МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

КІБЕРБЕЗПЕКА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

та варіанти завдань

для студентів-бакалаврів галузі знань 12 Інформаційні технології

(перша навчальна комп'ютерна практика)

Дніпро
2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

КІБЕРБЕЗПЕКА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

та варіанти завдань

для студентів-бакалаврів галузі знань 12 Інформаційні технології

(перша навчальна комп'ютерна практика)

Дніпро
НТУ «ДП»
2019

Саксонов Г.М.

Кібербезпека. Методичні рекомендації та варіанти завдань для студентів-бакалаврів галузі знань 12 Інформаційні технології (перша навчальна комп'ютерна практика) / Упоряд.: Г.М. Саксонов, О.А. Жукова, І.А. Сечкін ;

М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2019. – 13 с.

Упорядники:

Г.М. Саксонов, ст. викл.;

О.А. Жукова, доц.;

І.А. Сечкін, асист.

Затверджено методичною комісією зі спеціальності 125 Кібербезпека (протокол № 7 від 07.03.2019) за поданням кафедри безпеки інформації та телекомунікацій (протокол № 7 від 07.03.2019).

Подано методичні рекомендації та завдання для студентів-бакалаврів галузі знань 12 Інформаційні технології (Кібербезпека) .

Відповідальний за випуск зав. кафедри БІТ В.І. Корнієнко, д-р техн. наук, проф.

ЗАВДАННЯ 1

Мета роботы

Метою роботи є закріплення знань і умінь програмування на мові C/C++ при створенні реальної програми шифрування\ дешифрування тексту.

Найменування роботи

Розробка програми шифрування\ дешифрування тексту методом простої заміни.

Вимоги до роботи

Звіт з І-ої навчальної комп'ютерної повинен містить:

- Пояснювальну записку
- Програму шифрування\ дешифрування .
- Файли з початковим текстом, шифротекстом і тексто, що дешифрується.

Зміст пояснювальної записки

- Титульний лист.
- Завдання до роботи.
- Зміст.
- Укрупнена схема алгоритму.
- Початкові тексти програми шифрування\ дешифрування .
- Зміст файлів з початковим текстом, шифротекстом і дешифрованим текстом.

Зразок титульного листа приведений у додатку 1, а зразок завдання - в додатку 2.

Вимоги до програм шифрування і дешифровки

Програма шифрування\ дешифрування тексту повинна бути розроблена на мові програмування *C/C++* з використанням компіляторів *MS VisualC ++* і виконуватися як консольне застосування.

Програма повинна бути обратима, т.е застосована до відритого тексту повинна створювати шифротекст, а застосована до шифротексту тексту - повинна створювати файл з відкритим текстом.

Ці програми повинні використовувати один і той же ключ для шифрування (ПШ) і дешифровки (ПД) тексту.

При успішному виконанні програми ПШ і ПД зміст файлів повинен бути однаковим.

Варіант застосування програми в режимі шифруванні або дешифровки повинен здійснюватися параметром командного рядка при запуску програми.

1.1.Вимога до формування файлів

Текстовий файл з початковим текстом повинен містити не менше 200 *ASCII* символів довільного осмисленого тексту і може формуватися будь-яким текстовим редактором. Текст повинен бути розташованим по рядках не більше 80 символів.

Шифротекст, що формується програмою шифрування початкового тексту, повинен бути представлений файлом *Output.txt*. Дешифрований текст, відновлений з файлу *Output.txt*, повинен бути текстом, складеним з *ASCII* символів, і може складатися з довільного числа рядків будь-якої довжини.

2. Основи шифрування тексту методом простій заміни

2.1.Термінологія

Метод и способ преобразования исходного текста с целью его защиты от незаконных пользователей называется шифрованием(???).

Шифрування – оборотне перетворення інформації в цілях захована від неавторизованих осіб. Головним чином, шифрування служить завданням дотримання конфіденційності передаваної інформації.

