МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Кафедра прикладної математики

04-01-26

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з навчальної дисциплін **"Основи захисту і кодування інформації"** для студентів спеціальності 113 "Прикладна математика" денної форми навчання

Рекомендовано науково-методичною
комісією зі спеціальності
113 "Прикладна математика"
Протокол № 4
від 12 грудня 2016 року

Рівне - 2017

Методичні вказівки до виконання лабораторних робіт з навчальної дисциплін **"Основи захисту і кодування інформації"** для студентів спеціальності 113 "Прикладна математика" денної форми навчання / Рощенюк А.М. - Рівне, НУВГП, 2017. - 22 с.

Упорядник:
Рощенюк А.М. - ст. викладач кафедри прикладної математики.

ЗМІСТ

Лабораторна робота № 1

Тема: Шифри заміни

Мета: вивчити шифри заміни та їх властивості, вміти виконувати процедури шифрування та дешифрування.

Теоретична частина:

Найпростіший моноалфавітний шифр - **адитивний шифр**, його іноді називають **шифром зрушення**, а іноді - **шифром Цезаря**, але термін адитивний шифр краще показує його математичний зміст.

Припустимо, що текст складається з маленьких літер (від a до z) а зашифрований текст складається із великих літер (від A до Z). Щоб забезпечити застосування математичних операцій до вхідного й зашифрованого текстів, ми ставимо у відповідність кожній літері (для нижнього й верхнього регістру) числове значення, як це показане в табл. 1.

Таблиця 1.

Кодова таблиця латинських літер

Вихідний текст	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
Зашифров. текст	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
Числове значення	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Приклад.

Зашифрувати повідомлення "hello" за допомогою

а) адитивного шифру з ключем = 15;

б) мультиплікативний шифр із ключем = 7;

Рішення:

а) Ми застосовуємо алгоритм кодування вхідного тексту, буква за буквою:

Вхідний текст		Шуфрування	Шифрований текст	
h	07	(07+15) mod 26	22	W
e	04	(04+15) mod 26	19	T
l	11	(11+15) mod 26	00	A
l	11	(11+15) mod 26	00	A
o	14	(14+15) mod 26	03	D

Результат - "WTAAD".

Зверніть увагу, що шифр моноалфавитний, тому що два відображення однієї і тієї ж букви (l) вихідного тексту, зашифровані як один і той же символ (A).

б) У мультиплікативному шифрі алгоритм шифрування застосовує множення вихідного тексту на ключ, а алгоритм дешифрування застосовує поділ зашифрованого тексту на ключ.

Вхідний текст		Шуфрування	Шифрований текст	
h	07	(07*07) mod 26	23	X
e	04	(04*07) mod 26	02	C
l	11	(11*07) mod 26	25	Z
l	11	(11*07) mod 26	25	Z
o	14	(14*07) mod 26	20	U

Результат - "XCZZU".

Ми можемо комбінувати адитивні і мультиплікативні шифри, щоб отримати те, що названо **аффінним шифром** - комбінацією обох шифрів з парою ключів. Перший ключ використовується мультиплікативним шифром, другий - адитивним шифром. Для шифрування $C = (P * k_1 + k_2) \bmod 26$.

Практична частина:

1. Створити головну форму (меню) та заповнити підписами і кнопками (заголовок - назва дисципліни; меню - тема лабораторної роботи; тема №1 - шифр заміни...)

2. Зашифруйте повідомлення (своє ПІП), використовуючи один з наступних шифрів:

- адитивний шифр із ключем, де ключ номер варіанту;
- мультиплікативний шифр із ключем номер варіанту +3;
- афінний шифр із ключами: номер варіанту та номер варіанту+3.

3. Запишіть Ваше зашифроване повідомлення на листку та здайте викладачу.

4. Розшифрувати наступні повідомлення (дані викладачем), зашифровані з застосованням: адитивного, мультиплікативного та афінного шрифтів.

5. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу.

Контрольні питання:

1. Яка структура адитивного шифру?
2. Яка структура мультиплікативного шифру?
3. Яка структура афінного шифру?
4. Криптоаналіз адитивного шифру - це ...
5. Що таке моноалфавітні шрифти? Навести приклад.
6. Що таке багатоалфавітні шрифти? Навести приклад.
7. Що розуміється під атакою грубої сили.
8. Перерахуйте чотири види атак криптоаналізу.

Лабораторна робота № 2

Тема: Шифр Плейфера та подвійного квадрата

Мета: вивчити шифр Плейфера та подвійного квадрата, вміти виконувати процедури шифрування та дешифрування.

Теоретична частина:

Найбільш відомий шифр біграмами називається **Плейфер** (Playfair). Він застосовувався Великобританією в Першу світову війну. Відкритий текст розбивався на пари букв (біграми) і текст шифровки будувався з нього за правилами, що наводяться нижче.

Ключ засекречування в **шифрі Плейфера** містить 25 літер алфавіту, розміщених в матриці 5x5 (літери I і J розглядаються при шифруванні як однакові). За допомогою різного розміщення букв у матриці можна створити багато різних ключів засекречування.

