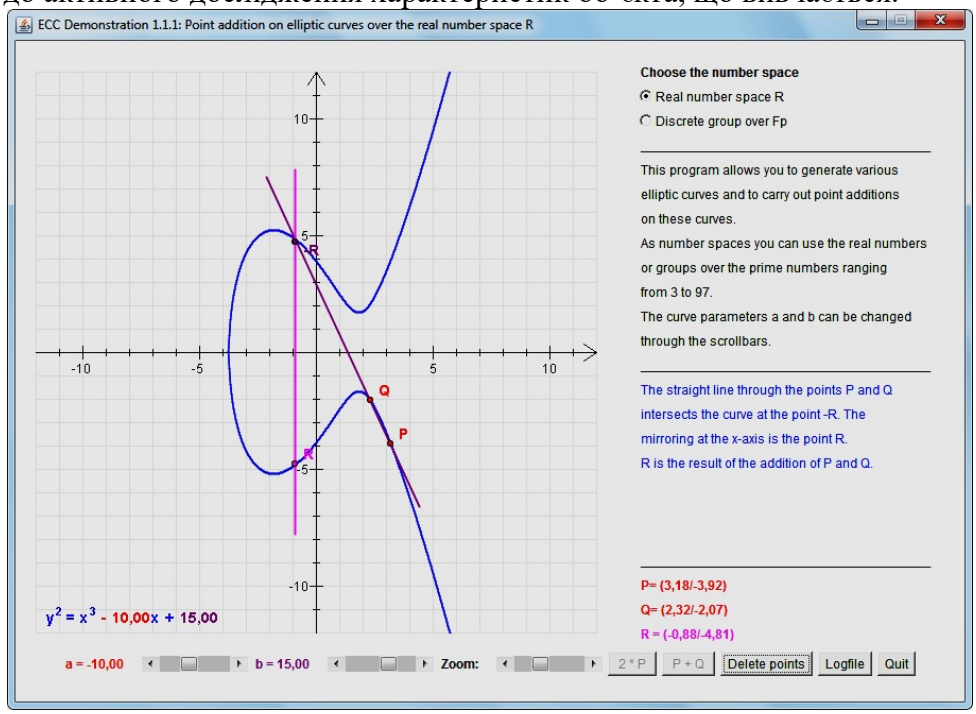

Рис. 1 Демонстрація криптографії на еліптичних кривих у середовищі CrypTool

Варто зазначити, що за допомогою засобу CrypTool студентам демонструються також математичні основи роботи асиметричних шифрів, стійкість яких спирається на гіпотези щодо складності розв'язання таких задач як розкладання великих чисел на прості множники та обчислення дискретних логарифмів в скінченному полі.

Загалом навчання математичних основ криптології з використанням інструментарію CrypTool надає можливість:

- у наочній формі представити математичні перетворення, на яких ґрунтуються криптографічні алгоритми;
- полегшити розуміння та запам'ятовування навчального матеріалу, стимулювати розвиток абстрактного і логічного мислення студентів;
- спонукати студентів до глибокого і всебічного аналізу властивостей досліджуваних об'єктів і процесів;
- активізувати пізнавальну діяльність студентів та розвинути у них інтерес до навчальної дисципліни;
- забезпечити інтенсифікацію навчання, раціональне та ефективне використання навчального часу.

При цьому необхідно враховувати, що активне сприйняття теоретичного матеріалу можливо тільки у тому випадку, коли візуалізовані об'єкти та процеси пояснюються. Поєднання коментарів викладача з навчальною демонстрацією дозволяє досягти максимальної інформаційної наповненості заняття, підтримувати увагу слухачів, розкрити найбільш суттєві та важливі моменти та покращити якість навчання криптології загалом.

Список використаних джерел:

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.The CrypTool Portal [Електронний ресурс]. – Режим доступу:http://www.cryptool.org/en.