**ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ
ТА ТЕХНОЛОГІЙ**

Кафедра спеціалізованих комп'ютерних систем

МЕТОДИЧНІ ВКАЗІВКИ

**до лабораторних робіт
з дисципліни**

***«ЗАХИСТ ІНФОРМАЦІЇ
В КОМП'ЮТЕРНИХ СИСТЕМАХ»***

Харків – 2017

Методичні вказівки розглянуто і рекомендовано до друку на засіданні кафедри спеціалізованих комп’ютерних систем 13 лютого 2017 р., протокол № 8.

Описано методику та практичне застосування елементів захисту інформації при проектуванні систем залізничної автоматики.

Методичні вказівки призначені для студентів спеціальності 123 — Комп’ютерна інженерія, які вивчають дисципліну «Захист інформації в комп'ютерних системах», денної та заочної форм навчання та інституту перепідготовки кадрів.

Укладач

проф. М. А. Мірошник

Рецензент

проф. С. В. Лістровий

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт
з дисципліни

*«ЗАХИСТ ІНФОРМАЦІЇ
В КОМП'ЮТЕРНИХ СИСТЕМАХ»*

Відповідальний за випуск Мірошник М. А.

Редактор Решетилова В. В.

Підписано до друку 05.04.17 р.

Формат паперу 60х84 1/16. Папір писальний.

Умовн.-друк.арк. 2,25. Тираж 50. Замовлення №

Видавець та виготовлювач Українська державна академія залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб’єкта видавничої справи ДК № 2874 від 12.06.2007 р.

ЗМІСТ

Вступ…… 4
1 Шифрування повідомлень за допомогою класичних методів підстановки……. 5
2 Шифрування і розшифрування повідомлень за схемою несиметричного шифрування RSA і Ель-Гамаля……. 12
3 Розрахунок параметрів алгоритмів цифрового підпису RSA і Ель-Гамаля……. 17
4 Захист мережі Wi-Fi…… 23
5 Побудова шифротвірних пристроїв симетричних потокових систем криптографічного перетворення інформації і їх криптоаналіз…… 28
6 Розрахунок параметрів протоколу аутентифікації з нульовою передачею знань Фейге – Фіата – Шаміра…….. 35
7 Протидія шкідливим програмам…… 41
8 Організація віртуальної приватної мережі (OpenVPN)…….. 49
Список літератури…….. 56

ВСТУП

Для зміцнення знань, отриманих студентами на лекціях, і набуття навичок, необхідних для самостійного розв’язання задач захисту інформації в комп'ютерних системах, навчальним планом зі спеціальної дисципліни «Захист інформації в комп'ютерних системах», що викладається при підготовці бакалаврів за спеціальністю 123 – Комп’ютерна інженерія, передбачається проведення лабораторних робіт.

Дані методичні вказівки допоможуть студентам підготуватися до самостійної і лабораторних робіт. Розділи методичних вказівок відповідають розділам зазначеної дисципліни та лабораторних робіт. Практичне застосування елементів захисту інформації при проектуванні систем залізничної автоматики розглядається в лабораторному практикумі цієї дисципліни.

На сучасному етапі розвитку суспільства одним із пріоритетних завдань є подальший розвиток методів автоматизованого проектування на базі нових інформаційних технологій . У центрі уваги вищої школи постійно перебувають питання підготовки фахівців у галузі інформаційної безпеки. Окремою проблемою є аналіз ефективності застосування тих чи інших інформаційних технологій у навчальному процесі.

Лабораторна робота складається з постановки задачі і її розв’язання, складання лабораторного макета та проведення експерименту. Для самостійної підготовки до лабораторної роботи необхідно вивчити матеріал за конспектом лекцій і літературними джерелами, зрозуміти методику розв’язання поданих задач і скласти короткий конспект матеріалів, необхідних для виконання лабораторної роботи. Для кожного заняття наведені: тема, мета заняття, коротке викладення відповідного теоретичного підґрунтя, контрольні запитання для самоперевірки, контрольний приклад і його розв’язання, приклади для розв’язання безпосередньо під час заняття.

1 ШИФРУВАННЯ ПОВІДОМЛЕНЬ ЗА ДОПОМОГОЮ КЛАСИЧНИХ МЕТОДІВ ПІДСТАНОВКИ

1.1 Теоретичні відомості до лабораторної роботи

Однією з найбільш простих серед схем шифрування підстановкою, стійких до частотного криптоаналізу, є схема Віженера. Таблиця є квадратною матрицею розмірності m x m, де m – число символів алфавіту. У першому рядку матриці записуються літери алфавіту в порядку черговості, в другому – та сама послідовність літер, але зі зсувом вліво на одну позицію, в третьому – із зсувом на дві позиції і т. д. Вивільнені справа місця заповнюються витісненими вліво буквами, записуваними в природній послідовності.

