МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Факультет інформаційних технологій

Кафедра програмного забезпечення систем

«ПРОГРАМНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

Методичні вказівки до лабораторних робіт

УЖГОРОД – 2023

Програмні технології захисту інформації: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти, спеціальності 121 Інженерія програмного забезпечення факультету інформаційних технологій УжНУ / Укладач: д.т.н., доц. Поліщук В.В. – Ужгород: 2023. – 31 с.

У методичних вказівках до лабораторних робіт з курсу «Програмні технології захисту інформації» розглянуто п’ять лабораторних робіт, що входять до складу робочої програми. Наведено теоретичний матеріал необхідний для виконання лабораторної роботи. До лабораторних робіт сформульовано завдання студентам, вимоги до порядку виконання та змісту звіту по проробленій роботі. У методичних вказівках наведена програма навчальної дисципліни, перелік тем на семінарське заняття та перелік запитань на підсумковий контроль.

Укладач: д.т.н., доц. Поліщук В.В., професор кафедри програмного забезпечення систем факультету інформаційних технологій ДВНЗ «УжНУ».

Рецензенти:

д.т.н., проф., декан факультету інформаційних технологій ДВНЗ «УжНУ» Повхан І.Ф.

к.ф-м.н., доц., завідувач кафедри програмного забезпечення систем ДВНЗ «УжНУ» Білак Ю.Ю.

Рекомендовано кафедрою програмного забезпечення систем від «19» травня 2023 р., протокол №11.

Розглянуто і схвалено науково-методичною комісією факультету інформаційних технологій УжНУ. Протокол №9 від 30.06.2023 р.

ЗМІСТ

Вступ

Мета вивчення навчальної дисципліни "Програмні технології захисту інформації" полягає в: освоєнні та розумінні програмних інструментів та методологій, які використовуються для захисту інформації в сучасному цифровому середовищі; аналіз загроз інформаційної безпеки, основними методам, принципам, алгоритмам захисту інформації в комп’ютерних та інформаційних системах, з урахуванням сучасних тенденцій розвитку інформаційної безпеки та кіберзахисту.

Ця дисципліна дозволяє студентам розширити свої знання та навички в галузі інформаційної безпеки, а також навчитися застосовувати їх у практичних ситуаціях.

Під час вивчення дисципліни "Програмні технології захисту інформації" студенти отримають знання про різні види загроз та атак на інформаційні системи, а також про методи їх виявлення та захисту. Вони ознайомляться з основними принципами криптографії, аутентифікації, авторизації та контролю доступу, а також з методами захисту даних та програмного забезпечення.

Вивчення дисципліни "Програмні технології захисту інформації" допоможе студентам отримати необхідні знання та навички для розробки та впровадження захисту інформації в програмному середовищі та забезпечення безпеки інформаційних систем.

Програма навчальної дисципліни

Модуль 1

Тема 1. Вступ. Проблеми теорії захисту інформації.

Тема 2. Характеристика загроз безпеки інформації

Тема 3. Несанкціонований доступ. Порушники безпеки

Тема 4. Шляхи забезпечення безпеки інформації: Концепція захисту інформації; Стратегія та архітектура захисту інформації; Види забезпечення безпеки інформації.

Тема 5. Політика безпеки інформації: Етапи реалізації систем захисту.

Тема 6. Моделі політики безпеки: Дискреційна політика безпеки; Мандатна політика безпеки; Рольова політика безпеки; Монітор безпеки.

Модуль 2

Тема 7. Криптографічні методи захисту інформації: Основні положення та визначення; Характеристика алгоритмів шифрування.

Тема 8. Методи захисту інформації в операційних системах.

Тема 9. Аналіз безпеки ПЗ та руйнуюче ПЗ.

Тема 10. Методи аналізу безпеки ПЗ.

Тема 11. Поняття про гешувальні алгоритми, їх призначення, вимоги до них.

Тема 12. Поняття про цифровий підпис, вимоги до нього. Основні положення керування ключами.

Теми лабораторних занять

№ з/п	Назва теми
1	Шифрування і розшифрування повідомлень шифрами заміни і перестановки
2	Шифрування і розшифрування повідомлень шифрами Полібія та Гронсфельда
3	Біграмні шифри та шифр Вернама
4	Алгоритм шифрування DES
5	Алгоритм шифрування RSA
6	Семінарське заняття по організаційних заходах щодо захисту інформації та нормативно-правових документів з питань захисту інформації

Лабораторна робота № 1

Тема: ШИФРИ ЗАМІНИ І ПЕРЕСТАНОВКИ

Мета роботи – практично освоїти основи побудови шифрів заміни і перестановки. Здійснити вибір ключів і провести процедуру зашифрування-розшифрування повідомлень. Зробити програмне забезпечення.

Короткі теоретичні відомості

Шифр заміни (шифр підстановки) – метод шифрування, при якому кожен елемент початкового тексту взаємно-однозначно замінюється одним, або декількома знаками деякого алфавіту. Шифр простої заміни замінює кожен знак вхідного алфавіту на деякий знак з того ж алфавіту, Результат заміни не залежить від розташування знаку у відкритому тексті. Ключами для шифрів заміни є таблиці заміни.

