МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Людмила Ковальчук
Наталія Маслова

МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ

Електронний навчальний посібник

Рекомендовано Державним вищим навчальним закладом
«Донецький національний технічний університет»
Міністерства освіти і науки України
як електронний навчальний посібник
для здобувачів освіти в закладах вищої освіти

Дрогобич
ДВНЗ «ДонНТУ»
2024

УДК: 512:511:519.72(075.8)
К56

Рекомендовано Вченою Радою Державного вищого навчального закладу «Донецький національний технічний університет» Міністерства освіти і науки України як електроннний навчальний посібник для здобувачів освіти в закладах вищої освіти (Протокол № 9 від 10.10.2024)

Автори:

Л.В. Ковальчук, д-р техн. наук, професор (Державний вищий навчальний заклад «Донецький національний технічний університет»).

Н.О.Маслова, к.т.н., доцент (Державний вищий навчальний заклад «Донецький національний технічний університет»).

Рецензенти:

1) Гулак Геннадій Миколайович, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.
2) Святний В.А., доктор технічних наук, професор, професор кафедри ЕТКІ (Державний вищий навчальний заклад «Донецький національний технічний університет»).

К56 Ковальчук Л.В., Маслова Н.О. Математичні методи криптографії. Електронний навчальний посібник. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 146с.: рис. 3, означень 147, теорем 29, бібліогр. 19.

ISBN 978-966-377-258-5

У електронний навчальний посібник включено елементи абстрактної алгебри, основи теорії чисел, базові поняття й теореми скінченних полів, які є необхідними при вивченні сучасних розділів криптології. Викладення матеріалів спирається на застосування сучасних алгебраїчних методів, й формує математичну основу для вивчення та аналізу криптосистем різного типу. У розділи посібника включено значну кількість прикладів і задач, призначених для спрощення розуміння й засвоєння матеріалу.

Електронний навчальний посібник призначений для здобувачів освіти, які намагаються отримати знання й закріпити навички з математичних основ криптології (криптографії та криптоаналізу).

УДК 512:511:519.72(075.8)

ISBN 978-966-377-258-5

ЗМІСТ

ПЕРЕДМОВА

Матеріали, включені в цей електронний навчальний посібник, призначені для створення математичної основи, необхідної (достатньої) для вивчення різних аспектів криптології — як симетричної, так і асиметричної; як класичної, так і сучасної. Ці розділи алгебри є ключовими для дисципліни, відомої сьогодні як прикладна алгебра.

Абстрактна алгебра вивчає алгебраїчні структури, такі як групи, кільця і поля, які є необхідними як для вивчення теорії чисел, так і для вивчення всіх без винятків розділів сучасної криптології.

Розділи теорії чисел, представлені в електронний навчальний посібнику, є необхідними в першу чергу для створення та аналізу класичних асиметричних криптосистем, які використовують кільця лишків та прості скінченні поля. Крім того, вивчення властивостей простих скінченних полів у рамках курсу теорії чисел підготовлює студентів до роботи з більш складними скінченними полями, які є їх розширеннями.

Повноцінному засвоєнню матеріалу сприяє розв’язування достатньої кількості задач. Тому кожен параграф містить не лише перелік питань для самоконтроля, а й значну кількість задач, багато з яких є авторськими. Задачі підвищеної складності позначені зірочками і зазвичай вимагають кількох нетривіальних кроків для розв’язання, хоча їх рівень складності може відрізнятися.

З метою поглибленого вивчення теорії чисел рекомендується ознайомитись з літературою [1, 3-5]; для отримання додаткових знань з абстрактної алгебри – [6–8]; для більш детального вивчення класичних асиметричних криптосистем – [5, 9], а для ознайомлення з теоретико-числовими алгоритмами, що не увійшли до цього посібника – [10] та [11].

Основи абстрактної алгебри, теорії чисел та криптографії тісно пов’язані між собою, оскільки математичні структури і методи, що розробляються в рамках абстрактної алгебри і теорії чисел, знаходять широке застосування в криптографії. В якості приклада наведемо той факт, що абстрактні алгебраїчні

структури, такі як кільця, групи та поля лежать в основі безпеки Blockchain. Тож наведений у посібнику матеріал має вагоме прикладне застосування, зокрема у криптології, що й відображено у роботах [12–18].

Електронний навчальний посібник здебільшого призначений для студентів прикладних спеціальностей, зокрема «Кібербезпека». Однак він буде корисний і тим, хто хоче окремо вивчати теорію чисел, оскільки містить основні базові результати, подані у вигляді теорем, та допоміжні, представлені як леми. Всі твердження супроводжуються повними та строгими доведеннями.

Електронний навчальний посібник є важливим ресурсом для вивчення основоположних аспектів криптології та криптографії, які базуються на ключових поняттях теорії чисел, такі як подільність, конгруенції, кільця лишків та прості поля, досліджує їх властивості, взаємозв'язки та застосування. Задачі, які включено у посібник, допомагають в кращому засвоєнні матеріалу, стимулюють аналітичне мислення, розвивають навички проблемного розв'язання та фахового застосування.