Для шифрування тексту встановлюється буквений ключ, який являє собою деяке слово або набір букв. Далі з повної матриці вибирається підматриця шифрування, що включає, наприклад, перший рядок і рядки матриці, початковими буквами яких є послідовні букви ключа.

Процес шифрування включає в себе таку послідовність дій:

• під кожною буквою тексту, що шифрується, записуються літери ключа, які повторюють його необхідну кількість разів;

• кожен символ (буква) тексту, що шифрується, замінюється на букву з підматриці шифрування, розташовану на перетині колонки, що містить змінну букву в першому рядку підматриці шифрування, і рядка, що починається з відповідної літери ключа;

• вихідний текст розбивається на підгрупи по h символів.

Розкрити шифротекст, отриманий з даного алгоритму, тільки на основі статистичних характеристик мови, неможливо, так як одні й ті самі символи відкритого тексту можуть бути замінені різними символами з шифрувальної матриці. З іншого боку, різні літери відкритого тексту можуть бути замінені однаковими символами з шифрувальної матриці.

Розшифровка тексту виконується в такій послідовності:

- під буквами шифротекста зверху послідовно записуються літери ключа;

- в рядку підматриці таблиці Віженера для кожної літери відшукується буква, відповідна знаку (букві) шифротексту; буква

першого рядка, що знаходиться над нею, і буде символом розшифрованого (вихідного) тексту;

- отриманий текст групується в слова за змістом.

Один з недоліків шифрування за схемою Віженера – невисока криптостійкість при невеликій довжині ключа. Крім того, в ключі не допускається повторення букв, бо інакше шифрування буде неоднозначним.

Основою шифру Плейфера, винайденого в 1854 році, є шифруюча таблиця (матриця) з випадково розташованими символами алфавіту вихідного повідомлення.

Відкритий текст розбивається на пари символів хіхі + 1, після чого кожна пара символів відкритого тексту замінюється на пару символів з таблиці таким чином:

а) якщо символи знаходяться в одному рядку, то кожен із символів пари замінюється на той, що стоїть праворуч від нього (за останнім символом у рядку слідує перший);

б) якщо символи знаходяться в одній колонці, то кожен символ пари замінюється на символ, розташований нижче його в колонці (за останнім нижнім символом слідує верхній);

в) якщо символи пари знаходяться в різних рядках і колонках, то вони вважаються протилежними кутами прямокутника. При цьому символ, що знаходиться в лівому кутку, замінюється на символ, який стоїть в іншому лівому кутку; заміна символу, що знаходиться в правому куті, здійснюється аналогічно;

г) якщо у відкритому тексті зустрічається два однакових символи поспіль, то перед шифруванням між ними вставляється деякий інший символ, що не несе смислового навантаження (наприклад, тире).

Ідея криптоперетворень на основі афінної системи Цезаря полягає в тому, що символи шифротексту виходять із символів вихідного тексту на основі відображення вигляду

$$j \to (aj + b)(\mathrm{mod}\ m),$$

де j – числовий код символу відкритого тексту; m – підстава (число символів) алфавіту вихідного тексту; (Aj + b) (mod m) – числовий код відповідного символу шифротексту. При цьому a, b –

цілі числа, такі, що 0 <a, b <m, при цьому числа a і m – взаємнопрості.

1.2 Приклад розв'язання типової задачі до лабораторної роботи

Наприклад, для латинського алфавіту m = 26. Приймемо a = 3, b = 5. Очевидно, що числа 3 і 26 взаємнопрості. Тоді можна отримати наступне відповідність між числовими кодами символів відкритого тексту і числовими кодами символів вектора заміни, а також між символами вихідного тексту і символами вектора заміни, які наведені у таблиці 1.1.

Таблиця 1.1 – Символи вихідного тексту і символи вектора заміни

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
алфавіт вихідного тексту	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
Aj+b	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2
вектор заміни	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

В цьому випадку результат шифрування тексту, наприклад, WE ARE STUDENTS, на основі даної таблиці буде таким: TR FER HKNORSKH. Так, наприклад, в даному випадку символ W вихідного тексту, який має порядковий номер в алфавіті 22, відображається в символ T, що має порядковий номер в алфавіті 19, оскільки (3-22 + 5) mod26 = 19.