Шифр пропорційної заміни. Основною слабкістю шифру простої однобуквенної заміни є віддзеркалення в частоті шифропозначень ймовірнісних властивостей букв відкритого тексту. Щоб наблизити частоти зустрічаємості букв до рівноймовірних, можна надати кожній шифрвеличині по декілька шифропозначень, причому тим більше, чим більше ймовірність появи букви у відкритому тексті. Такий шифр називається шифром пропорційної заміни, а використаний метод – рандомізацією відкритого тексту.

Шифр багатоалфавітної заміни. Шифр багатоалфавітної заміни використовує сукупність шифрів простій заміни. Ця сукупність, як правило, є довготривалим ключем.

На кожному такті шифрування черговий символ відкритого тексту замінюється на символ шифрованого тексту за допомогою таблиці заміни, номер якої задається разовим ключем.

При скінченній довжині ключа шифр називається періодичним шифром багатоалфавітної заміни, оскільки при довгому відкритому тексті ключ в даному шифрі застосовується повторно необхідну кількість разів.

Однією із старих і найбільш відомих багатоалфавітних систем є криптосистема Виженера. Нехай треба зашифрувати відкритий текст $a_1, a_2, ..., a_l$ на ключі $k = \gamma_1, \gamma_2, ..., \gamma_p$. Занумеруємо букви алфавіту та пропуск відкритого тексту і ключа числами в десятковій системі числення. Підпишемо під послідовністю чисел повідомлення послідовність чисел ключа і додамо числа цих послідовностей за модулем n, де n - потужність алфавіту повідомлень. Рівняння шифрування і розшифрування i-ї букви повідомлення виражаються відповідно формулами:

$$b_i = (a_i + \gamma_i) (\mathrm{mod}\, n),\ i = 1, 2, ..., p,$$

$$a_i = (b_i - \gamma_i) (\mathrm{mod}\, n),\ i = 1, 2, ..., p.$$

Де a_i, b_i, γ_i – номери букв у відкритому тексті, криптограмі і ключі відповідно.

При псевдовипадковому ключі шифр називається шифром багатоалфавітної заміни з нескінченним періодом, якщо гарантується відсутність повторне використання ключа при будь-яких допустимих довжинах криптограм.

Шифри перестановки. Відмінність цього типу шифру від шифрів заміни полягає в тому, що при зашифруванні буква a_i відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту a_j, внаслідок чого букви розташовуються на нових місцях, тобто переставляються.

Ключем для даного шифру також служить таблиця заміни, тільки не букв алфавіту, а їх індексів (номерів місць) в тексті, який підлягає зашифруванню. У загальному випадку, розмір таблиці заміни дорівнює довжині відкритого тексту. Такі таблиці зручно формувати (і записувати) у вигляді підстановок.

Приклад

Задається перестановка з n елементів. Текст, що підлягає зашифруванню, розбивається на блоки довжини n. У кожному блоці символи переставляються відповідно до заданої перестановки.

Розглянемо приклад шифрування для перестановки

1	2	3	4	5
3	2	5	1	4

Вихідний текст:

«СВЯЩЕ ННАЯР ИМСКА ЯИМПЕ РИЯЬЭ»

Зашифрований текст

«ЩВСЕЯЯННРАКМИАСПИЯЕМЬИРЭЯ»

Зашифрований текст виписується без пропусків.

Шифр вертикальної перестановки. Шифр вертикальної перестановки є різновидом шифрів маршрутної перестановки, в яких відкритий текст записується в певну геометричну фігуру за деякоим "маршрутом", а потім за іншим "маршрутом" виписується з неї.

Для зашифрування шифром вертикальної перестановки будується прямокутна таблиця, кількість рядків якої визначається довжиною тексту, а кількість стовпців дорівнює довжині ключа. Ключ шифру – деяка перестановка n чисел, де n - число стовпців в таблиці. Відкритий текст стандартно вписується в прямокутник по рядках зліва направо. Букви криптограми виписуються по вертикалі, при цьому стовпці вибираються в порядку, визначеному ключем.

Порядок виконання роботи.

1. Вивчити короткі теоретичні відомості про шифри заміни і перестановки.

2. Створити програмне забезпечення для реалізації шифрів заміни та перестановки.

3. Скласти звіт, приєднавши отримані результати.

Вимоги до звіту.

У звіті повинні бути приведені:

1. Короткі теоретичні відомості про шифри заміни і перестановки.
2. Відкриті повідомлення.
3. Зашифровані (розшифровані) повідомлення.
4. Лістинг та скриншоти роботи програми.

Лабораторна робота №2

Тема: ШИФР ПОЛІБІЯ ТА ГРОНСФЕЛЬДА

Мета роботи – практично освоїти основи побудови шифрів Полібія та Гронсфельда. Здійснити вибір ключів і провести процедуру зашифрування-розшифрування повідомлень. Зробити програмне забезпечення.

