Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

РЕАЛІЗАЦІЯ АЛГОРИТМУ ШИФРУВАННЯ ІЗ ПРАВДОПОДІБНИМ ЗАПЕРЕЧЕННЯМ (ДЛЯ ЧИСЕЛ ДОВЖИНОЮ ЩОНАЙМЕНШЕ 4 096 БІТІВ)

Методичні рекомендації до лабораторної роботи з дисципліни
«Теорія чисел, груп, полів, кілець»

для студентів
спеціальності 125 «Кібербезпека»

Харків – 2021

УДК 511.17
Р 31

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфокомунікаційної інженерії імені В. В. Поповського Харківського національного університету радіоелектроніки;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна.

Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 5 від 10 червня 2021 року)

Реалізація алгоритму шифрування із правдоподібним запереченням (для чисел довжиною
Р 31 щонайменше 4096 бітів) : методичні рекомендації до лабораторної роботи з дисципліни «Теорія чисел, груп, полів, кілець» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко, Ю. М. Рябуха. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 56 с.

Методичні рекомендації щодо реалізації алгоритму шифрування із правдоподібним запереченням розроблені для здобувачів вищої освіти факультету комп'ютерних наук за спеціальністю «Кібербезпека». У лабораторному практикумі вивчаються різні варіанти побудови алгоритмів шифрування із заперечуванням. Наводяться практичні приклади і лістинги програмних реалізацій з використанням спеціальної бібліотеки NTL. Контроль засвоєння матеріалу здійснюється за результатами завдань для самостійної роботи, які наведені в останньому розділі. Окремі завдання розділені за категоріями складності, тобто у міру збільшення бітової довжини секретних ключів (до 4096 біт), що дозволяє поглибити навички реалізації обчислень з великими числами.

УДК 511.17

Навчальне видання

Кузнецов Олександр Олександрович
Полуяненко Микола Олександрович
Полуяненко Ольга Олександрівна
Рябуха Юрій Миколайович

Реалізація алгоритму шифрування із правдоподібним запереченням (для чисел довжиною щонайменше 4096 бітів)

Методичні рекомендації до лабораторної роботи з дисципліни
«Теорія чисел, груп, полів, кілець»

для студентів спеціальності 125 «Кібербезпека»

Коректор *О. В. Анцибора*
Комп'ютерне верстання *В. В. Савінкова*
Макет обкладинки *І. М. Дончик*

Формат 60 х 84/16. Ум. друк. арк. 2,82. Наклад 50 пр. Зам № 218/2021.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009
Видавництво ХНУ імені В. Н. Каразіна
Тел. 705-24-32

Зміст