Слід зауважити, що незалежно від величини m нумерацію символів алфавіту потрібно починати з 0, оскільки в іншому випадку буде мати місце ситуація, коли одному з символів вихідного алфавіту неможливо буде поставити у відповідність будь-який символ через те, що результатом перетворення (aj + b) (mod m) виявиться 0. Так, для наведеного прикладу, якщо нумерацію символів латинського алфавіту робити з 1, то символу

G, який буде в цьому випадку мати порядковий номер j = 7, неможливо буде поставити у відповідність ніякого символу, так як (3j + 5) (mod 26) = 0.

На додаток до описаних методів розглянемо метод гамування. Даний метод заснований на додаванні символів вихідного тексту і деякої послідовності символів, що формується на основі ключа, по модулю, рівному довжині алфавіту n. Для дешифрування шифротексту, тобто відновлення початкового тексту, одержувач зашифрованого повідомлення виконує перетворення, тобто кожен біт отриманого зашифрованого тексту складає по модулю 2 з відповідним бітом гамма-послідовності.

Наприклад, якщо перші значення, згенеровані датчиком ПВЧ (псевдовипадкові числа), є 21794567, то відкритий текст НАКАЗ зашифрують таким чином (при цьому код кожної букви відкритого тексту записується в двійковому вигляді з використанням п'яти розрядів, а кожна цифра гамма-послідовності – чотирьох):

10000	10001	01001	01011	00001	01000
m_1	m_2	m_3	m_4	m_5	m_6
00100	00101	11100	10100	01010	11001
Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
10100	10100	10101	11111	01011	10001
c_1	c_2	c_3	c_4	c_5	c_6

Потім кожному п’ятирозрядному двійковому числу ставиться у відповідність літера вихідного алфавіту. При цьому розмірність алфавіту повинна бути не більше 32 символів, щоб була можливість їх подати у вигляді п’ятирозрядного двійкового числа, а нумерація символів повинна проводитися з 0 до 31.

В даному випадку, якщо виключити з алфавіту, наприклад, символ видання, щоб зробити його розмірність рівною 32, отримаємо, що перший символ слова П відобразиться в символ У, тоді шифротекст буде УУФЯКР.

1.3 Хід виконання лабораторної роботи

Постановка задачі для виконання лабораторної роботи

Зашифрувати своє прізвище, використовуючи:

а) методи шифрування підстановкою на основі:

1) схеми Віженера, використовуючи як ключ слово БЛАГО;

2) шифру Плейфера, якщо шифруюча схема задана таблицею 1.2;

3) афінної системи Цезаря, де як ключ виступає пара чисел (a, b), значення яких задані в таблиці варіантів вихідних даних (таблиця 1.3). Історична довідка: слово «афінний» походить від латинського affine, що означає «суміжний», «сусідній».

б) метод гамування, за умови, що перші значення гамма-послідовності, згенеровані датчиком псевдовипадкових чисел, є 32461587942. Код кожної букви шифрованого тексту записується в двійковому вигляді з використанням п'яти розрядів, а кожна цифра гамми – чотирьох.

Таблиця 1.2

А	Ь	М	Б	Ц	,
Г	Н	Ч	Ы	О	Д
Ъ	Е	В	У	Ю	Э
Ж	Р	К	И	З	Й
С	Х	Щ	П	Т	Л
.	Я	-	Ш	Ф	_

Таблиця 1.3

Номер варіанта	a	b	Номер варіанта	a	b	Номер варіанта	a	b
1	5	9	10	7	9	19	3	7
2	7	8	11	3	7	20	9	6
3	3	6	12	9	6	21	5	10
4	9	7	13	5	4	22	7	4
5	5	7	14	7	6	23	3	9
6	7	8	15	3	8	24	5	7
7	3	8	16	9	5	25	7	5
8	9	9	17	5	9	26	7	6
9	5	8	18	7	8			

Розв'язання типового прикладу.

Нехай необхідно зашифрувати повідомлення DATA MANAGEMENT SYSTEM за допомогою схеми Віженера при h = 5 і ключовому слові REGIN. У цьому випадку повна матриця (26 x 26) і подматриця шифрування мають вигляд, показаний відповідно у таблицях 1.4 і 1.5.

Тоді процес шифрування ілюструється таблицею 1.6.

Таблиця 1.4

ABCDEFGH…XYZ
BCDEFGHI… YZA
CDEFGHIJ … ZAB
DEFGHIJK … ABC
..
ZABCDEFG…WXY

Таблиця 1.5

ABCD . . . XYZ
RSTU . . .
EFGH . . .
GHIJ . . .
IJKL . . .
NOPQ . . .

