

ЗМІСТ

Вступ.....	5
Розділ 1. Основні характеристики криптографічних систем.....	6
1.1. Основні поняття криптології.....	6
1.2. Основні види криптографічних атак (нападів) залежно від відомої інформації.....	7
1.3. Класифікація сучасних криптосистем.....	8
1.4. Основи теорії секретних систем.....	8
1.5. Математична структура секретних систем.....	12
1.5.1. Секретні системи.....	12
1.5.2. Способи зображення систем.....	13
1.5.3. Приклади секретних систем.....	14
1.6. Оцінка секретних систем.....	19
1.7. Алгебра секретних систем.....	20
1.8. Чисті й змішані шифри.....	21
1.9. Подібні системи.....	22
1.10. Теоретична секретність.....	24
1.10.1. Абсолютна секретність.....	24
1.10.2. Ненадійність.....	28
1.10.3. Ідеальні секретні системи.....	32
1.10.4. Приклади ідеальних секретних систем.....	33
1.10.5. Використання ненадійності та надлишковості.....	34
1.11. Практична секретність.....	34
1.11.1. Загальні підходи до розв'язування криптограм.....	34
1.11.2. Статистичні методи.....	36
1.11.3. Метод ймовірних слів.....	39
Питання і задачі для самоконтролю.....	41
Розділ 2. Криптографічні протоколи.....	42
2.1. Вступ у протоколи.....	42
2.2. Передавання інформації з використанням симетричної криптографії.....	46

2.3. Односпрямовані функції	48
2.4. Передавання інформації з використанням криптографії з відкритими ключами	50
2.5. Змішані криптосистеми	51
2.6. Головоломки Меркла	52
2.7. Цифрові підписи	53
2.8. Цифрові підписи і шифрування.....	59
2.9. Генерація випадкових і псевдовипадкових послідовностей	62
2.10. Основні протоколи	63
2.10.1. Обмін ключами	63
2.10.2. Встановлення достовірності	69
2.10.3. Формальний аналіз протоколів перевірки достовірності та обміну ключами	72
2.11. Проміжні протоколи. Вручення бітів.	73
2.12. Розвинені протоколи	75
2.12.1. Докази з нульовим знанням	75
2.12.2. Сліпі підписи	78
2.12.3. Особова криптографія з відкритими ключами	79
2.13. Езотеричні протоколи	80
2.13.1. Безпечні вибори	80
2.13.2. Безпечні обчислення з декількома учасниками.....	84
2.13.3. Електронна готівка ⁸⁷	
Питання для самоконтролю	
Список літератури.....	95