Дешифровка – процес зворотний шифруванню, тобто перетворення шифрованого повідомлення в початковий текст.

Ключ – якась послідовність символів, що визначає перетворення початкового тексту в шифротекст.

2.2. Шифрування методом простій заміни

Найбільш відомими і часто використовуваними шифрами є шифри заміни. Вони характеризуються тим, що окремі частини початкового тексту замінюються на яких-небудь інші букви, числа, символи і тому подібне. При цьому заміна здійснюється так, щоб потім по шифрованому повідомленню можна було однозначно відновити передане повідомлення. Наприклад, кожній букві англійського алфавіту ставиться у відповідність якась інша буква цього ж алфавіту.

В ході виконання завдання 1-ої навчальної комп'ютерної практики пропонується якийсь умовний метод шифрування, заснований на методі шифрування Віжінера.

Суть цього методу полягає в наступному.

Початковий текст задається набором символів m_i, де $i = 0, n$.

Наприклад, для початкового тексту «Це курсова робота» n=18 і при цьому m_0=’Э’, m_1=’т’, m_3=’ ’ ,…, m_6=‘р’.

Користувач програми шифрування задає ключ, тобто якийсь довільний набір символів k_j, де $j = 0, L$.

При цьому $m<<n$, тобто довжина ключа значно менше довжини початкового тексту. Приклад ключа «*SuperStar*»: $L = 8$, k_0 = ’S’, k_1 = ’u’, , k_5=’ S’.

Ключ «підписується» з повторенням під початковим повідомленням.

Для початкового прикладу це виглядатиме у вигляді масиву *S[2][n]*

Початковий текст	Э	т	о		к	у	р	с	о	в	а	я		р	а	б	о	т	а
Ключ з повторенням	S	u	p	e	r	S	t	a	r	S	u	p	e	r	S	t	a	r	S

Повтор ключа здійснюється до тих пір, поки не завершитися початковий текст.

Символьний масив *S* перетвориться в масив A[2][n], елементи якого є цілими числами, що визначається *ASCII* кодом відповідного елементу масиву *C*.

Наприклад,*

Початковий текст	76	78	56	…	70
Ключ з повторенням	43	51	98	…	49

Складається вектор V_i, де $i = 0,$,n, елементи якого визначаються як

$V_i=A_{1i} \oplus A_{2i,}$ де $\oplus$ - операція того, що «виключає або».

* В даному прикладі *ASCII*-коди не відповідають *ASCII*-кодам букв повідомлення, приведеного вище.

Елементи вектора *V* також будуть цілими числами.

З цілочисельного вектора *V* формується символьний вектор *W* елементами якого будуть символи, *ASCII* коди яких відповідатимуть символам вектора *V*.

Кожен символ вектора *W* послідовного заноситься у файл *Output.txt.*

2.3. Дешифровка шифротексту

Дешифровка шифротексту здійснюється на основі бітової операції $\oplus$ для якої справедливо

$$m_i \oplus k_i = c_i$$
$$c_i \oplus k_i = m_i$$

де m_i – символ початкового тексту

k_i – символ ключа

c_i – шифрований символ

Таким чином, якщо до шифрованого символу знов застосувати операцію $\oplus$ з тим же символом ключа, що і при шифруванні, то результатом буде початковий символ. Тому дешифровка шифротекста проводиться в зворотному порядку процесу шифрування.

У **кожному варіанті** роботи потрібна розробка програми шифрування \ дешифровки тексту по описаних вище правилах. Відмінність варіантів виконання роботи полягає в різних способах введення і перетворення даних програм.

2.4. Способи введення ключа в програму шифрування тексту (позначається *B1*)

- **B1=1** – текст ключа вводиться користувачем програми з клавіатури.
- **B1=2** – текст ключа вводиться користувачем як параметр командного рядка при запуску програми.