Таблиця 1.6 – Процес шифрування

текст, що шіфрується	DATA MANAGEMENT SYSTEM
ключ	REGI NREGINREGI NREGIN
текст після заміни	UEZI ZRRGORDITB FPWZMZ
остаточний шифротекст	UEZIZ RRGOR DITBF FWZMZ

Так, наприклад, під першою літерою тексту, що шіфрується, D розташовується буква R ключа. У першому рядку підматриці (див. таблицю 1.5) знаходимо букву D і вибираємо з даної підматриці букву, що знаходиться на перетині рядка з початковою літерою R (першою літерою ключа) і колонки, початковою літерою якого є D. Цією буквою є U. Потім виконується заміна вихідної букви D на букву U у вихідному тексті і т.д. Відкритий текст "ШИФР Плейфера" за допомогою шифрувальної таблиці 1.7.

Таблиця 1.7 – Шифрувальна таблиця

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

перетвориться в шифротекст РДІИЙ-РЛУЮ М.

Література [1, с. 334 – 344; 2 с. 339 – 346; 3, с. 28 – 43; 4, с. 39 – 51].

Контрольні питання

1 Для чого необхідна модель поведінки потенційного порушника?

2 Класи безпеки. Сутність та стисла характеристика.

3 Які основні поняття використовуються при описі елементарної моделі захисту?

4 Наведіть вираз для визначення елементарного захисту, розкрийте його фізичний зміст.

5 Наведіть умову міцності перешкоди з виявленням та блокуванням несанкціонованого доступу.

6 Наведіть та проаналізуйте формулу для розрахунку міцності перешкоди з властивостями виявлення та блокування.

7 Наведіть та проаналізуйте формулу для розрахунку міцності перешкоди з урахуванням можливої відмови системи контролю.

8 Наведіть та проаналізуйте формулу для розрахунку міцності багатокільцевого захисту при використанні неконтрольованих перешкод.

9 Наведіть та проаналізуйте формулу для розрахунку міцності багатокільцевого захисту з контрольованими перешкодами.

10 Наведіть та проаналізуйте формулу для розрахунку сумарної міцності дублюючих перешкод.

2 ШИФРУВАННЯ І РОЗШИФРУВАННЯ ПОВІДОМЛЕНЬ ЗА СХЕМОЮ НЕСИМЕТРИЧНОГО ШИФРУВАННЯ RSA І ЕЛЬ-ГАМАЛЯ

2.1 Теоретичні відомості до лабораторної роботи

Виступаючи в ролі відправника і одержувача повідомлення, зашифрувати, а потім розшифрувати за допомогою криптоалгоритму RSA повідомлення, яке являє собою ім'я та прізвище студента, у вигляді послідовності цілих чисел в діапазоні 0 ... 33, де між буквами алфавіту і числами із зазначеного діапазону існує взаємно однозначна відповідність (пробілу між ім'ям і прізвищем відповідає 0). Вибір відкритого ключа для шифрування зробити самостійно.

Значення пари простих чисел p, q вибираються з таблиці 2.1 відповідно до варіанта завдання.

Таблиця 2.1

Номер варіанта	p	q	Номер варіанта	p	q
1	11	5	11	19	11
2	7	13	12	11	17
3	17	3	13	23	5
4	3	19	14	19	17
5	11	13	15	41	3
6	19	5	16	5	43
7	7	17	17	31	13
8	13	3	18	29	11
9	23	5	19	41	5
10	7	23	20	17	19

2.2 Розв'язання типового прикладу шифрування та розшифрування повідомлення CAB

2.2.1 Дії отримувача повідомлення

а) Оберемо p=3, q=11;

б) визначимо $N=p \cdot q=33$;

в) обчислення $\varphi(N)=(3-1)(11-1)=20$;

г) вибір K_e з урахуванням умов $1<K_e \leq 20$, $(K_e, 20)=1$.

Нехай $K_e=7$;

д) обчислення значення секретного ключа K_d з використанням методу ланцюгових дробів Евкліда за допомогою розв'язання рівняння $7K_d=1(\text{mod}20)$ або $K_d=7^{-1}(\text{mod}20)$. Рішенням є $K_d=3$. Дане рівняння також може бути розв'язано на основі співвідношення $K_d = K_e^{\varphi(n)-1}(\text{mod}n)$, де $n = \varphi(N)$, тобто за допомогою попереднього обчислення значення функції Ейлера для величини $\varphi(N)$ (тобто необхідно обчислити $\varphi(\varphi(N))$). У наведеному прикладі маємо: $K_d = K_e^{\varphi(20)-1}(\text{mod}20) = K_e^{8-1}(\text{mod}20) = = 7^7(\text{mod}20) = = 823543(\text{mod}20) = 3(\text{mod}20)$;

е) пересилання відправнику повідомлення пари чисел ($N=33$, $K_e=7$).

