

ЗМІСТ

ВСТУП	3
1 КРИПТОГРАФІЯ З PYTHON	6
1.1 Загальні відомості про криптографію	6
1.2 Основна термінологія криптографії	7
1.3 Шифрування.....	8
1.3.1 Подвійне шифрування	8
1.3.2 Гібридна криптографія	9
2 ЗАГАЛЬНІ ВІДОМОСТІ PYTHON.....	10
2.1 Мова програмування Python	10
2.2 Установка Python	12
2.3 Основи написання програм.....	14
2.4 Змінні та типи даних.....	18
2.5 Операції з числами.....	21
2.6 Умовні вирази	27
2.7 Операції з рядками.....	30
2.8 Умовні конструкції.....	33
2.9 Цикли.....	36
2.10 Функції.....	40
3 КРИПТОГРАФІЯ З PYTHON	46
3.1 Зворотний шифр	46
3.2 Шифр Цезаря.....	47
3.2.1 Алгоритм шифру Цезаря.....	47

3.2.2 Злом шифру Цезаря	49
3.3 Алгоритм ROT13	50
3.4 Транспозиційний шифр	53
3.4.1 Шифрування транспозиційного шифру.....	55
3.4.2 Розшифровка транспозиційного шифру.....	57
3.5 Шифрування файлів	59
3.6 Розшифровка файлів.....	62
3.7 Base64 кодування і декодування	65
3.7.1 Програма для кодування.....	66
3.7.2 Програма для декодування	66
3.8 Різниця між ASCII і base64	67
3.9 Криптографія з Python - процес XOR.....	67
3.9.1 Алгоритм	68
3.10 Мультиплікативний Шифр	69
3.11 Криптографія з Python – Афіний Шифр	72
3.12 Злом моноалфавітного шифру	73
3.12.1 Моноалфавітний шифр.....	73
3.13 Простий підстановлювальний Шифр	77
3.13.1 Тестування простого підстановлювального шифру.....	79
3.13.2 Розшифровка простого підстановлювального шифру	82
4 МОДУЛІ КРИПТОГРАФІЇ PYTHON.....	84
4.1 Модуль криптографії.....	84
4.2 Розуміння VignereCipher	87

4.3 Впровадження VignereCipher.....	90
4.4 Одноразовий шифрувальний блок.....	92
4.5 Впровадження OneTimePadCipher.....	93
5 СИМЕТРИЧНА І АСИМЕТРИЧНА КРИПТОГРАФІЯ.....	96
5.1 Симетрична криптографія	96
5.2 Стандарт шифрування даних (DES).....	96
5.3 Асиметрична криптографія	98
6 РОЗУМІННЯ АЛГОРИТМУ RSA	101
6.1 Алгоритм	101
6.2 Створення ключів RSA	103
6.3 Генерація ключів RSA.....	103
6.3.1 Алгоритми генерації ключів RSA.....	103
Модуль Кріптомата.....	103
Модуль РабінМіллер.....	104
7 ШИФРУВАННЯ RSA	109
7.1 Шифрування RSA	110
7.2 Авторизація	111
7.3 Аутентифікація	112
7.4 Шифрування RSA	112
7.5 Злом RSACipher	114
ЗМІСТ.....	117