Секретний ключ=

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

Рис. 1. Приклад секретного ключа Плейфера

Перед шифруванням вихідний текст розбивається на пари; якщо дві літери у парі однакові, то для їх виокремлення вставляється фіктивна літера. Якщо після вставки фіктивної літери число символів в початковому тексті непарне, то в кінці додається ще один фіктивний символ.

Шифр використовує три наступні правила:

а) якщо дві літери-пари розташовані в одному і тому ж рядку таблиці ключа засекречування, відповідний шифруючий символ для кожної літери - наступний символ праворуч в тому ж самому рядку (з поверненням до початку рядка, якщо символ вихідного тексту - останній символ в рядку);

б) якщо ці дві літери-пари розташовані в одному і тому ж стовпці таблиці ключа засекречування, відповідний шифруючий символ для кожної літери - символ нижче нього в тому ж самому стовпці (з поверненням до початку стовпчика, якщо символ вихідного тексту - останній символ в стовпці);

в) якщо ці дві літери-пари не перебувають в одному рядку або стовпці таблиці засекречування, відповідний шифруючий символ для кожної літери - символ, який знаходиться в цьому ж рядку, але в тому ж самому стовпці, що й інший символ.

Приклад 1.

Нехай нам потрібно зашифрувати вихідний текст **"hello"**, що використовує ключі відображені на Рис. 1. Коли ми групуємо літери по парам,

ми отримуємо "**he**, **ll**, **o**", дві однакові літери "**l**", отже, повинні вставити будь-який символ, наприклад "**x**" між двома літерами "**l**", після чого отримаємо "**he**, **lx**, **lo**".

Після шифрування маємо: **he -> EC** **lx -> QZ** **lo -> BX**.

Оригінальний текст: **hello** Зашифрований текст: **ECQZBX**.

З цього прикладу ми можемо бачити, що наш шифр - фактично багатоалфавітний шифр: дві появи літери "**l**" зашифровуються як "**Q**" і "**B**".

Приклад 2.

Використовуючи для шифрування код (див. рис. 2.), зашифрувати вихідний текст "*нехай консули будуть уважні*".

П	Р	И	К	Л	А	Д	Б
В	Г	Е	Є	Ж	З	І	Ї
Й	М	Н	О	С	Т	У	Ф
Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Рис. 2. Приклад секретного ключа Плейфера

Повідомлення:	не	ха	йк	он	су	ли	бу	ду	ть	ув	аж	ні
Шифровка:	ЧН	ЬП	ОП	СО	ТФ	АК	ДФ	Ю	ЬА	ЙІ	ЛЗ	УЕ

Зашифрований текст: ЧН ЬП ОП СО ТФ АК ДФ Ю ЬА ЙІ ЛЗ УЕ

Шифр подвійного квадрату

Даний шифр на перший погляд не відрізняється від шифру Плейфера. Для шифрування він використовує дві таблиці, однак ці, здавалося б і не настільки значні зміни привели до появи на світ нової криптографічної системи ручного шифрування. Вона виявилася така надійна і зручна, що застосовувалася німцями навіть у роки Другої Світової війни. Шифрування методом подвійного квадрата дуже просте.

Наведемо приклад використання шифру «подвійний квадрат» для українських текстів. Маємо дві таблиці з випадково розташованими в них алфавітами:

Ч		В	І	П
О	К	Й	Д	У
Г	Ш	З	Є	Ф
Л	Ї	Х	А	,
Ю	Р	Ж	Щ	Н
Ц	Б	И	Т	Ь
.	С	Я	М	Е

Е	Л	Ц	Й	П
.	Х	Ї	А	Н
Ш	Д	Є	К	С
І		Б	Ф	У
Я	Т	И	Ч	Г
М	О	,	Ж	Ь
В	Щ	З	Ю	Р

Для шифрування повідомлення розбиваються на біграми. Перша літера біграма знаходиться в лівій таблиці, а друга в правій. Потім будується уявний

прямокутник так, щоб літери біграми лежали в його протилежних вершинах. Інші дві вершини цього прямокутника дають літери шифровки.

Припустимо, що шифрується біграм тексту ОЖ - отримаємо біграм АЦ.

Якщо обидві літери біграми повідомлення лежать в одному рядку, то і шифруючи літери беруться з цього ж рядка. Перша літера біграма шифровки береться з лівої таблиці в стовпці, що відповідає другій літері біграми повідомлення. Друга буква біграми шифровки береться з правої таблиці в стовпці, що відповідає першій букві біграми повідомлення. Так, біграм-повідомлення ТО перетворюється в біграм-шифровку ЖБ.

Приклад 3.

Використовуючи для шифрування шифр подвійного квадрату, зашифрувати вихідний текст "приїзджаю шостого".