Короткі теоретичні відомості.

Квадрат Полібія. Один з найдавніших простих шифрів приписують грецькому громадському діячеві та науковцю Полібію. Шифрування відбувається наступним чином: обирається слово-ключ, кількість літер в якому залежить від мови; ключ записується в першому рядку квадрата, в подальших рядках виписуються літери алфавіту, відсутні в ключі; кожна літера повідомлення замінюється на ту, що стоїть в квадраті на рядок нижче (при розшифруванні – на рядок вище) (рис. 1).

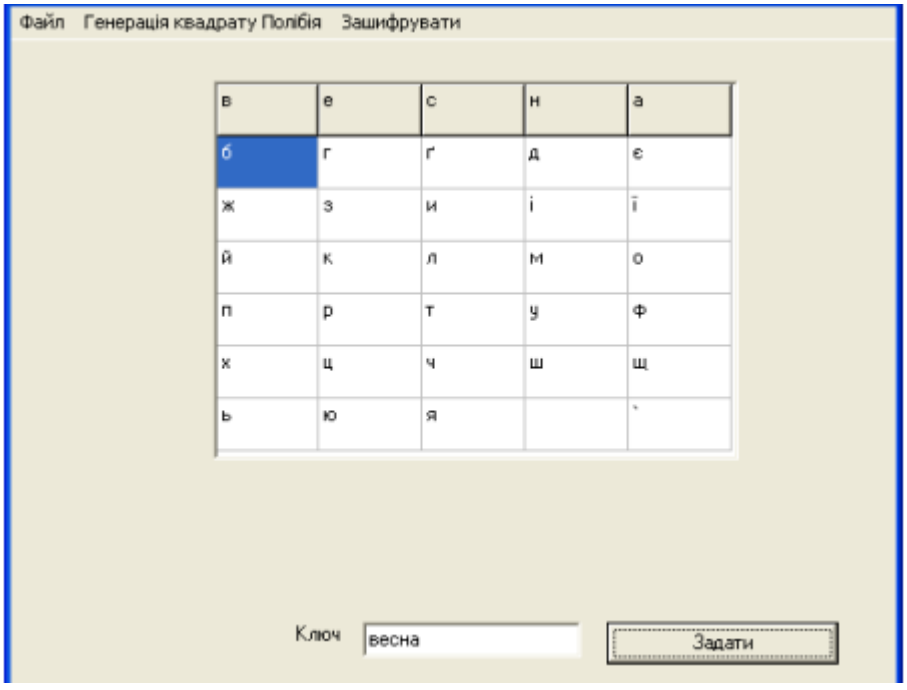

Рис. 1. Квадрат Полібія

Шифр Гронсфельда. Ключем є деяке десяткове число. Цифри цього числа циклічно записуються під символами відкритого тексту. При шифруванні кожна буква відкритого тексту зсувається за алфавітом на число позицій, зазначених під нею.

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M

14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Вихідний текст	G	E	R	M	A	N	Y
Ключ	1	3	5	7	9	1	3
Зашифрований текст	H	H	W	T	J	O	B

Порядок виконання роботи.

1. Вивчити короткі теоретичні відомості про шифри.
2. Створити програмне забезпечення для реалізації шифрів Полібія та Гронсфельда, з можливістю вибору українського або латинського алфавіту.
3. Скласти звіт, приєднавши отримані результати.

Вимоги до звіту.

У звіті повинні бути приведені:

1. Короткі теоретичні відомості про шифри.
2. Приклади реалізації шифрів.
3. Лістинг та скриншоти роботи програми.

Лабораторна робота №3

Тема: БІГРАМНІ ШИФРИ ТА ШИФР ВЕРНАМА

Мета роботи – практично освоїти основи побудови біграмних шифрів та шифру Вермана. Здійснити вибір ключів і провести процедуру зашифрування-розшифрування повідомлень. Зробити програмне забезпечення.

Короткі теоретичні відомості.

Біграмні шифри. У біграмних шифрахи повідомлення розбивається на біграми – блоки по дві букви Біграмні шифри були запропоновані Іоганном Трісемусом (Німеччина). У 1508 році він опублікував першу друковану роботу з криптології «Поліграфія». Шифр Playfair, заснований на біграмном шифрі, використовувався Великобританією в Першу світову війну. Для зашифрування застосовується квадрат Полібія, заповнений літерами алфавіту випадковим чином або з використанням ключового слова. За певним правилом біграма відкритого тексту замінюється на біграму: кожна буква біграми поміщається в квадрат Полібія (рис. 2).

c	i	p	h	e
r	a	b	d	f
g	k	l	m	n
o	q	s	t	u
v	w	x	y	z

Рис. 2. Квадрат Полібія для біграмного шифру

Якщо обидві літери опинилися в одному рядку, наприклад, rb, то при шифруванні беруться букви, що стоять праворуч від них: rb → ad. Якщо обидві літери опинилися в одному стовпці, наприклад, bx, то при шифруванні беруться букви, що стоять під ними: bx → lp. Якщо букви біграми лежать в різних рядках і стовпцях,

наприклад, rt, то при шифруванні беруться букви з «кутів прямокутника»: rt → do.