2.2.2 Дії відправника повідомлення:

а) подання повідомлення у вигляді послідовності цілих чисел (тобто вихідне повідомлення довжиною n, подане у двійковому вигляді, розбивається на блоки однакової довжини h, кожен з яких може бути поданий у вигляді десяткового числа з діапазону значень $0 \ldots 2^h-1$). Якщо в нашому випадку вважати, що кожен символ повідомлення являє собою окремий блок, а також прийняти, що літера А подається числом 1, літера В – числом 2, а літера С – числом 3, то передане повідомлення можна подати послідовністю чисел 3, 1, 2, тобто $m_1 = 3$, $m_2 = 1$, $m_1 = 2$;

б) шифрування тексту з використанням ключа і модуля $N = 33$, надісланих одержувачем, за формулою

$$C_i = m_i^{K_e}(\text{mod}N) = m_i^7(\text{mod}33)$$

Маємо:

$C_1 = 37(\text{mod}33) = 2187(\text{mod}33) = 9$;

$C_2 = 1^7(\text{mod}33) = 1(\text{mod}33) = 1$;

$C_3 = 2^7(\text{mod}33) = 128(\text{mod}33) = 29$.

Відправлення отримувачу криптограми C = C_1, C_2, C_3, = 9, 1, 29;

в) дії отримувача повідомлення: розшифрування прийнятої криптограми за формулою

$$m_i = C_i^{K_d} (\text{mod} N) = C_i^3 (\text{mod} 33) \ .$$

Маємо:

$$m_1 = 9^3(\text{mod}33) = 729(\text{mod}33) = 3;$$
$$m_2 = 1^3(\text{mod}33) = 1(\text{mod}33) = 1;$$
$$m_3 = 29^3(\text{mod}33) = 24389(\text{mod}33) = 2.$$

Таким чином, відновлено вихідне повідомлення

$$M = m_1, m_2, m_3 = 3, 1, 2 = CAB.$$

2.3 Постановка завдання лабораторної роботи

Відповідно до заданих значень параметрів алгоритму Ель-Гамаля, які наведені в таблиці 2.2, зробити шифрування повідомлення M (свого прізвища) і його розшифрування. Значення K вибрати довільно.

Для того щоб згенерувати пару ключів (K_c, K_d), спочатку обирають деяке велике просте число P і велике ціле число G, причому G<P. Дані числа можуть бути опубліковані серед користувачів. Одержувач повідомлення обирає випадкове число X (X<P), яке виступає як секретний ключ K_d, і обчислює

$$Y = G^X \text{mod} PY, \qquad (2.1)$$

де Y виступає як відкритий ключ K_e, використовується при шифруванні повідомлення M.

Для того щоб зашифрувати повідомлення, його відправник обирає випадкове ціле число K (1 < K < P-1) таке, що (K, P-1) = 1, а потім обчислює числа

$$a = G^K \text{mod} P, \ b = Y^K M \text{mod} P \qquad (2.2)$$

Пара чисел (a, b) є шифротекстом, причому довжина шифротексту вдвічі більше довжини вихідного відкритого тексту M, який маскується співмножником Y^K. Для того щоб розшифрувати шифротекст (a, b), обчислюють

$$M = \frac{b}{a^X} \bmod P. \qquad (2.3)$$

Так як $a^X = G^{KX} \bmod P$ (що слідує з (2.2)), то вираз (2.3) набуває вигляду $\frac{b}{a^X} = \frac{Y^K M}{G^{KX}} \bmod P$, а з урахуванням (2.1) $\frac{b}{a^X} = \frac{G^{KX} M}{G^{KX}} \bmod P = M(\bmod P)$, тобто співвідношення (2.3) справедливо.

Нехай P=7, G=2, X=3, M=5 (G<P, X<P). У ролі K оберемо число виходячи з умов $(1 < K < P - 1)$, $(K, P - 1) = 1$.

Єдино можливим значенням, що задовольняє ці умови, є K=5.

Обчислимо пару чисел (a, b), попередньо визначивши

$$Y = G^X(\bmod P) = 2^3(\bmod 7) = 8(\bmod 7) = 1,$$
$$a = G^K(\bmod P) = 2^5(\bmod 7) = 32(\bmod 7) = 4,$$
$$b = Y^K M(\bmod P) = 1^5 5(\bmod 7) = 5,$$

Таким чином, шифротекст (a, b) = (4, 5).