Повідомлення:	пр	иї	зд	жа	ю	шо	ст	ог	о
Шифровка:	ПЕ	,Й	ЄШ	ЧЙ	ЛТ	ДБ	ЩР	НЮ	ХЛ

Зашифрований текст: ПЕ ,Й ЄШ ЧЙ ЛТ ДБ ЩР НЮ ХЛ

Практична частина:

1. Відкрити проект з попередньої лабораторної роботи та доповнити кнопками головне меню.

2. Зашифруйте повідомлення введене з клавіатури використовуючи один з наступних шифрів.

- шифр Плейфера;
- шифр подвійного квадрату.

3. Розшифрувати введене повідомлення, зашифроване з застосовуванням шифру Плейфера та шифру подвійного квадрату.

4. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу.

Контрольні питання:

1. Який принцип шифрування Плейфера?
2. Який принцип шифрування подвійного квадрату?
3. Де знайшли застосування біграмні шрифти?
4. В чому відмінність шифрування Плейфера та подвійного квадрату?

Лабораторна робота № 3

Тема: Шифр Віженера

Мета: вивчити шифр Віженера, вміти виконувати процедури шифрування та дешифрування.

Теоретична частина:

Один з цікавих видів багатоалфавитного шифру був створений Блезом де Віженером, французьким математиком шістнадцятого століття. Шифр Віженера використовує різну стратегію створення потоку ключів.

А	Б	В	Г	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	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
Я	_	А	Б	В	Г	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
Ю	Я	_	А	Б	В	Г	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
Ь	Ю	Я	_	А	Б	В	Г	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
Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	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	Д	Е	Є	Ж	З	И	І	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	Д	Е	Є	Ж	З	И	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	Д	Е	Є	Ж	З	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	Д	Е	Є	Ж	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	Д	Е	Є	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	Д	Е	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	Д	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	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
Г	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
В	Г	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
Б	В	Г	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

Список Віженера (Vigenere tableau) - таблиця Віженера, утворена наступним чином: в перший рядок вписується весь алфавіт, в наступних рядках вводиться зсув на 1 літеру вліво, так отримується квадратна таблиця.

Щоб зашифрувати повідомлення, вибирають лозунг (ключ-слово), який підписують під текстом. Потім у стовпчику шукають літеру повідомлення, а у рядку – літеру ключа-слова, на їх перетині знаходиться підстановка.

Приклад.

Подивимося, як ми можемо зашифрувати повідомлення "Захист_інформації", використовуючи ключове слово на 4 символи "Мова". Далі з повної матриці вибирається підматриця шифрування, що включає перший рядок і рядки матриці, початковими літерами яких є початкові літери ключа М, о, в, а.

А	Б	В	Г	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	_
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н
В	Г	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
А	Б	В	Г	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	_

В процесі шифрування отримаємо:

Текст шифровки	З	А	Х	И	С	Т	_	І	Н	Ф	О	Р	М	А	Ц	І	Ї
Ключ	М	О	В	А	М	О	В	А	М	О	В	А	М	О	В	А	М
Шифрограма	Ф	О	Ч	И	В	Е	Б	І	Я	Ж	Р	Р	Ю	О	Ш	І	Ч

Зашифрований текст: ФОЧИВЕБІЯЖРРЮОШІЧ

Практична частина:

1. Відкрити проект з попередньої лабораторної роботи та доповнити кнопками головне меню.
2. Зашифруйте повідомлення введене з клавіатури шифром Віженера.
3. Розшифрувати наступне повідомлення (дане викладачем), зашифроване з застосовуванням шифру Віженера.
4. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу.

Контрольні питання:

1. Який принцип шифрування з використанням системи Віженера?
2. Який принцип побудови таблиці Віженера?
3. Де знайшла застосування система Віженера?

Лабораторна робота № 4

Тема: Шифри перестановки

Мета: вивчити шифри перестановки, вміти виконувати процедури шифрування та дешифрування.

Теоретична частина:

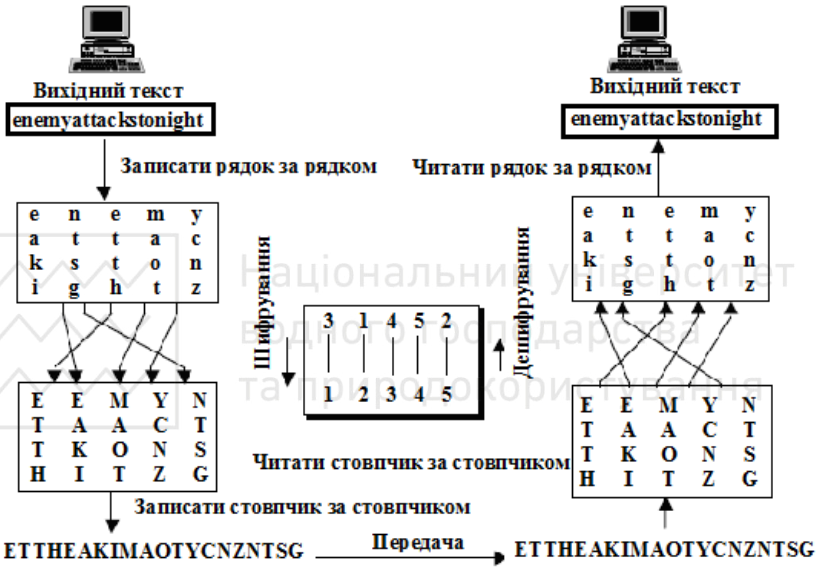
Наступні два простих шифри-перестановки, що застосовувалися в минулому і не передбачали використання ключ. У першому методі текст

записується в таблиці стовпець за стовпцем і потім передається рядок за рядком. У другому методі текст написаний в таблиці рядок за рядком і потім передається стовпець за стовпцем.