Вихідний текст	gr	ea	tb	ri	ta	in	is	th	el	ar	ge
Зашифрований текст	og	if	sd	ac	qd	ek	pq	yd	pn	ba	nc

У другу світову війну застосовувався біграмний шифр Double Playfair, що використовує подвійний квадрат Полібія (рис. 3). Цей шифр був запропонований англійцем Чарльзом Уїнстоном в 1854г. Для зашифрування біграми використовуються два квадрата. Перша буква біграми поміщається в перший квадрат, друга – у другій.

c	i	p	h	e
r	a	b	d	f
g	k	l	m	
o	q	s	t	u
v	w	x	y	z

d	o	u	b	l
e	s	q	a	r
c	f	g	h	i
k	m	n	p	t
v	w	x	y	z

Рис. 3. Біграмний шифр з подвійним квадратом Полібія

Якщо букви біграми утворюють прямокутник, то беруться букви з «кутів прямокутника». Якщо обидві літери лежать в одному рядку, то беруться букви з того ж рядка, що стоять на тих же місцях в протилежних таблицях.

Вихідний текст	tw	ok	ey	wo	rd	sa	re	ch	os	en
Зашифрований текст	my	ko	bz	wi	ec	pb	er	bg	mr	uu

Шифр Вернама. Шифри гамування. У основі шифрів гамування лежить метод "накладання" ключової послідовності, яка називається ***гаммою***, на відкритий текст. "Накладання" є додавання за деяким фіксованим модулем. Такі криптосистеми належать до багатоалфавітних шифрів заміни, і мають високі криптологічні властивості.

Нехай букви алфавіту A впорядковані в деякому природному порядку. Поставимо у відповідність кожній букві алфавіту її номер. Тоді можна

покласти: $A=\{1,2,...,n\}$, $|A|=n$. Припустимо, що M – деяка підмножина множини відкритих текстів A^l, K – множина ключів γ, кожен з яких є послідовністю $\gamma=\gamma_1,\gamma_2,...,\gamma_l$ з l символів. Для ключа $\gamma=\gamma_1,\gamma_2,...,\gamma_l$ і повідомлення $m=a_1,a_2,...,a_l$ введемо функцію

$$E_\gamma(a_1,a_2,...,a_l)=(b_1,b_2,...,b_l)\in C,$$

де $b_i=a_i+\gamma_i(\mathrm{mod}\,n)$, $i=1,2,...,l$. Тоді трійка множин M, K, C разом з введеною функцією $E_\gamma(a_1,a_2,...,a_l)$ називається *шифром гамування*, послідовність $\gamma_1,\gamma_2,...,\gamma_l$ – *гаммою*.

Процедура зашифрования називається *модульним гамуванням*, а кількість знаків в алфавіті – *модулем гамування*.

Перед зашифруванием формується дворядковий запис, де в одному рядку послідовно виписані знаки відкритого тексту, а в іншому – відповідні знаки гамми:

$$\begin{array}{l} a_1\ a_2\ a_3\ a_4\ a_5... \\ \gamma_1\ \gamma_2\ \gamma_3\ \gamma_4\ ...\ \gamma_l\ \gamma_1\ \gamma_2\ \gamma_3 \end{array}$$

Кожному знаку відкритого тексту відповідає свій знак гамми, тобто вони утворюють вертикальні біграми знаків.

Шифр Вернама здійснює побітове додавання n - бітового відкритого x_i тексту і n - бітового ключа k_i:

$$y_i=x_i\oplus k_i,\qquad i=1,2,...,n.$$

Шифр Вернама є абсолютно стійким шифром. Для абсолютної стійкості шифр необхідні: повна випадковість (рівноймовірно) ключа (це, зокрема, означає, що ключ не можна виробляти за допомогою якого-небудь детермінованого пристрої); рівність довжини ключа і довжини відкритого тексту; однократність використання ключа. У разі порушення хоча б однієї з цих умов шифр перестає бути абсолютно стійким і з’являються принципові можливості для його розкриття (хоча вони можуть бути важко реалізованими).

Вихідний текст	0	0	1	1	0	1	0	1
Гамма шифра	1	0	1	1	0	0	0	1
Зашифрований текст	1	0	0	0	0	1	0	0
Гамма шифра	1	0	1	1	0	0	0	1
Вихідний текст	0	0	1	1	0	1	0	1

Порядок виконання роботи.

1. Вивчити короткі теоретичні відомості про шифри.

2. Створити програмне забезпечення для реалізації біграмних шифрів та шифру Вермана. (Для Шифру Вермана вхідними даними є текстове повідомлення).

3. Скласти звіт, приєднавши отримані результати.

Вимоги до звіту.

