МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ФІЗИКА, ЕЛЕКТРОНІКА, ЕЛЕКТРОТЕХНІКА

ФЕЕ: 2016

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 18–22 квітня 2016 року)

Суми
Сумський державний університет
2016

Дослідження криптостійкості шифрування даних з використанням стандарту «IDEA»

Демчик С.Л., *студент*
ЖВІ ім.С.П.Корольова, м. Житомир

Алгоритм IDEA є симетричним блоковим шифром. Алгоритм IDEA складається з восьми раундів, за якими йде кінцеве перетворення. Алгоритм поділяє блок даних на чотири 16-бітові підблоки. Кожний раунд отримує на вході чотири 16-бітові підблоки та створює чотири 16-бітові вихідні підблоки, тобто всього в алгоритмі використовується 52 раундових ключа.

Алгоритм розгортання ключа визначає порядок отримання раундових ключів із початкового ключа шифрування *K*. Він містить два компоненти: розширення ключа шифрування *K*; вибір раундових ключів. Проведено дослідження криптостійкості алгоритму на прикладі.

Нехай ключ шифрування даних *K* дорівнює:
$K = 0001000200030004000500060007000{8}_{16}$; $M = 0000\ 0001\ 0002\ 0003_{16}$
K – ключ шифрування даних, *M* – вхідне повідомлення

Визначимо ключі розширеного ключа K_P шляхом розбиття ключа шифрування даних *K* на вісім частин і циклічного зсуву бітів ключа шифрування даних *K*. Якщо розбиття на блоки по 64 біт неможливо, останній блок доповнюється різними способами певною послідовністю біт. Для уникнення витоку інформації про кожному окремому блоці використовуються різні режими шифрування.

Вичерпна комп'ютерна перевірка показує, що кожний біт виходу цієї структури залежить від кожного біта входів незашифрованого блоку даних і від кожного біта раундових ключів. Ця структура повторюється в алгоритмі вісім разів, забезпечуючи високоефективну дифузію.

Алгоритм IDEA має 128-бітовий ключ, що забезпечує його криптостійкість. Внутрішня структура алгоритму IDEA забезпечує стійкість до криптоаналізу. Проте, істотним недоліком цього алгоритму є те, що він не передбачає збільшення довжини ключа, а також не всі роботи з криптоаналізу були опубліковані, тобто цілком можливо, що шифр буде зламаний в майбутньому.