МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

IMA :: 2017

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 17–21 квітня 2017 року)

Суми
Сумський державний університет
2017

Візуалізація алгоритму симетричного шифрування AES

Лаврик Т.В., *старший викладач*, Шепотько Д. Ю., *студент*
Сумський державний університет, м. Суми

З метою забезпечення захисту інформації криптографічні алгоритми, що використовуються для шифрування інформації, мають відповідати вимогам криптостійкості та надійності. Одним із таких алгоритмів є алгоритм Advanced Encryption Standard (AES).

AES – це ітераційний блочний симетричний шифр. Цей алгоритм перетворює 128-бітний блок, використовуючи секретний ключ. Для розшифрування отриманого 128-бітного блоку використовується інше перетворення з тим же ключем. Довжина ключа може бути 128, 192 або 256 біт. Від довжини ключа залежить число раундів шифрування: 128 біт – 10 раундів; 192 біта – 12 раундів; довжина 256 біт – 14 раундів. Раунд складається з 4 різних перетворень: SubBytes – функція для підстановки байтів, що використовує таблицю замін; ShiftRows – функція, що забезпечує циклічний зсув рядків у матриці байтів; MixColumns – функція, яка змішує дані всередині кожного стовпця матриці байтів; AddRoundKey – додавання елементів матриці з раундовим ключем (операція XOR).

Алгоритм AES є найбільш поширеним, оскільки в алгоритмі не виявлено суттєвих уразливостей. Зокрема, криптоалгоритм не піддається таким видам криптоаналітичних атак, як диференціальний і лінійний криптоаналіз, криптоаналіз на основі зв'язаних ключів.

Для майбутніх фахівців з кібербезпеки є важливим розгляд сутності сучасних симетричних і асиметричних криптографічних алгоритмів, зокрема й алгоритму AES. Для кожного криптоалгоритму слід досліджувати як спроектовано алгоритм, чому він працює, як можна його атакувати і як він використовується на практиці. Тому з навчальною метою розроблено демонстраційний тренажер «Криптографічний алгоритм симетричного шифрування AES».

Демонстраційний тренажер дозволяє візуалізувати процес шифрування на кожному раунді та детально розглянути перетворення, що відбуваються при шифруванні. Тренажер розроблено на мові програмування ActionScript 3.0 на платформі Adobe Flash Professional CS6, що дозволяє реалізувати тренажер методом покадрової анімації з навігацією за шкалою часу.