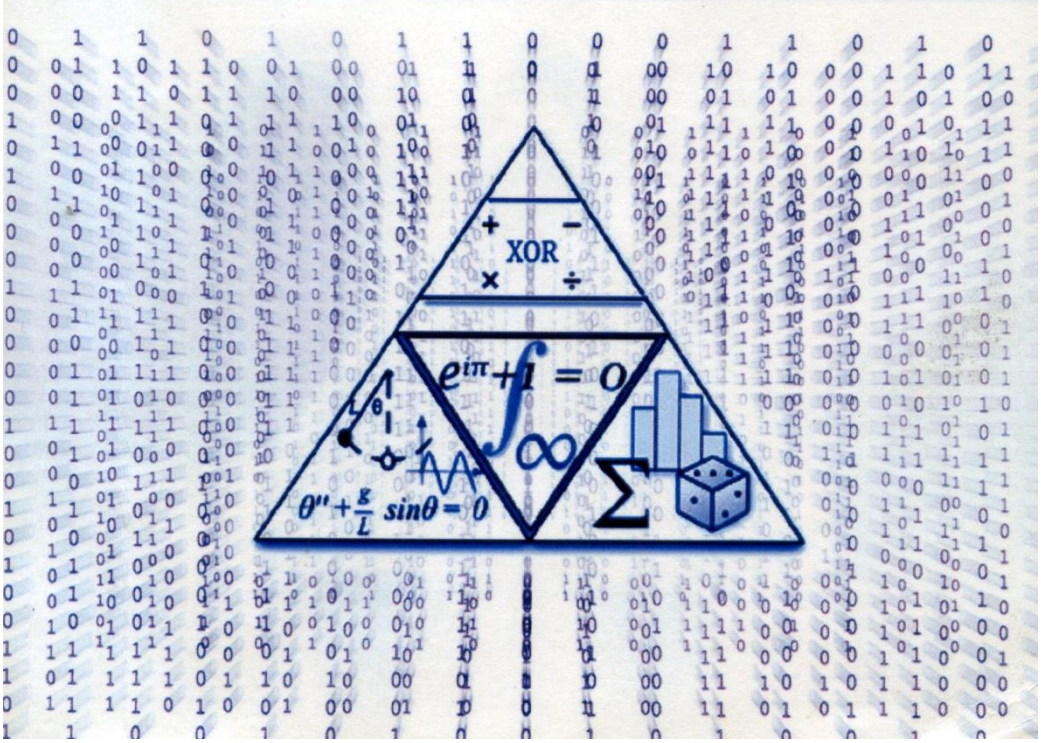
Основи криптографічного захисту інформації



УДК 004.056.55(075)
ББК 32.973я73
О 75

Автори:
Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук

Затверджено Міністерством освіти і науки, молоді та спорту України як підручник для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Управління інформаційною безпекою». Лист № 1/11-7280 від 04.08.2011 року.

Рецензенти:
Г.Ф. Конахович, доктор технічних наук, професор
В.Ю. Богданович, доктор технічних наук, професор
Г.В. Кузнєцов, доктор технічних наук, професор

Основи криптографічного захисту інформації : підручник /
О75 Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
ISBN 978-966-641-430-7

У підручнику розглядаються питання організації та функціонування надійних систем криптографічного захисту інформації. Наведено методику генерації та оцінювання якості псевдовипадкових послідовностей, а також методи генерації псевдовипадкових простих чисел.

Наводяться характеристики стійкості розповсюджених блокових шифрів та асиметричних криптоалгоритмів, описані криптографічно стійкі генератори псевдовипадкових чисел, викладено принципи організації, функціонування та забезпечення надійності інфраструктури відкритих ключів.

Підручник призначено для студентів вищих навчальних закладів та аспірантів, а також фахівців, які займаються криптографією.

УДК 004.056.55(075)
ББК 32.973я73

784719

ISBN 978-966-641-430-7

© Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, 2011

ЗМІСТ