

ЗМІСТ

ВСТУП.....	3
ЛАБОРАТОРНА РОБОТА 1. КВАНТОВІ ЗАГРОЗИ ДЛЯ КЛАСИЧНИХ КРИПТОСИСТЕМ: АНАЛІЗ RSA, ElGamal/DSA/ECDSA.....	4
Вказівки з підготовки до виконання лабораторної роботи.....	4
Теоретичні відомості.....	5
Хід роботи.....	8
Індивідуальне завдання для виконання.....	15
Контрольні запитання.....	16
ЛАБОРАТОРНА РОБОТА 2. ДОСЛІДЖЕННЯ КВАНТОВИХ АЛГОРИТМІВ ТА ЇХ ВПЛИВУ НА КРИПТОГРАФІЧНІ ЗАДАЧІ. АЛГОРИТМ ШОРА.....	18
Вказівки з підготовки до виконання лабораторної роботи.....	18
Теоретичні відомості.....	19
Хід роботи.....	24
Індивідуальне завдання для виконання.....	26
Контрольні запитання.....	28
ЛАБОРАТОРНА РОБОТА 3. ДОСЛІДЖЕННЯ КВАНТОВИХ АЛГОРИТМІВ ТА ЇХ ВПЛИВУ НА КРИПТОГРАФІЧНІ ЗАДАЧІ. АЛГОРИТМ ГРОВЕРА.....	30
Вказівки з підготовки до виконання лабораторної роботи.....	30
Теоретичні відомості.....	31
Хід роботи.....	33
Індивідуальне завдання для виконання.....	35
Контрольні запитання.....	36

ЛАБОРАТОРНА РОБОТА 4. ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ХЕШ-ФУНКЦІЙ ТА ЇХ СТІЙКОСТІ В КЛАСИЧНІЙ І КВАНТОВІЙ МОДЕЛЯХ: BIRTHDAY ATTACK (АТАКА ДНЯ НАРОДЖЕННЯ) ТА АЛГОРИТМ ВНТ (BRASSARD-HØYER-TAPP ALGORITHM).....	38
Вказівки з підготовки до виконання лабораторної роботи.....	38
Теоретичні відомості.....	39
Хід роботи.....	41
Індивідуальне завдання для виконання.....	43
Контрольні запитання.....	45
ЛАБОРАТОРНА РОБОТА 5. ДОСЛІДЖЕННЯ БЕЗПЕКИ БЛОЧНИХ ШИФРІВ ТА ЇХ СТІЙКОСТІ ДО КВАНТОВИХ АТАК.....	47
Вказівки з підготовки до виконання лабораторної роботи.....	47
Теоретичні відомості.....	48
Хід роботи.....	52
Індивідуальне завдання для виконання.....	55
Контрольні запитання.....	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	58
ДОДАТКИ.....	59
ДОДАТОК А. Програмний код для RSA ТА DSA/ECDSA подібної схеми.....	59
ДОДАТОК Б. Алгоритм Шора.....	64
ДОДАТОК В. Алгоритм Гровера.....	74
ДОДАТОК Г. Програмний код схеми Even–Mansour та імітація атаки ВНТ.....	80