Виконаємо розшифрування цього шифротексту, використовуючи секретний ключ X = 3.

Маємо: $M = b/a^X \bmod P = 5/4^3(\bmod 7)$. Цей вираз також можна подати у вигляді $4^3 M = 5(\bmod 7)$, оскільки операція ділення в кінцевому полі еквівалентна операції визначення оберненого елемента. Для його розв'язання спочатку знайдемо розв'язання рівняння $64y = 1(\bmod 7)$, тобто $y = 64^{-1}(\bmod 7)$, а потім обчислимо $M = 5y(\bmod 7)$. Розв'язання рівняння $64y = 1(\bmod 7)$ можна здійснити, використовуючи або розширений алгоритм Евкліда (метод ланцюгових дробів Евкліда), або метод, заснований на використанні функції Ейлера $\varphi(P)$ (див. приклад завдання 1).

В останньому випадку $y = a^{-1}(\bmod P) = a^{\varphi(P)-1}(\bmod P)$. Так як P = 7 – просте число, то $y = 64^{\varphi(7)-1}(\bmod 7) = 64^{6-1}(\bmod 7) = 64^5(\bmod 7)$.

Оскільки модулярна арифметика задовольняє властивості комутативності, то можна записати

$$y = 64^5(\text{mod}7)=[64^2(\text{mod}7)\cdot 64^2\text{mod}7)]\text{mod}7=$$
$$= [(4096\ \text{mod}7)Ч(262144\text{mod}7)]\text{mod}7=$$
$$= [(1\text{mod}7)(1\text{mod}7)]\text{mod}7 = 1\text{mod}7 = 1,$$

тобто $y = 1$. Тоді $M = 1\cdot 5(\text{mod}7) = 5$, що відповідає заданому значенню.

Таблиця 2.2 Варіанти вихідних даних

Номер варіанта	P	G	X	Номер варіанта	P	G	X
1	37	2	13	12	47	5	11
2	43	4	19	13	43	6	19
3	47	3	7	14	47	7	7
4	37	4	5	15	37	4	19
5	43	2	21	16	47	5	21
6	47	3	7	17	43	2	13
7	43	3	11	18	47	4	19
8	37	2	17	19	37	2	7
9	47	3	13	20	43	3	11
10	37	5	13	21	47	4	13

Література [7, с. 334 – 344; 8, с. 339 – 346; 2, с. 28 – 43; 1, с. 39 – 51].

Контрольні питання

1 Методи, способи і засоби добування інформації з обмеженим доступом (ІзОД).

2 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах.

3 Який загальний порядок категорування об'єктів?

4 Основний зміст робіт з категорування об'єктів.

5 Порядок контролю документації на об'єкт, що атестується.

6 Який порядок призначення комісії з категорування?

7 Представники яких спеціальностей повинні призначатися до складу комісії з категорування?

8 Які дані потрібні для використання програми шифрування за допомогою першого алгоритму?

9 Які дані потрібні для використання програми шифрування за допомогою другого алгоритму?

10 Які дані потрібні для використання програми шифрування за допомогою третього алгоритму?

11 Які дані потрібні для використання програми шифрування за допомогою четвертого алгоритму?

12 Які параметри шифротексту допомагають виявити, який з алгоритмів дешифрування використовувати?

3 РОЗРАХУНОК ПАРАМЕТРІВ АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ RSA І ЕЛЬ-ГАМАЛЯ

3.1 Теоретичні відомості до лабораторної роботи

Ідея алгоритму цифрового підпису (ЦП) Ель-Гамаля ґрунтується на тому, що для обґрунтування практичної неможливості фальсифікації ЦП використовується трудомістка обчислювальна задача знаходження дискретного логарифму в кінцевому полі натуральних чисел.

Для генерації пари ключів спочатку обирається велике просте число p (порядку $\sim 10^{308} = 2^{1024}$), а також число g (порядку $\sim 10^{154} = = 2^{512}$), що є твірним елементом поля Галуа GF(p), таке, що $g < p$. Крім того, відправник документа вибирає випадкове ціле число x ($1 < x < p - 1$), що виступає у ролі секретного ключа, тобто $X = K_c$, після чого вираховує відкритий ключ

$$K_o = g^{Kc}(\mathrm{mod} p), \qquad (3.1)$$

який використовується для перевірки цифрового підпису та передається всім потенційним одержувачам повідомлення.

Для того щоб підписати повідомлення M, спочатку відправник хешує його за допомогою хеш-функції $h(\cdot)$ в ціле

число m, тобто m = h(M) (1 < m < p – 1), а потім генерує випадкове ціле число R, (1 < R < p – 1), таке, що (R, (p-1)) = 1 (тобто числа R і (p-1) є взаємнопростими).