Приклад:

Зашифрувати текст "*enemyattackstonight*" (атака супротивника сьогодні ввечері) використовуючи шифр перестановки з ключем "3, 1, 4, 5, 2".

Шифр перестановки з ключем «3, 1, 4, 5, 2» - схема.



Практична частина:

1. Відкрити проект з попередньої лабораторної роботи та доповнити кнопками головне меню.
2. Зашифруйте повідомлення введене з клавіатури використовуючи шифр перестановки з ключем **«3, 1, 4, 5, 2».**
3. Розшифрувати наступні повідомлення (дане викладачем), зашифроване з застосовуванням шифру перестановки з ключем «3, 1, 4, 5, 2».
4. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу.

Контрольні питання:

1. Що таке блоковий та потоковий шифр?
2. Який принцип шифрування блокового шифру перестанови без ключа?
3. Який принцип шифрування блокового шифру перестанови з ключем?

Лабораторна робота № 5

Тема: Системи з відкритим ключем. Криптосистема RSA

Мета: Отримати навички реалізації та криптоаналізу у криптосистемі RSA. Вміти виконувати процедури шифрування та дешифрування за допомогою даного алгоритму.

Загальні відомості

Концепцію систем з відкритим ключей запропонували у 1976 році Діффі і Хеллман. Криптосистеми з відкритим ключем засновуються на використанні особливих властивостей шифрування, що являє собою розрахунок оберненої величини від якоїсь функції, що не може бути реалізована числовими методами.

В сучасній криптографії стандартом де-факто на системи з відкритим ключем є система RSA спроектована Rivest, Shamir і Adleman.

RSA – криптографічна система відкритого ключа, що забезпечує такі механізми захисту як шифрування і цифровий підпис (аутентифікація – встановлення автентичності).

Теоретична частина:

Розглянемо математичні результати, покладені в основу алгоритму RSA.

Теорема 1. *(Мала теорема Ферма.)*

Якщо p - просте число, то

$$x^{p-1}=1(mod\ p) \qquad (1)$$

для будь-якого x, простого відносно p, і

$$x^{p}=x\ (mod\ p) \qquad (2)$$

для будь-якого x.

Визначення. Функцію Эйлера j(n) називається число позитивних цілих, менших n і простих відносно n.

n	2	3	4	5	6	7	8	9	10
$j(n)$	1	2	2	3	2	6	4	6	4

Теорема 2. Якщо $n=pq$, (p і q - відмінні один від одного прості числа) то $\varphi(n)=(p-1)(q-1)$.

Теорема 3. Якщо $n=pq$, (p і q - відмінні один від одного прості числа) і x - просте відносно p і q,то $x^{\varphi(n)}=1\ (mod\ n)$.

Слідування. Якщо $n=pq$, (p і q - відмінні один від одного прості числа) і є просте відносно $j(n)$ $E_{e,n}$: x®x^e ($mod\ n$) є взаємно однозначним на Z_n.

Очевидний і той факт що якщо e - просте відносно (n), то існує ціле d, таке, що

$$ed=1\ (mod\ \varphi(n)) \qquad (3)$$

На цих математичних фактах і заснований популярний алгоритм RSA.

Нехай $n=pq$, де p і q - різні прості числа. Якщо e і d задовольняють рівнянню (3), то відображення $E_{e,n}$ і $E_{d,n}$ є інверсіями на Z_n. Як $E_{e,n}$ так і $E_{d,n}$ легко розраховуються, коли відомі e, d, p, q. Якщо відомі e і n, але p і q

невідомі, то $E_{e,n}$ являє состою однобічну функцію, перетворення $E_{d,n}$ по заданому *n* рівнозначно розкладанню *n*. Якщо *p* і *q* - досить великі прості числа, то розкладання *n* практично не здійсненне. Це і закладено в основу системи шифрування RSA.

Алгорипт генерування ключів:

1. Вибираємо два досить великі прості числа **p** і **q**
2. Обчислюємо їх добутку **n=p*q** - модуль.
3. Обчислюємо значення функції Ейлера від **n:** $\varphi(n)=(p-1)(q-1)$.
4. Обираємо, випадковим чином, елемент **e** (1 < e < φ(n)), що не перевищує значення $\varphi(n)$ і взаємно простий з ним.
5. Вираховується число **d**, обернене до числа e за mod φ(n), тобто таке, що $d<\varphi(n)$ і $ed \equiv 1 \bmod \varphi(n)$.
6. Як результат покладають:

- Відкритий ключ RSA: (e, n);
- Секретний ключ RSA: (d, n).

