АНАЛІЗ ТА МОДЕЛЮВАННЯ ШИФРІВ ДОКОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ

Кирик О.І., Нікольський Є.С., Плахтій О.С.

Науковий керівник — доц. каф. «Інформаційні системи», канд. техн. наук,

Болтенков В.О.

Захист інформації у системах зберігання, обробки та передачі даних являється однією з провідних інформаційних технологій у бізнесі, фінансах електронному документообігу. Найбільш ефективним засобом захисту інформації є криптографія. Більшість сучасних комп'ютерних криптосистем у тій чи іншій мірі використовують принципи докомп'ютерної історичної криптографії — шифри заміни, перестановки, багатократної перестановки. Мета дослідження — показати різноманіття і важливість історичних шифрів. Програмні алгоритми шифрування засновані на математичних моделях історичних шифрів. Основною формулою історичного шифрування є

$$Y_i = (X_i + C_i) \bmod N_a,$$

де: Y_i — зашифрований символ,
X_i — вхідний символ,
C_i — символ ключа,
N_a — розмір алфавіту,
$i = \overline{1,M}$
де M — довжина повідомлення.

У більшості шифрів використовується операція підсумування за модулем, це дозволяє не вийти за рамки алфавіту [1]. В результаті дослідження створена колекція історичних шифрів. Вона включає: шифр Цезаря/Августа, шифр класичної перестановки, квадрат Полібія, поліпшений шифр Полібія, таблицю Віженера, таблицю Тритемія, шифр “Атбаш” та імітацію шифрувальної машини “Енігма”. Програма може зашифровувати/розшифровувати як текстові, так і бінарні файли. Це можливо за рахунок використання кодування Unicode, в якому кожен символ представлений 16-бітним кодом.

Висновки. Створена програмна колекція демонструє, що історичні шифри є основою сучасної криптографії. Це дозволяє використовувати програмний продукт для ефективного навчання в курсі “Захист інформації”.

1. Смарт Н. Криптография. — М.: Техносфера, 2005.