Після цього відправник обчислює ціле число a:

$$a = g^R (\mathrm{mod}\ p) \qquad (3.2)$$

і, застосовуючи, наприклад, розширений алгоритм Евкліда (метод ланцюгових дробів Евкліда), обчислює за допомогою секретного ключа K_c ціле число b з рівняння

$$m = K_c \cdot a + R \cdot b (\mathrm{mod}(p-1)), \qquad (3.3)$$

тобто $b = R^{-1}(m - K_c a)(\mathrm{mod}(p-1))$.

Пара чисел (a, b) утворює цифровий підпис = (a, b), що проставляється під документом M. Трійка чисел (M, a, b) пересилається адресатові, в той час як пара чисел (K_c, R) тримається в секреті. Після прийняття підписаного повідомлення (M, a, b) одержувач перевіряє відповідність підпису C документу M. Для цього спочатку хеширується документ M, тобто визначається m = h(M), а потім перевіряється справедливість співвідношення

$$K_o^a a^b (\mathrm{mod} p) = g^m (\mathrm{mod} p)\ , \qquad (3.4)$$

або з урахуванням (3.1) і (3.2),

$$(g^{Kc})^{gR}(\mathrm{mod} p)\, g^{Rb}(\mathrm{mod} p) = g^m (\mathrm{mod} p)\,. \qquad (3.5)$$

Справедливість рівностей (3.4), (3.5) також підтверджується виконанням умови (3.3) відповідно до такої властивості: якщо $a^x = a^y (\mathrm{mod}\ N)$, то $x = y (\mathrm{mod}\ N - 1)$. У разі виконання рівності (3.4) одержувач визнає повідомлення M справжнім.

Необхідно зазначити, що рівність (3.4) буде виконуватися тоді і тільки тоді, коли підпис під документом отриманий за допомогою саме того секретного ключа, з якого був отриманий відкритий ключ. Це є підставою для твердження, що відправником цього повідомлення був володар саме цього

секретного ключа, не розкриваючи при цьому сам ключ, і що відправник підписав саме цей конкретний документ. Необхідною вимогою при формуванні цифрового підпису за алгоритмом Ель-Гамаля є генерація випадковим чином значення R при постановленні цифрового підпису під кожен документ. Ця вимога обумовлена можливістю зловмисника розкрити секретний ключ K_C, якщо йому вдалося розкрити значення R, повторно використане для постановлення цифрового підпису.

Таким чином, схема Ель-Гамаля є характерним прикладом підходу, що допускає пересилку документа у відкритій формі (неконфіденційного) разом з цифровим підписом (a, b), а процедура встановлення автентичності документа полягає в перевірці відповідності цифрового підпису повідомленням.

Порівняно зі схемою цифрового підпису RSA головна перевага схеми Ель-Гамаля полягає в тому, що при однаковому рівні криптостійкості цілі числа, які беруть участь в обчисленнях, мають запис на 25% коротше, що зменшує складність обчислень майже в два рази і дозволяє помітно скоротити обсяг використовуваної пам'яті. Проте в схемі Ель-Гамаля довжина цифрового підпису, що виходить, в 1,5 рази більше, ніж у схемі RSA, що в свою чергу збільшує час її обчислення.

Криптостійкість схеми ЦП Ель-Гамаля визначається трудомісткістю підробки ЦП зловмисником, оцінюється виходячи з наступних міркувань.

У розпорядженні зловмисника є: алгоритм обчислення хеш-функції $h(\cdot)$, саме повідомлення M, а також числа a, b і відкритий ключ K_0.

Для того щоб змінити і перепідписати змінене повідомлення, зловмисникові необхідно визначити секретний ключ Kc за допомогою розв'язання задачі дискретного логарифмування із співвідношення (3.1) або на підставі порівняння (3.5), де визначення Kc здійснюється опосередковано, тобто через попереднє визначення R з рівняння (3.2).

Слід також зазначити, що при обчисленні R шляхом піднесення g до степеня, зведення за модулем p та порівняння результату з відомим значенням a, можна обмежити безліч чисел, що підбираються – кандидатів на значення R, на основі умови $(R, (p-1)) = 1$.

3.2 Постановка задачі лабораторної роботи

Задача 3.2.1 Виступаючи (по черзі) в ролі учасника інформаційного обміну – відправника і одержувача документа M, хеш-значення якого дорівнює m, при заданих значеннях p, g, K_C (значення R вибрати самостійно), сформувати цифровий підпис за схемою Ель-Гамаля для документа M і здійснити перевірку цифрового підпису, якщо обчислене значення хеш-функції h(M) дорівнює m. Варіанти вихідних даних наведені в таблиці 3.1 (значення m = 5 для всіх номерів варіантів).