Шифрування відбувається блоками. Для цього повідомлення записують у цифровій формі і розбивають на блоки так, щоб кожен блок позначав число, яке не перевищу *n*.

Алгоритм шифрування *E* у системі *RSA* полягає у піднесенні *M* до степеня *e*. Записуємо це так:

$$E(M)=M^e \bmod n. \tag{6}$$

В результаті отримаємо блок криптотексту

$$D(C)=C^d \bmod n. \tag{7}$$

Приклад 1. Зашифруємо повідомлення "CAB". Для простоти будемо використовувати маленькі числа (на практиці застосовуються набагато більші).

Виберемо p=3 і q=11.

Визначимо n=3*11 =33.

Знайдемо (p-1)(q-1)=20. Отже, у якості d, взаємно простої з 20, приймемо наприклад, d=3.

Виберемо число e. Як таке число може бути узяте будь-яке число, для якого задовольняється співвідношення (e*3)(mod 20)=1, наприклад 7.

Примітка: для простого знаходження числа e досить вирішити в цілих числах рівняння $e=\frac{a*20+1}{3}$, де *a*=1,2, ..., *n* (перебираючи значення *n* до першого цілого e).

Представимо повідомлення як послідовність цілих чисел за допомогою відображення: A®1, B®2, B®3 Тоді повідомлення приймає вид (3,1,2). Зашифруємо повідомлення за допомогою ключа {7,33}.

C[1] = (3^7) (mod 33) = 2167 (mod 33) = 9.
C[2] = (1^7) (mod 33) = 1 (mod 33) = 1.
C[3] = (2^7) (mod 33) = 126 (mod 33) = 29.

Розшифруємо отримане зашифроване повідомлення C {9,1,29} на основі закритого ключа {3,33}:

M[1] = (9^3) (mod 33) = 729 (mod 33) = 3.
M[2] = (1^3) (mod 33) = 1 (mod 33) = 1.
M[3] = (29^3) (mod 33) = 24369 (mod 33) = 2.

Приклад 2. Шифруємо слово БІГ.

Коефіцієнти p=3, *q*=7.

Визначимо n=p*q=3*7=21.

Знайдемо (p-1)(q-1)=12.

Виберемо *d* = 5.

Знайдемо число e для якого справедливо *ed* mod ((p-1)(q-1))=1. (вирішуємо рівняння $e = \frac{a*12+1}{5}$ де *a*=1,2, ..., *n)* вибераємо з безлічі рішень відмінне від числа d число, e = 17.

Представимо слово для шифрування у вигляді послідовності чисел 2, 6, 4 (порядковий номер букв у алфавіті).

Шифрування по відкритому ключу (17,21):

$C_1 = 2^{17}$ mod (21) = 131032 mod (21) =11.
$C_2 = 6^{17}$ mod (21) = 16926659444736 mod (21) = 6.
$C_3 = 4^{17}$ mod (21) = 17179869184 mod (21) = 16.

Отримане зашифроване повідомлення: 11, 6, 16.

Розшифруємо зашифроване повідомлення по секретному ключу (5, 21):

$M_1 = 11^5$ mod (21) = 161051 mod (21) = 2.
$M_2 = 6^5$ mod (21) = 7776 mod (21) = 6.
$M_3 = 16^5$ mod (21) = 1048576 mod (21) = 4.

У підсумку одержуємо вихідне повідомлення БІГ.

Отже, у реальних системах алгоритм RSA реалізується в такий спосіб: кожен користувач вибирає два великих простих числа, відповідно до описаного вище алгоритму. Наприклад, вибиремо два простих числа *e* і *d.* Як результат множення перших двох чисел *(p* і *q*) установлюється *n {e, n}* утворить відкритий ключ, а *{d, n}* - закритий (хоча можна взяти і навпаки).

Відкритий ключ публікується і доступний кожному, хто бажає послати власнику ключа повідомлення, що зашифровується зазначеним алгоритмом. Після шифрування, повідомлення неможливо розкрити за допомогою відкритого ключа, але власник закритого ключа легко може розшифрувати прийняте повідомлення.

Практична частина:

1. Вивчити опис криптосистеми RSA та відомості з елементарної теорії чисел. Розібрати схему шифрування алгоритмом RSA.

2. Відкрити проект з попередньої лабораторної роботи № 1 та доповнити кнопками головне меню.

3. Зашифрувати повідомлення алгоритмом RSA за ключами поданими у варіанті. Передостання цифра номеру студентського квитка означає номер варіанту відкритого тексту, остання цифра номеру студентського квитка означає ключі шифрування.

4. Розшифрувати отриманий шифртекст.

5. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу. У звіті необхідно вказати свою ключову пару (відкритий та секретний ключ), шифртекст та поновлений текст.

Завдання:

i	j			
0. Криптографія	p=7	q=17	d=119	e=167
1. Криптоаналіз	p=5	q=7	d=23	e=191
2. Синхронізація	p=3	q=11	d=19	e=179
3. Апроксимація	p=11	q=13	d=119	e=239
4. Конфіденційність	p=13	q=17	d=191	e=191
5. Маршрутизатор	p=11	q=7	d=59	e=239
6. Інтерполяція	p=5	q=11	d=41	e=161
7. Моноалфавітні	p=7	q=13	d=71	e=143
8. Поліалфавітні	p=11	q=17	d=157	e=213
9. Гомофонічні	p=5	q=13	d=47	e=95

Контрольні питання:

1. У чому полягає суть систем з відкритим ключем (СВК)?

2. За допомогою яких ключів шифрується і розшифровується повідомлення в СВК?

3. Які головні вимоги пред'являються до СВК?

4. На яких математичних фактах заснований алгоритм RSA?

5. Як вибираються числа P і Q в алгоритмі RSA?

6. Які значення користувач що генерує ключі RSA, повідомляє іншим користувачам, а які зберігає в таємниці?

7. Чи можна розшифрувати повідомлення за допомогою відкритого ключа?

8. Як обчислюється значення функції Ейлера? Для чого воно використовується в алгоритмі RSA?

Лабораторна робота № 6

Тема: Електронний цифровий підпис. Алгоритм Ель-Гамаля

Мета: Ознайомитися зі схемами цифрового підпису та отримати навички створення й перевірки дійсності ЦП.

Загальні відомості:

Протягом багатьох століть при веденні ділової переписки, складінні контрактів і оформленні будь-яких інших важливих паперів підпис відповідальної особи або виконавця був неодмінною умовою визнання його статусу або незаперечним свідченням його важливості. Подібний акт переслідував дві цілі:

- гарантування істинності листа шляхом звірення підпису з наявним зразком;
- гарантування авторства документа (з юридичної точки зору).

З переходом до безпаперових способів передачі й зберігання даних, а також з розвитком систем електронного переказу коштів, в основі яких – електронний аналог паперового платіжного доручення, проблема віртуального підтвердження автентичності документа набула особливого значення. Розвиток будь-яких подібних систем тепер неможливий без існування електронних підписів (ЕЦП) під електронними документами.

Процес генерації ЕЦП відбувається в такий спосіб

Учасник А обчислює хеш-код від ЕД. Отриманий хеш-код проходить процедуру перетворення з використанням свого секретного ключа. Після чого отримане значення (яке і є ЕЦП) разом з ЕД відправляється учасникові В.

Учасник В повинен одержати ЕД з ЕЦП і сертифікований відкритий ключ учасника А, а потім зробити розшифрування на ньому ЕЦП, сам ЕД зазнає операції хешування, після чого результати порівнюються, і якщо вони збігаються, то ЕЦП визнається дійсним, а якщо ні, то неправильним.

У наш час застосовуються кілька алгоритмів цифрового підпису:

- RSA (найбільш популярний);
- Digital Signature Algorithm, DSA (алгоритм цифрового підпису американського уряду, який застосовують у стандарті цифрового підпису (Digital Signature Standard, DSS), також використовується часто);
- алгоритм Ель-Гамаля (іноді можна зустріти);
- алгоритм, який застосовують у стандарті ГОСТ Р34.10-94 (в основі лежить DSA і є варіацією підпису Ель-Гамаля);
- так само існують алгоритми підписів, в основі яких лежить криптографія еліптичних кривих, вони схожі на всі інші, але в деяких ситуаціях працюють ефективніше.

Теоретична частина:

Електронний підпис RSA

Для здійснення підпису повідомлення $m=m_1m_2m_3..m_n$ необхідно обчислити хеш-функцію $y=h(m_1m_2m_3..m_n)$, яка ставить у відповідність повідомленню m число y. На наступному кроці досить забезпечити підписом тільки число y, і цей підпис буде відноситися до всього повідомлення m.

Далі за алгоритмом RSA обчислюються ключі (e,n) і (d,n).

Потім обчислюється $s = y^d \bmod n$ (d секретний ключ).

Число s це і є цифровий підпис. Він просто додається до повідомлення й виходить підписане повідомлення {m,s}.

Тепер кожний, хто знає параметри того, хто підписав повідомлення (тобто числа e і n), може перевірити дійсність підпису.

Для цього необхідно перевірити виконання рівності $h(m) = s^e \bmod n$.

Алгоритм Ель-Гамаля

Для генерації пари ключів спочатку вибирається просте число p і два випадкові числа g і x. Обидва ці числа повинні бути менші p.