У звіті повинні бути приведені:

1. Короткі теоретичні відомості про шифри.
2. Приклади реалізації шифрів.
3. Лістинг та скриншоти роботи програми.

Лабораторна робота №4

Тема: АЛГОРИТМ ШИФРУВАННЯ DES

Мета роботи – практично освоїти алгоритм для симетричного шифрування DES. Здійснити вибір ключів і провести процедуру зашифрування-розшифрування повідомлень. Зробити програмне забезпечення.

Короткі теоретичні відомості.

DES (англ. Data encryption standard) - алгоритм для симетричного шифрування, розроблений фірмою IBM і затверджений урядом США в 1977 році як офіційний стандарт (FIPS 46-3). Розмір блоку для DES дорівнює 64 біта. В основі алгоритму лежить мережу Фейстеля з 16 циклами (раундами) і ключем, що має довжину 56 біт.

Оригінальний текст - блок 64 біт.

Процес шифрування складається з початкової перестановки, 16 циклів шифрування і кінцевої перестановки.

Початкова перестановка табл. 1:

Таблиця 1.

Початкова перестановка IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Розбити IP (T) на дві частини L_0, R_0, де L_0, R_0 - відповідно 32 старших бітів і 32 молодших бітів блоку.

Нехай $T_i = L_i R_i$ визначається: $L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$.

Основна функція шифрування.

Аргументами функції є 32-бітовий вектор R_{i-1} і 48-бітовий ключ k_i, який є результатом перетворення 56-бітового ключа шифра к.

Для обчислення функції f послідовно використовуються:

1. Функція розширення E;

2. сума по модулю 2 з ключем k_i;

3. перетворення S, що складається з 8 перетворень S-блоків $S_1,....,S_8$;

4. перестановка P.

Таблиця 2.

Функція розширення E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Отриманий після перестановки блок $E(R_{i-1})$ складається по модулю 2 з ключами k_i, а потім представляється у вигляді восьми послідовних блоків $B_1,...,B_8$.

$E(R_{i-1}) \oplus k_i = B_1 B_2 ... B_8$.

Кожен блок є 6-бітовим блоком. Далі кожен із блоків трансформується в 4-бітовий блок B'_j за допомогою перетворень S_j, табл. 3.

Таблиця 3.

S перестановки

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S_4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S_6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S_7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S_8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Припустимо, що перша 6-бітова частина 48-бітового вхідного блоку має значення 110110. Оскільки вона перша, то заміна буде виконуватися на першому S-боксі, табл. 4:

Таблиця 4.

Приклад трансформації 6-бітного блоку у 4-бітний

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Перша "1" та останній "0" вхідної частини разом (10 дають двійку в десятковому представленні) вказують, що для заміни буде використовуватися рядок № 2. Середні чотири біти (1011) дають в десятковому представленні число 11. Отже, для заміни буде використано стовпчик № 11. На перетині рядка № 2 та стовпчика № 11 знаходиться комірка з числом 7. Воно, точніше його двійкове представлення 0111, і буде результатом застосування S-боксу. Таким чином, замість 6-бітного числа 110110 отримаємо 0111. Аналогічним чином виконуються й заміни інших 6-бітних частин вхідного 48-бітного числа.

Значення функції $f(R_{i-1}, k_i)$ отримується перестановкою P, відносно $B'_1 B'_2 ... B'_8$, табл. 5.

Таблиця 5.

Перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

$$f(R_{i-1}, k_i) = P(B'_1 B'_2 \dots B'_8)$$

Кінцева перестановка діє на T_{16} і є оберненою до початкової, табл. 6.

Таблиця 6.

Кінцева перестановка

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Схема розшифрування. При розшифрування даних всі дії виконуються в зворотному порядку. У 16 циклах розшифрування, на відміну від шифрування с допомогою прямого перетворення мережею Фейстеля, тут використовується зворотне перетворення мережею Фейстеля.

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus f(L_i, k_i)$$

Порядок виконання роботи.

1. Вивчити короткі теоретичні відомості про алгоритм шифрування DES.
2. Створити програмне забезпечення для реалізації алгоритму DES, зашифрування та розшифрування тексту.
3. Скласти звіт, приєднавши отримані результати.

Вимоги до звіту.

У звіті повинні бути приведені:

1. Короткі теоретичні відомості.
2. Зашифровані (розшифровані) повідомлення.
3. Лістинг та скриншоти роботи програми.

Лабораторна робота №5

Тема: АЛГОРИТМ ШИФРУВАННЯ RSA

Мета роботи – практично освоїти алгоритм з відкритим ключем RSA. Здійснити вибір ключів і провести процедуру зашифрування-розшифрування повідомлень. Зробити програмне забезпечення.

Короткі теоретичні відомості.

Перший повноцінний алгоритм з відкритим ключем, який можна використовувати для шифрування і цифрового підпису: RSA.

