УДК 681.3

ВИКОРИСТАННЯ МОДЕЛЮВАННЯ ПОТОКОВИХ ШИФРІВ У ЛАБОРАТОРНОМУ ПРАКТИКУМІ З ДИСЦИПЛІНИ “ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ЕОМ”

Кісельов Є.М., к.т.н., доц. (ЗДІА)

З розвитком і ускладненням засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від безпеки використовуваних їм інформаційних технологій, яка визначається ступенем захищеності і стійкості як комп'ютерних систем в цілому, так і окремих програм. Тому актуальною є підготовка фахівців у області захисту інформації в комп'ютерних мережах і системах.

Одним з методів забезпечення конфіденційності передаваних повідомлень є застосування потокових шифрів, типова реалізація яких є скремблером. Саме на прикладі скремблювання і відбувається практичне вивчення побітного шифрування в дисципліні «Засобу захисту інформації в мережах ЕОМ». В ході лабораторної роботи по цій темі передбачається моделювання функціонування скремблера і дескремблера за допомогою програми Electronics WorkBench [1] (рис.1).

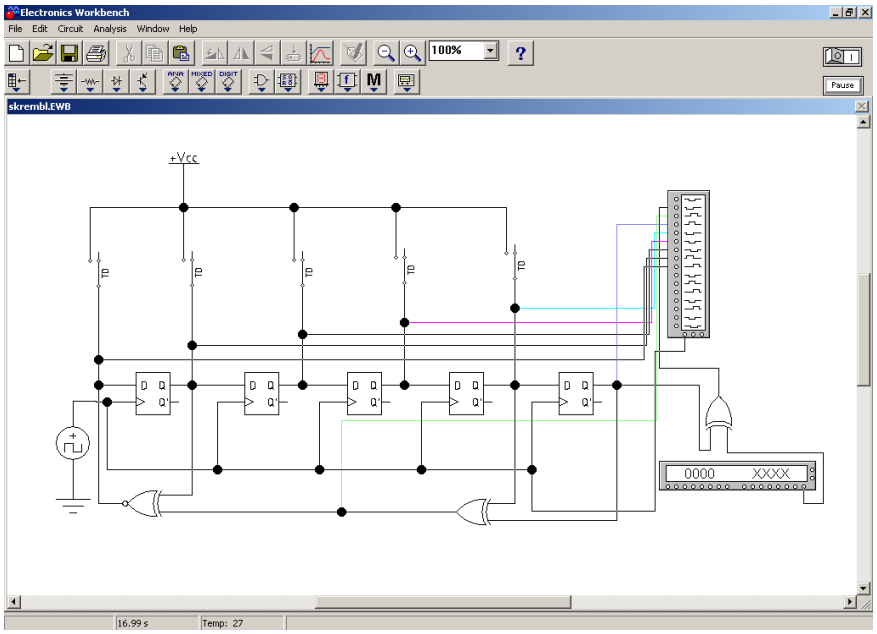

Рис. 1.

На рис.1 показаний варіант завдання для скремблера з п'ятирозрядним ключем [2]. Роль джерела інформації виконує генератор слів, кожен регістр ключа побудовано на основі D – тригера, до входу якого підключається програмований часовий перемикач, задаючий початкове значення розряду. Циклічна зміна стану ключа визначається системою зворотного зв'язку, що включає два елементи «Виключаєче АБО». Аналіз скремблера проводиться за допомогою логічного аналізатора, з'єднаного як з виходом і входом скремблера, так і з кожним D, – тригером (рис. 2).

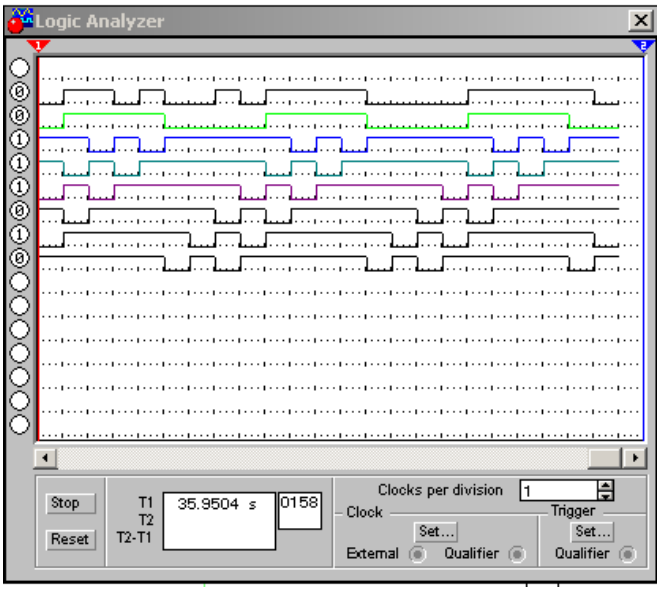

Рис. 2

Варіанти завдань для моделювання скремблера відрізняються величиною розрядності ключа, способами організації зворотного зв'язку і початковим значенням кодуючої послідовності.

Досвід використання пропонованого підходу для вивчення потокових шифрів показав його ефективність, особливо при поєднанні апаратного і програмного способу реалізації скремблювання.

Перелік використаної літератури

1. Карлащук В.И. Электронная лаборатория на IBM PC: программа Electronics Workbench и ее применение. – М.: Солон-Р, 2001. – 726 с.
2. http://www.citforum.ru/security/belyaev_book/