Щоб задати аргументи командного рядка для відладки треба

— *Вибравши проект* ***в Оглядачі рішення****, в меню* ***Проект*** *виберіть команду* ***Свойства конфігурації***

— *Перейдіть на вкладку* ***Відладка.***

— *У полі* ***Аргументи командного рядка*** *введіть аргументи командного рядка, які використовуватимуться.*

- **B1=3** – текст ключа є заздалегідь підготовленим текстом файлу на диску.

2.5. Спосіб введення ключа в програму дешифровки тексту (позначається *B2*)

- **B2=1** – текст ключа вводиться користувачем програми дешифровки з клавіатури.
- **B2=2** – текст ключа вводиться користувачем програми дешифровки як параметр командного рядка при запуску програми.
- **B2=3** – текст ключа є заздалегідь підготовленим текстом файлу на диску.

2.6. Спосіб обліку і перетворення регістра символів (позначається ***R*****)**

При шифруванні і дешифровці тексту можемо враховувати відмінність коду *ASCII* між заголовними і прописними символами тексту ключа і початкового тексту або перетворювати всі символи до заголовних, або прописним символам. Способи такої відмінності позначаються як *R*:

- **R=1** – всі символи ключа перетворяться в прописні, а символи початкового тексту в заголовних.
- **R=2** – всі символи ключа перетворяться в заголовні, а символи початкового тексту в прописні.
- **R=3** – всі символи ключа і початкового тексту прописні.
- **R=4** – всі символи ключа і початкового тексту заголовні.
- **R=5** – символи ключа і початкового тексту не перетворяться.

3. Спосіб підстановки рядка символів ключа

Позначимо як *P* спосіб підстановки рядка символів ключа. При описі методу шифрування передбачалося, що символи тексту ключа підставляються з повторенням, починаючи з першого символу ключа.

- пряма підстановка, при якій ***P=1*.**

Наприклад,

Початковий текст	Э	Т	о		к	у	р	с	о	в	а	я		р	а	б	о	т	а
Ключ з повторенням	S	U	p	e	r	S	t	a	r	S	u	p	e	r	S	t	a	r	S

- зворотна підстановка (*P=2*) – коли символи ключа розташовуються в зворотному порядку.

Наприклад,

Початковий текст	Э	Т	о		к	у	р	с	о	в	а	я		р	а	б	о	т	а
Ключ з повторенням	r	A	t	S	r	e	p	u	S	r	a	t	S	r	e	p	u	S	R

- комбінована підстановка (*P=3*) – коли символи ключа розташовуються в прямому і зворотному порядку по черзі.

Наприклад,

Початковий текст	Э	Т	о		К	у	р	с	о	в	а	я		р	а	б	о	т	а
Ключ з повторенням	S	u	p	e	R	S	t	a	r	r	a	t	S	r	e	p	u	S	S

