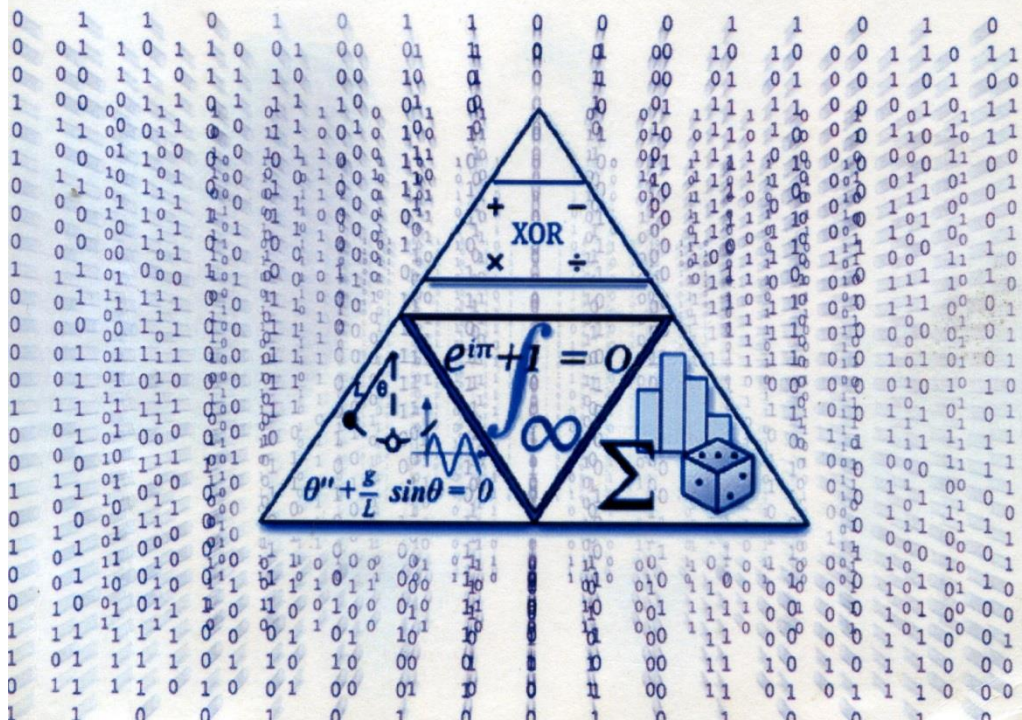


# Основи криптографічного захисту інформації



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. Кузнецов**, 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

ВСТУП.....	6
ГЛАВА 1 ОСНОВНІ ПОНЯТТЯ І ЗАДАЧІ КРИПТОЛОГІЇ.....	8
1.1 Предмет криптології, криптографія і криптоаналіз.....	8
1.2 Моделі відкритого тексту.....	14
1.3 Симетричні і асиметричні криптосистеми.....	17
1.4 Практичні вимоги до симетричних криптосистем.....	19
Питання до розділу 1.....	21
РОЗДІЛ 2 ЕЛЕМЕНТАРНІ ШИФРИ І ЇХ ВЛАСТИВОСТІ.....	23
2.1 Класифікація шифрсистем.....	23
2.2 Властивості елементарних шифрів.....	25
2.3 Теорема Маркова.....	33
Питання до розділу 2.....	33
РОЗДІЛ 3 МОДЕЛІ ЗАГРОЗ БЕЗПЕКИ КРИПТОСИСТЕМ.....	35
3.1 Формальна модель загроз.....	35
3.2 Атаки на симетричні і асиметричні шифрсистеми.....	38
3.3 Теоретична стійкість, абсолютно стійкий шифр.....	41
3.4 Поняття практичної стійкості.....	43
Питання до розділу 3.....	47
РОЗДІЛ 4 ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ І МЕТОДИ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ.....	48
4.1 Дані для формування ключової інформації.....	48
4.2 Статистичне тестування ПВП.....	52
4.3 Генератори псевдовипадкових послідовностей.....	60
Питання до розділу 4.....	71
РОЗДІЛ 5 ПРИНЦИПИ ПОБУДОВИ БЛОКОВИХ ШИФРІВ НА ПРИКЛАДІ АЛГОРИТМУ DES.....	72
5.1 Криптосхема алгоритму DES.....	72
5.2 Криптографічні властивості алгоритму DES.....	77
5.3 Режими роботи блокових алгоритмів.....	82
5.3.1 Режим зчеплення шифрованих блоків (CBC).....	83
5.3.2 Відновлення після помилок у CBC.....	85
5.3.3 Режим зворотного зв'язку з шифром (CFB).....	86
5.3.4 Режим зворотного зв'язку за виходом (OFB).....	88
Питання до розділу 5.....	89