Щоб підписати повідомлення M, спочатку вибирається випадкове число k, взаємно просте з p-1. Потім обчислюється

$$a = g^k \bmod p \tag{1}$$

і за допомогою розширеного алгоритму Евкліда знаходиться b з наступного рівняння:

$$M = (xa + kb) \bmod \quad (p-1). \tag{2}$$

Підписом є пара чисел: a і b. Випадкове значення k повинне зберігатися в таємниці. Для перевірки підпису потрібно переконатися, що

$$y^a a^b \bmod \quad p = g^M \bmod \quad p. \tag{3}$$

ПРИКЛАД (алгоритм Ель-Гамаля)

1. Нехай загальні параметри для деякого співтовариства користувачів p=23 і g=5. Нехай секретний ключ x=7.

2. Обчислимо відкритий ключ y: $y = 5^7 \bmod 23 = 17$.

Нехай потрібно поставити підпис на повідомлення m=baaqab. Перейдемо до обчислення підпису по алгоритму.

3. Насамперед, обчислюється хеш-функція. Нехай її значення h(m)=h(baaqab)=M=3.

4. Потім генерується випадкове число k, наприклад k=5. Обчислюємо по формулах (1, 2): $a = 5^5 \bmod 23 = 20$; і по розширеному алгоритму Евклида знаходимо b =(7*20+5*b) mod 22=21.

Таке b існує, тому що НСД(k,p-1)=1. Одержали b=21.

5. Одержали підписане повідомлення у вигляді {baaqab,20,21}

Отримане повідомлення перевіримо на дійсність:

1. Насамперед, обчислюється хеш-функція h(baaqab)=M=3.

2. Потім обчислюємо ліву частину, формула (3) $17^{20} * 20^{21} \bmod 23 = 16 * 15 \bmod 23 = 10$ і після цього праву частину $5^3 \bmod 23 = 10$.

По тому, що ліва частина збіглася із правою, можна зробити висновок, що підпис вірний.

Практична частина:

1. Відкрити проект з попередньої лабораторної роботи № 1 та доповнити кнопками головне меню.

2. Абоненти деякої мережі застосовують підпис Ель-Гамаля (або RSA) із загальними параметрами p=23, g=5. Для зазначених секретних параметрів абонентів знайти відкритий ключ (y) і побудувати підпис для повідомлення m.

3. Програмно реалізувати шифрування в криптосистемі Ель-Гамаля (або RSA) p=23, g=5, та x (згідно варіанту).

4. Збережіть всі файли в окремому каталозі для звіту та захистіть роботу. У звіті необхідно вказати відкритий ключ y.

Завдання:

У всіх варіантах будемо припускати, що h(m)=m для всіх значень m.

1)	x=11, k=3, m=15	9)	x=9, k=19, m=15
2)	x=10, k=15, m=5	10)	x=19, k=19, m=15
3)	x=3, k=13, m=8	11)	x=5, k=5, m=12
4)	x=18, k=7, m=5	12)	x=11, k=19, m=8
5)	x=9, k=19, m=15	13)	x=9, k=8, m=15
6)	x=5, k=10, m=8	14)	x=12, k=8, m=15
7)	x=4, k=4, m=4	15)	x=6, k=11, m=13
8)	x=12, k=19, m=15	16)	x=7, k=9, m=10

1. **Контрольні питання:**
2. Для чого потрібен цифровий підпис?
3. Які схеми цифрового підпису існують?
4. Яка схема найпоширеніша? Чому?
5. Як здійснюється підпис RSA?
6. Яка відмінність підпису RSA від шифру RSA?
7. Як здійснюється підпис Ель-Гамаля?
8. Як здійснюється перевірка на дійсність підпису Ель-Гамаля?
9. Які основні параметри системи складають основу шифру Ель-Гамаля?
10. Яким чином виконується шифрування методом Ель-Гамаля?
11. В чому його різниця шифрування методом Ель-Гамаля від RSA?

Приклади написання частин програм в середовищі С++

1) Шифрування адитивним шифром:

```
A="abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ";
alfabet =A.toCharArray();
*************
for(int i = 0; i< inText.length; i++)//inText - вхідне повідомлення для шифрування
        for(int j=0; j<alfabet.length;j++)
        {
          if((int)(inText[i])==(int)(alfabet[j]))
          {
            k=(((j+1)*key1+key2)%53);// шифрування символу
            if(k==0)
              k=53;

            inText[i]=alfabet[k-1];
            break;
          }
        }
```

Дешифрування адитивного шифру:

```
for(int i = 0; i< inText.length; i++)//inText - вхідне повідомлення для дешифрування
        for(int j=0; j<alfabet.length;j++)
        {
          if((int)(inText[i])==(int)(alfabet[j]))
          {
            k=j+1-key2;
            while(k%key1!=0)//процес дешифрування символу
            {
              k+=53;
            }
            k=k/key1;
            inText[i]=alfabet[k-1];
            break;
          }
        }
```