НОМЕРИ ЗАВДАНЬ

№	B1	B2	R	P	№	B1	B2	R	P	№	B1	B2	R	P	№	B1	B2	R	P
1	1	1	1	1	**28**	1	1	4	1	**55**	1	1	2	2	**82**	1	1	5	3
2	2	1	1	1	**29**	2	1	4	1	**56**	2	1	2	2	**83**	2	1	5	3
3	3	1	1	1	**30**	3	1	4	1	**57**	3	1	2	2	**84**	3	1	5	3
4	1	2	1	1	**31**	1	2	4	1	**58**	1	2	2	2	**85**	1	2	5	3
5	2	2	1	1	**32**	2	2	4	1	**59**	2	2	2	2	**86**	2	2	5	3
6	3	2	1	1	**33**	3	2	4	1	**60**	3	2	2	2	**87**	3	2	5	3
7	1	3	1	1	**34**	1	3	4	1	**61**	1	3	2	2	**88**	1	3	5	3
8	2	3	1	1	**35**	2	3	4	1	**62**	2	3	2	2	**89**	2	3	5	3
9	3	3	1	1	**36**	3	3	4	1	**63**	3	3	2	2	**90**	3	3	5	3
10	1	1	2	1	**37**	1	1	5	2	**64**	1	1	3	2	**91**	1	1	1	3
11	2	1	2	1	**38**	2	1	5	2	**65**	2	1	3	2	**92**	2	1	1	3
12	3	1	2	1	**39**	3	1	5	2	**66**	3	1	3	2	**93**	3	1	1	3
13	1	2	2	1	**40**	1	2	5	2	**67**	1	2	3	2	**94**	1	2	1	3
14	2	2	2	1	**41**	2	2	5	2	**68**	2	2	3	2	**95**	2	2	1	3
15	3	2	2	1	**42**	3	2	5	2	**69**	3	2	3	2	**96**	3	2	1	3
16	1	3	2	1	**43**	1	3	5	2	**70**	1	3	3	2	**97**	1	3	1	3
17	2	3	2	1	**44**	2	3	5	2	**71**	2	3	3	2	**98**	2	3	1	3
18	3	3	2	1	**45**	3	3	5	2	**72**	3	3	3	2	**99**	3	3	1	3
19	1	1	3	1	**46**	1	1	1	2	**73**	1	1	4	3	**100**	1	1	2	3
20	2	1	3	1	**47**	2	1	1	2	**74**	2	1	4	3	**101**	2	1	2	3
21	3	1	3	1	**48**	3	1	1	2	**75**	3	1	4	3	**102**	3	1	2	3
22	1	2	3	1	**49**	1	2	1	2	**76**	1	2	4	3	**103**	1	2	2	3
23	2	2	3	1	**50**	2	2	1	2	**77**	2	2	4	3	**104**	2	2	2	3
24	3	2	3	1	**51**	3	2	1	2	**78**	3	2	4	3	**105**	3	2	2	3
25	1	3	3	1	**52**	1	3	1	2	**79**	1	3	4	3	**106**	1	3	2	3
26	2	3	3	1	**53**	2	3	1	2	**80**	2	3	4	3	**107**	2	3	2	3
27	3	3	3	1	**54**	3	3	1	2	**81**	3	3	4	3	**108**	3	3	2	3

ЛІТЕРАТУРА

1. Аршинов М.Н., Садовский Л.Е. Коды и математика, - М., Наука, 1983.
2. Домашев А.В., Попов О.В., Правиков Д.И., Прокофьев И.В. Щербаков А.Ю. Программирование алгоримов защиты информацыии. Учебное пособие. – М.: «Нолидж», 2000.
3. Новиков Ф.А. Дискретная математика для программистов, - СПб: Питер, 2001.
4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976.
5. Цикоза В.А., Чурина Т.Г. Методы программирования. Ч-1,- Новосибирск, 1999.
6. Ященко В.В. Введение в криптографию, - СПб: Питер, 2001.

Додаток 1

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗВІТ
з виконання
І-ої навчальної комп'ютерної практики

ВИКОНАВ

студент групи

_____

ПЕРЕВІРИВ

_____

Дніпро
201___

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАВДАННЯ

Спеціальность_____
Група _____
П.І.Б. студента_____

Тема роботи

_____
_____
_____

Завдання видав _____

Завдання прийняв _____

Упорядники:

Саксонов Геннадій Михайлович

Жукова Олена Андріївна

Сечкін Ігор Арнольдович

КІБЕРБЕЗПЕКА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

та варіанти завдань

для студентів-бакалаврів галузі знань 12 Інформаційні технології

(перша навчальна комп'ютерна практика)

Видано в редакції упорядників

Комп'ютерний дизайн, верстка та обробка – О.А. Жукова

Підписано до друку 25.04.2019. Формат 30х42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 0,7.
Обл.-вид. арк. 0,7. Тираж 6 пр. Зам. №

Національний технічній університет «Дніпровська політехніка»

49005, м. Дніпро, просп. Д. Яворницького, 19