Безпека RSA заснована на труднощі розкладання на множники великих чисел. Відкритий і закритий ключі є функціями двох великих (100 - 200 розрядів або навіть більше) простих чисел. Відновлення відкритого тексту по шифротексту і відкритого ключа еквівалентно розкладанню на множники двох великих чисел.

Для генерації двох ключів використовуються два великих випадкових простих числа, p і q. Для максимальної безпеки вибирайте p і q рівної довжини. Розраховується добуток:

$n = p \cdot q.$

Потім випадковим чином вибирається ключ шифрування *e*, такий що *e* і *(p-1) (q-1)* є взаємно простими числами. Нарешті розширений алгоритм Евкліда використовується для обчислення ключа дешифрування d, такого що

$$ed = 1(\mathrm{mod}(p-1)\cdot(q-1)).$$

$$d = e^{-1} \bmod (p-1)\cdot(q-1).$$

Два простих числа p і q більше не потрібні. Вони повинні бути відкинуті, але не повинні бути розкриті.

Для шифрування повідомлення *m* воно спочатку розбивається на цифрові блоки, менші *n*. Тобто, якщо *p* і *q* - 100-розрядні прості числа, то *n* буде містити близько 200 розрядів, і кожен блок повідомлення m_i повинен бути близько 200 розрядів в довжину. Формула шифрування виглядає так:

$$c_i = m_i^e \bmod n.$$

Для розшифрування повідомлення беремо кожен зашифрований блок c_i:

$$m_i = c_i^d \bmod n.$$

Шифрування RSA

Відкритий ключ: n добуток двох простих чисел p і q (p і q повинні зберігатися в секреті) e число, взаємно просте з (p-1) (q-1).

Закритий ключ: d e^{-1} mod ((p-1) (q-1)).

Шифрування: c = m^e mod n.

Дешифрування: m = c^d mod n.

Приклад 1.

Якщо p = 47 і q = 71, то n = pq = 3337.

Ключ *e* не повинен мати спільних множників

(p-1) (q-1) = 46 * 70 = 3220.

Виберемо (випадково) *e* рівним 79. В цьому випадку

d = 79^{-1} mod 3220 = 1019.

При обчисленні цього числа використаний розширений алгоритм Евкліда. Опублікуємо *e* і *n*, зберігши в секреті *d*. Відкинемо p і q. Для шифрування повідомлення:

m = 6882326879666683

спочатку розділимо його на маленькі блоки. Для нашого випадку підійдуть трьохбуквені блоки. Повідомлення розбивається на шість блоків m_i

m_1 = 688

m_2 = 232

m_3 = 687

m_4 = 966

m_5 = 668

m_6 = 003

Перший блок шифрується, як 688^{79} mod 3337 = 1570 = c_l

Виконуючи ті ж операції для наступних блоків, створює шифротекст повідомлення: c = 1570 2756 2091 2276 2423 158

Для дешифрування потрібно виконати таке ж піднесення до степеня, використовуючи ключ дешифрування 1019:

$1570^{1019} \bmod 3337 = 688 = m_1$.

Аналогічно відновлюється решта повідомлення.

Приклад 2.

Етап	Опис операції	Результат операції
Генерація ключів	Обрати два простих різних числа	$p = 3557,$ $q = 2579$
	Обчислити добуток	$n = p \cdot q = 3557 \cdot 2579 = 9173503$
	Обчислити функцію Ейлера	$\varphi(n) = (p-1)(q-1) = 9167368$
	Обрати відкриту експоненту	$e = 3$
	Обчислити секретну експоненту	$d = e^{-1} \mod \varphi(n)$ $d = 6111579$
	Опублікувати *відкритий ключ*	$\{e, n\} = \{3, 9173503\}$
	Зберегти *секретний ключ*	$\{d, n\} = \{6111579, 9173503\}$
Шифрування	Обрати текст для шифрування	$m = 111111$
	Обчислити шифротекст	$c = E(m)$ $= m^e \mod n$ $= 111111^3 \mod 9173503$ $= 4051753$
Розшифрування	Обчислити вихідне повідомлення	$m = D(c) =$ $= c^d \mod n$ $= 4051753^{6111579} \mod 9173503$ $= 111111$

Порядок виконання роботи.

1. Вивчити короткі теоретичні відомості про алгоритм шифрування RSA.

2. Створити програмне забезпечення для реалізації алгоритму RSA, зашифрування та розшифрування тексту.

3. Скласти звіт, приєднавши отримані результати.

Вимоги до звіту.

У звіті повинні бути приведені:

1. Короткі теоретичні відомості.

2. Зашифровані (розшифровані) повідомлення.

3. Лістинг та скриншоти роботи програми.