2) Шифрування Віженера:

```
//створення таблиці для шифрування
 abc="абвгдеєжзиіїйклмнопрстуфхцчшщьюя ".toCharArray();
      alfabet = new char[33][33];
      boolean status= true;
      for(int i =0 ,j=0; i<33;i++,j++)
      {
```

```
        int k=0;
        while(status)
        {
            if(j>32)
                j%=33;
            alfabet[i][j++]=abc[k++];
            if(k==33)
                status=false;
        }
        j=i;
        status=true;
    }
public String Encrypt(String key,String word)
  {
    char table[][] = new char[2][word.length()];
    table[0]=word.toCharArray();//заповнення першого рядка таблиці повідомленням яке потрібно шифрувати
    char[] encr_word=new char[word.length()];
    int k=0;
    for(int i=0;i<word.length();i++) {//заповненн другого рядка таблиці ключом
        table[1][i] = key.charAt(k++);
        if(k>=key.length())
            k=0;
    }
    for(int i=0; i<table[0].length;i++)//процес шифрування
    {
        int pw=0,pk=0;
        for(int j=0;j<alfabet.length;j++)
        {
            if(table[0][i]==alfabet[j][0])
            {
                pw=j;
                break;
            }
        }
        for(int j=0;j<alfabet.length;j++)
        {
            if(table[1][i]==alfabet[0][j])
            {
                pk=j;
                break;
            }
```

```
        }
        encr_word[i]=alfabet[pw][pk];
    }
    return new String(encr_word);
  }
```

3) Дефифрування подвійний квадрат

```
public String Decrypt(String text)
  {
    char[] decrchar;
    char[] charText3 = text.toCharArray();//вхідне повідомлення
    //helping variable (half of text length)
    int p= (charText3.length)/2;
    decrchar = new char[2*p];//вихідне повідомлення
    //створення змінних позицій літер в таблиці
    int ia=-1,ja=-1,ib=-1,jb=-1;
    //створення вихідного тексту
    for(int f=0; f<2*p; f+=2) {
      for (int i = 0; i < 5; i++)
      {
        for (int j = 0; j < 5; j++)
        {
          if (Table1[i][j] == charText3[f])
          {
            ia=i;  ja=j;
          }
          if (Table2[i][j] == charText3[f+1])
          {
            ib=i;  jb=j;
          }
          if(ia!=-1&&ib!=-1)
            break;
        }
        if(ia!=-1&&ib!=-1)
          break;
      }
      if(ia==ib)
      {
        if(ja==0)
          decrchar[f]=Table1[ia][4];
        else
          decrchar[f]=Table1[ia][ja-1];
        if(jb==0)
```

```
            decrchar[f+1]=Table2[ib][4];
        else
            decrchar[f+1]=Table2[ib][jb-1];
    }
    if(ja==jb)
    {
        if(ia==0)
            decrchar[f]=Table1[4][ja];
        else
            decrchar[f]=Table1[ia-1][ja];
        if(ib==0)
            decrchar[f+1]=Table2[4][jb];
        else
            decrchar[f+1]=Table2[ib-1][jb];
    }
    if(ja!=jb && ia!=ib)
    {
        decrchar[f]=Table1[ia][jb];
        decrchar[f+1]=Table2[ib][ja];
    }
    ia=ja=jb=ib=-1;
  }
  return new String(decrchar);
}
```

4) Створення відкритого та закритого ключа RSA

```
public void CreateKeys (int p, int q,int[] keys)
  {
    int n = p*q;
    int f = (p-1)*(q-1);
    int d=2;
    int dhelp = 2;
    while(dhelp!=1)
    {
      d++;
      dhelp=d;
      int fhelp = f;
     while (dhelp != fhelp)
        if (dhelp > fhelp) {
            dhelp = dhelp - fhelp;
        } else {
            fhelp = fhelp - dhelp;
        }
```

```
}
 int k=1;   int e;
 while(((double)(k*f+1)/d)%1!=0)
 {
     k++;
 }
 e=(k*f+1)/d;
 keys[0]=e;
 keys[1]=n;
 keys[2]=d;
}
```

Література:

1. Алферов А.П., Зубов А.Ю. та ін. Основы криптографии: Учеб. пособие для студ. вузов, обучающихся по группе спец. в области информ. безопасности. - М.: Гелиос АРВ, 2001. - 480 с.
2. Бабаш А.В., Шанкин Г.П. Криптография / В.П.Шерстюк (ред.), Э.А.Применко (ред.). - М.: ООО Издательство "Солон-Р", 2002. - 511 с.
3. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел: Навч. посібник /Державний ун-т інформаційно-комунікаційних технологій. - К.: ДУІКТ, 2006. - 126 с.
4. Вербіцький О.В. Вступ до криптології. - Львів: Вид-во Наук.-техн. літ., 1998. - 247 с.
5. Математические компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И Берник, Г.В. Матвеев, С.В. Агиевич. - МН.: Новое знание, 2003. - 382 с.

Інформаційні ресурси:

1. Защита информации и ее взлом. - http://algolist.manual.ru/defence/
2. Основы теории криптографии и криптоанализа - http://vunivere.ru/category1/section7/subject1984