План лабораторного заняття № 4
Тема № 2 “Криптографічні методи захисту інформації”

Навчальний час: 4 год.

Міжпредметні зв’язки: навчальна дисципліна “Захист інформації в інформаційних системах” взаємопов’язана з такими дисциплінами як “Економіко-математичне моделювання”, “Інформатика” та ін.

Мета і завдання лабораторного заняття: ознайомлення з найбільш простими методами шифрування.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Опишіть алгоритм шифрування за допомогою шифру Віженера.
2. Що можна сказати про криптографічну стійкість шифру Віженера?
3. Назвіть переваги шифру Віженера.
4. Які недоліки має шифр Віжерена?
5. У якому випадку шифр Віженера буде важко зламати?

Завдання:

1. Для першої підгрупи студентів автоматизувати процес шифрування слова на англійській мові на основі шифру Віженера (див.табл.1).

Ключ обрати таким за правилом:

k+m, де k – перша цифра у порядковому номері студента у підгрупі, m – друга цифра порядкового номеру.

2. Для другої підгрупи студентів автоматизувати процес шифрування слова на українській мові на основі шифру Віженера (див.табл.2).

Ключ обрати таким за правилом:

k+m, де k – перша цифра у порядковому номері студента у підгрупі, m – друга цифра порядкового номеру.

Оформити звіт.

Хід виконання лабораторної роботи:

Метод Цезаря ліг в основу дещо складніших алгоритмів, наприклад шифру Віженера. Варіант шифру зсуву ROT13 використовується в англомовному сегменті Інтернету для приховування спойлерів, розгадок головоломок тощо. Шифр Віженера (фр. Chiffre de Vigenère) – метод поліалфавітного шифрування літерного тексту з використанням ключового слова.

Шифр Віженера є шифром подстановки, тобто шифром, у якому кожна літера початкового тексту заміняється літерою шифр-тексту. Для взлому таких шифрів використовується частотний криптоаналіз.

Шифр Віженера складається з послідовності декількох шифрів Цезаря з різними значеннями зсуву. Для зашифровування може використовуватися таблиця алфавітів, так звана tabula recta або квадрат (таблиця) Віженера (рис.1). Стосовно до латинському алфавіту таблиця Віженера складається з рядків по 26 символів, причому кожен наступний рядок зсувається на декілька позицій. Таким чином, в таблицю виходить 26 різних шифрів Цезаря.

Ключ утворюється послідовністю літер k_1, k_2,.., k_i. Першу літеру повідомлення зсувають на величину ключа k_1, другу літеру повідомлення – на k_2 і т.д. Якщо ключ k_1, k_2,.., k_i вже перебрано, а літери в повідомленні ще залишаються, то ключ знову застосвують до тих літер повідомлення, які ще не були зашифровані. Це можна представити у вигляді:

$$E(m_i) = (m_i+k_i) \mathrm{mod} N, \qquad (1)$$

де m_i – поточна літера повідомлення, N – число літер в алфавіті, k_i – літера ключа.

Так, якщо якщо літерою ключа вибрано A, тобто k_i=A, то (m_i+k_i)=0 (немає зсуву),
Якщо k_i=B, то (m_i+k_i)=1 (зсув на 1),
k_i=C, то (m_i+k_i)=2 (зсув на 2),
k_i=D, то (m_i+k_i)=3 (зсув на 3),
k_i=E, то (m_i+k_i)=4 (зсув на 4), і т.д.

Головний недолік шифру полягає в тому, що його ключ повторюється.

Зауваження. Оскільки алфавіт – англійський, то N=26 (число літер в алфавіті). Нехай користувач вирішив використати ключ – DAFB, тобто D зсуває на 3 позиції літеру, A – не зсуває, F – на 5, B – на одну позицію.

Англійський алфавіт: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Припустимо, що потрібно зашифрувати слово “PROGRAMM”. Тоді алгоритм шифрування (формула (1)) з використанням ключа DAFB буде мати вигляд:

Для першої літери P слова PROGRAMM буде використано першу літеру ключа – D:

E(P)=(P+D)=S

Для шифрування 2-ї літери R у повідомленні буде використана наступна літера ключа – A:

E(R)=(R+A)=R.

Для шифрування літери O застосовується літера ключа F:

E(O)=(O+F)=T

Для літери G – літера ключа B:

E(G)=(G+B)=T і т.д.

Таблиця 1

Таблиця Віженера для англійського алфавіту
(по вертикалі вибираємо літери відкритого тексту, а по горизонталі – ключа, на перетині цих значень отримуємо знаки шифротексту)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Таблиця 2

Таблиця Віженера для українського алфавіту
(по вертикалі вибираємо літери відкритого тексту, а по горизонталі – ключа, на перетині цих значень отримуємо знаки шифротексту)

	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
а	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
ґ	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	ї	і	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

Додаткові завдання для студентів: опрацювання теоретичного матеріалу теми, написати план-конспект заняття за вибраною темою із використанням демонстраційного матеріалу.

Форми контролю знань – презентація виконаних завдань, обговорення виконаних завдань.

Рекомендована література до теми лабораторного заняття:

Основна та допоміжна література:

1. Харин Ю.С. Математические основы криптологии: учеб.пособ. / Ю.С.Харин, В.И.Берник, Г.В.Матвеев. – Мн.: БГУ, 1999. – 319 с.
2. Зима В. Безопасность глобальных сетевых технологий / В.Зима, А.Молдован, Н.Молдован. – СПб.: БХВ-Петербург, 2003. – 368 с.
3. Щербаков А. Прикладная криптография / А. Щербаков, А.Домашев. – М., 2003. – 404 с.

4. Пономаренко Н.Н. Защита информации в телекоммуникационных системах: учеб. пособ. / Н. Н. Пономаренко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк.авиац.ин-т», 2015. – 40 с.
5. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин,
6. А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
7. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/

Інтернет-ресурси:
https://books.ifmo.ru/file/pdf/56.pdf
http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002

Обладнання заняття, ТЗН тощо: комп'ютери.

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики
(підпис) (ПІБ, посада, науковий ступінь, вчене звання)