Лабораторна робота №6

Тема: СЕМІНАРСЬКЕ ЗАНЯТТЯ ЗГІДНО ІНДИВІДУАЛЬНИХ ТЕМ

1. Законодавча база України відповідно до систем безпеки.
2. Поняття про інформацію з обмеженим доступом.
3. Критерії європейського стандарту у галузі оцінки захищеності комп’ютерних систем.
4. Основні поняття українського стандарту у галузі оцінки захищеності комп’ютерних систем – НД ТЗІ 2.5-004-99 України.
5. Основні рівні довіри відповідно до європейського стандарту.
6. Послуги та механізми безпеки інформаційних систем.
7. Класифікація сучасних криптосистем та основні вимоги до них.
8. Класифікація симетричних криптосистем та основні вимоги щодо їх безпеки.
9. Класифікація асиметричних криптосистем та основні вимоги щодо їх безпеки.
10. Основні поняття роботи К. Шеннона "Теорія зв’язку в секретних системах".
11. Комбіновані криптосистеми. Їх переваги та недоліки.
12. Сітка Х. Фейстеля, її переваги та недоліки.
13. Основні модифікації шифру DES (3DES, DESX). Переваги та недоліки.
14. Основні операції шифрування алгоритму криптографічного перетворення ГОСТ 28147-89.
15. Сучасні потокові шифри, їх переваги та недоліки.
16. Протокол забезпечення конфіденційності даних за допомогою асиметричного алгоритму RSA.
17. Протокол колективного підпису на основі протоколу ECPR.
18. Сучасні алгоритми побудови каскадних геш-функцій на універсальних класах.
19. Безпека керування ключами.Протоколи забезпечення безпеки ключів.

20. Основні принципи захисту інформації при підключенні до мережі Інтернет.
21. Захист інформації в інформаційних системах за допомогою міжмережевих екранів.
22. Захист інформації на мережному рівні за допомогою протоколів TLS, SSL, IPSec.
23. Основні режими використання мережних протколів.
24. Забезпечення конфіденційності, цілісності та автентичності даних в IP-мережах з використанням протоколу ESP (IPSec).
25. Забезпечення безпеки даних в інформаційних системах за допомогою Log-сервера.
26. Забезпечення безпеки даних в інформаційних системах за допомогою Proxy-сервера.
27. Організація захисту пам’яті в сучасних ПК.
28. Захист пам’яті ПК методом граничних регістрів.
29. Захист пам’яті методом ключей захисту.
30. Моделі безпеки, що застосовуються при побудові захисту в СУБД.
31. Формальні моделі доступу до інформації. Дискреційний та мандатний доступ до даних в інформаційних системах.
32. Основи захищеності сучасних операційних систем.
33. Підсистема захисту в ОС Windows. Основні послуги та механізми захисту.
34. Підсистема захисту в ОС Linux. Основні переваги і недоліки.
35. Порівняння архітектури Windows та Linux. Основні можливості підсистем захисту ОС.

Перелік питань на підсумковий контроль

1. Вкажіть у чому складність створення систем захисту інформації.
2. Опишіть поняття захисту інформації в ІТС та її роботи з організації.
3. Опишіть поняття теорії захисту інформації та її періоди розвитку.
4. Наведіть особливості теорії захисту інформації.
5. Вкажіть у чому полягають формальні та неформальні підходи до розгляду питань теорії захисту інформації.
6. Вкажіть, які є напрямки розвитку теорії захисту інформації.
7. Вкажіть, що собою представляє загроза безпеки КС.
8. Вкажіть, які загрози безпеки КС відносять до випадкових.
9. Вкажіть, які загрози безпеки КС відносять до навмисних.
10. Вкажіть, що собою представляє загроза розкриття і їх протидія.
11. Вкажіть, що собою представляє загроза порушення цілісності і їх протидія.
12. Вкажіть, що собою представляє загроза відмови в обслуговуванні.
13. Вкажіть напрями повсякденної діяльності в ІТС для підтримки її працездатності.
14. Вкажіть якими послугами забезпечується доступність в ІТС.
15. Вкажіть, що собою представляє спосіб несанкціонованого доступу та які мети переслідує зловмисник.
16. Вкажіть, що таке комп'ютерне піратство та категорії порушників безпеки.
17. Вкажіть, що визначає модель порушника безпеки.
18. Опишіть концепцію захисту інформації.
19. Опишіть стратегію захисту інформації та ієрархічний підхід до забезпечення безпеки інформації.
20. Опишіть етапи розробки концепції захисту інформації.
21. Вкажіть поняття політики захисту інформації.
22. Охарактеризуйте правові та організаційно-адміністративні заходи протидії комп'ютерним злочинам.

23. Охарактеризуйте інженерно-технічні заходи протидії комп’ютерним злочинам.

24. Вкажіть комплекс задач при розробці політики безпеки.

25. Вкажіть правила забезпечення політики безпеки інформації.

26. Опишіть перший етап проектування та реалізації системи захисту.

27. Вкажіть, які ймовірні загрози виділяють у комп’ютерних мережах.

28. Вкажіть, яким заходам повинна визначатися політика безпеки.

29. Опишіть другий етап проектування та реалізації системи захисту – реалізація політики безпеки.

30. Опишіть третій етап проектування та реалізації системи захисту – підтримка політики безпеки.

31. Опишіть дискреційну політику безпеки.