РОЗДІЛ 6 БЛОКОВІ ШИФРИ ГОСТ 28147-89 I RIJNDAEL .....	90
6.1 Схеми шифрування ГОСТ 28147-89 i Rijndael .....	90
6.2 Порівняння раундів шифрування ГОСТ 28147-89 i Rijndael .....	93
6.3 Формування ключових елементів .....	98
6.4 Вибір вузлів замін і констант, дифузійні характеристики .....	100
6.5 Показники стійкості, продуктивності і зручність реалізації алгоритмів .....	104
Питання до розділу 6 .....	109
РОЗДІЛ 7 КРИПТОСИСТЕМИ З ВІДКРИТИМИ КЛЮЧАМИ .....	111
7.1 Односторонні функції з секретом і асиметричні системи .....	111
7.2 Криптосистема RSA .....	114
7.3 Криптосистема Ель-Гамала .....	119
7.4 Криптосистеми на основі еліптичних кривих .....	120
Питання до розділу 7 .....	126
РОЗДІЛ 8 ТЕСТУВАННЯ ЧИСЕЛ НА ПРОСТОТУ І ВИБІР ПАРАМЕТРІВ RSA .....	128
8.1 Тест на основі малої теореми Ферма .....	129
8.1.1 Основні властивості псевдопростих чисел .....	129
8.1.2 Властивості чисел Кармайкла .....	130
8.2 Тест Соловея-Штрассена і Ейлерові псевдопрості числа .....	131
8.3 Тест Рабіна-Міллера і сильні псевдопрості числа .....	134
8.4 Загальні вимоги до вибору параметрів RSA .....	136
8.5 Метод Гордона побудови сильних простих чисел .....	138
8.5.1 Приклад побудови сильного простого числа .....	139
Питання до розділу 8 .....	140
РОЗДІЛ 9 ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПДПИС .....	142
9.1 Забезпечення цілісності і авторства в електронному документообігу .....	142
9.2 Функції хешування .....	147
9.3 Алгоритм SHA-1 .....	149
9.4 Стандарти алгоритмів формування і перевірки ЕЦП .....	151
9.5 Протоколи взаємодії і сертифікати в стандарті X.509 .....	154
9.6 Структура сертифіката відкритих ключів .....	157
9.6.1 Приклад сертифіката в технології Fortezza .....	159
Питання до розділу 9 .....	160

РОЗДІЛ 10 КРИПТОГРАФІЧНІ ПРОТОКОЛИ.....	162
10.1 Поняття криптографічного протоколу .....	162
10.2 Розподіл ключів і аутентифікація .....	164
10.3 Розподіл секрету .....	170
10.4 Стандарти криптопротоколів в Інтернет.....	172
10.4.1 Формальний аналіз криптографічних протоколів.....	176
Питання до розділу 10.....	177
РОЗДІЛ 11 АРХІТЕКТУРА СИСТЕМИ ЕЦП .....	179
11.1 Архітектура системи ЕЦП.....	179
11.2 Управління сертифікатами і ключами.....	184
11.2.1 Резервне зберігання пар ключів .....	186
11.3 Управління інфраструктурою відкритих ключів (РКІ).....	186
11.3.1 Управління політиками.....	188
11.3.2 Реалізація засобів аудиту і зберігання налаштувань в РКІ.....	188
11.4 Проект системи, центри сертифікації ключів.....	189
11.4.1 Акредитація центру сертифікації.....	192
11.4.2 Сертифікація і допуск до експлуатації.....	192
Питання до розділу 11.....	194
ЛІТЕРАТУРА .....	195