32. Опишіть переваги та недоліки дискреційної політики безпеки.

33. Опишіть мандатну політику безпеки.

34. Опишіть переваги та недоліки мандатної політики безпеки.

35. Опишіть рольову політику безпеки.

36. Опишіть політику безпеки - монітор безпеки.

37. Вкажіть, що собою представляє криптографія.

38. Вкажіть для забезпечення чого можна використовувати криптографію.

39. Вкажіть, що застосовують для виявлення несанкціонованих змін у переданих повідомленнях.

40. Вкажіть, що собою представляє криптографічний захист.

41. Вкажіть, які вимоги ставляться перед криптографічними системами захисту інформації.

42. Опишіть поняття симетричного шифрування.

43. Опишіть поняття несиметричного шифрування.

44. Розкрийте поняття потокових та блокових алгоритмів шифрування.

45. Охарактеризуйте найпопулярніші алгоритми шифрування.

46. Опишіть особливості симетричних криптоалгоритмів.

47. Опишіть особливості несиметричних криптоалгоритмів.

48. Вкажіть, які методи захисту інформації у операційних системах.

49. Зобразіть загальну схему алгоритму шифрування DES.

50. Опишіть алгоритм шифрування DES.

51. Опишіть алгоритм операції розгортання ключа у DES.

52. Вкажіть на переваги та недоліки алгоритму шифрування DES.

53. Опишіть алгоритм шифрування RSA.

54. Наведіть означення спадкування та включення у об’єктно-орієнтованому аналізі.

55. Опишіть поняття нелегітимних відносин руйнуючого програмного забезпечення.

56. Опишіть основні підкласи, що відносяться до класу руйнуючого програмного забезпечення.

57. Сформулюйте загальний критерій безпеки системи.

58. Опишіть поняття безпеки програмного забезпечення.

59. Опишіть контрольно-іспитовий метод аналізу безпеки ПЗ.

60. Опишіть логіко-аналітичний метод аналізу безпеки ПЗ.

61. Опишіть формальну постановку задачі аналізу безпеки ПЗ за допомогою контрольно-іспитових методів.

62. Наведіть схему аналізу безпеки програм контрольно-іспитовими методами.

63. Опишіть формальну постановку задачі аналізу безпеки ПЗ за допомогою логіко-аналітичних методів.

64. Наведіть схему аналізу безпеки програм логіко-аналітичними методами.

65. Наведіть означення геш-функції.

66. Дайте означення стійкості за першим та другим прообразом.

67. Дайте означення односторонньої геш-функції.

68. Вкажіть, коли геш-функція стійка до колізій.

69. Вкажіть, що собою представляють безключові геш-функції.

70. Вкажіть, що собою представляють ключові геш-функції.

71. Розкрийте поняття електронного цифрового підпису.

72. Наведіть властивості електронного цифрового підпису.

73. Сформулюйте вимоги до електронного цифрового підпису.

74. Опишіть, як класифікуються електронні цифрові підписи.

75. Опишіть алгоритми генерації та верифікації ЕЦП.

76. Опишіть схеми ЕЦП з додаванням та відновленням повідомлення.

77. Розкрийте поняття симетричної та асиметричної схеми ЕЦП.

78. Вкажіть, як використовується RSA для цифрового підпису.

79. Вкажіть, що розуміють під керуванням ключами.

80. Вкажіть, яка мета керування ключами.

81. Вкажіть основні стани криптографічного ключа у життєвому циклі.

82. Вкажіть перехідні стани криптографічного ключа у життєвому циклі.

83. Вкажіть, якими функціями керування ключами підтримується його життєвий цикл.

84. Вкажіть, які етапи та процеси містить життєвий цикл керування ключами.

Література та джерела

1. Бобало Ю. Я. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.
2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грай- воронський, О. М. Новіков. - К. : Видавнича група ВНУ, 2009. - 608 с.
3. Юдін О. К. Захист інформації в мережах передачі даних: підручник МОН України / О. К. Юдін, Г. Ф. Конахович, О. Г. Корченко. - К. :, 2009. - 714 с.
4. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
5. Березюк Б. М. Системи і мережі передавання даних: навч. посіб. / Б. М. Березюк. - Серія “Дистанційне навчання”. № 34. - Львів : Вид-во Національного університету “Львівська політехніка”, 2005. - 200 с.
6. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К. : ДУТ, 2015. - 288 с.
7. Про захист персональних даних [Електронний ресурс]: закон України № 2297-VI: [прийнятий Верховною Радою України 2010 р. : редакція від 27 жовтня 2022 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Про інформацію [Електронний ресурс]: закон України № 2657-XII: [прийнятий Верховною Радою України 1992 р. : редакція від 21 березня 2023 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
9. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: закон України № 2163-VIII: [прийнятий Верховною Радою України 2017 р. : редакція від 17 серпня 2022 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
10. Про державну таємницю [Електронний ресурс]: закон України № 3855-XII: [прийнятий Верховною Радою України 1994 р. : редакція від 31 березня 2023 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text