Розв'язання типового прикладу до задачі 3.2.1.

Нехай p = 11, g = 2, K_C = 8. Тоді з урахуванням (3.1) $K_o = g^{Kc}(\text{mod}p) = 2^8 \text{mod} 11 = = 256 \text{mod} 11 = 3$. Нехай m = 5. У ролі R обираємо R = 9. Умова (9, 10) = 1 виконується. Згідно з (3.2) знаходимо $a = 2^9 \text{mod} 11 = 512 \text{mod} 11 = 6$. Число b – другий компонент цифрового підпису – визначимо відповідно до (3.3), тобто $5 = (8 \cdot 6 + 9b)(\text{mod}10) = 48 + 9b(\text{mod}10)$, або $9b(\text{mod}10) = = 5 - 48 = -43$, що також можна записати у вигляді $9b = = -43(\text{mod}10)$. Для визначення b спочатку розв'яжемо рівняння $9y = 1(\text{mod}10)$, використовуючи метод ланцюгових дробів Евкліда.

$$10 = 9 \cdot 1 + 1,\ q_0 = 1,\ r_0 = 1;\ n_0 = q_0 = 1;$$
$$9 = 9 \cdot 1 + 0,\ q_1 = 9,\ r_1 = 0.$$

Тоді $y = (-1)^1 n_0 = -1$, отже, $b = -43 \cdot y(\text{mod}10) = 43(\text{mod}10) = 3$.

Рівняння $9y = 1(\text{mod}10)$ також може бути розв'язано на основі співвідношення $K_d = K_e^{\varphi(n)-1}(\text{mod}\, n)$ за допомогою попереднього обчислення значення функції Ейлера.

Таким чином, цифровий підпис є пара (a, b) = (3, 3).

Перевірка підпису: використовуючи відкритий ключ K_O=3, обчислюємо $K_0^a a^b(\text{mod}p) = 3^6 \cdot 6^3(\text{mod}11) = 10$ і $g^m(\text{mod}\ p) = = 2^5(\text{mod}11) = 10$. Отже, згідно з (3.4) прийняте повідомлення вважається справжнім.

Задача 3.2.2. Виступаючи (по черзі) в ролі учасника інформаційного обміну – відправника і одержувача документа M, хеш-значення якого дорівнює m, при заданих значеннях p, q сформувати цифровий підпис за схемою RSA для документа M і здійснити перевірку цифрового підпису, якщо обчислене

значення хеш-функції h(M) дорівнює m. Варіанти вихідних даних наведені в таблиці 3.2 (значення m = 5 для всіх номерів варіантів). Вибір ключів здійснити самостійно, виходячи з відповідних вимог до них (див. розділ 5 цих методичних вказівок).

Розв'язання типового прикладу до задачі 3.2.2.

За варіантами вихідних даних, наведених у таблицях 3.1 та 3.2, кожний студент виконує індивідуальне завдання.

Таблиця 3.1 – Варіанти вихідних даних

Номер варіанта	p	g	K_c	Номер варіанта	p	g	K_c
1	13	6	5	14	17	5	4
2	17	3	6	15	17	3	5
3	13	2	7	16	19	3	4
4	19	2	5	17	23	5	3
5	23	5	4	18	13	2	4
6	17	6	3	19	19	2	5
7	19	3	5	20	13	5	5
8	13	7	4	21	17	5	6
9	19	2	4	22	19	4	2
10	23	5	2	23	23	5	4
11	17	5	5	24	13	7	3
12	19	2	6	25	19	3	6
13	13	2	4	26	17	3	5

Таблиця 3.2 – Варіанти вихідних даних

Номер варіанта	p	q	Номер варіанта	p	q
1	11	43	14	19	37
2	13	49	15	41	13
3	53	23	16	29	43
4	31	19	17	19	37
5	47	13	18	41	13
6	19	43	19	29	43
7	37	17	20	31	53
8	13	19	21	29	41

Продовження таблиці 3.2

Номер варіанта	p	q	Номер варіанта	p	q
9	29	43	22	41	17
10	41	23	23	17	49
11	19	29	24	41	17
12	11	53	25	13	53
13	23	31	26	23	43

Література [7, с. 334 – 344; 8 с. 339 – 346; 2, с. 28 – 43; 1, с. 39 – 51].

Контрольні питання

1 Які канали витоку інформації можливі при роботі засобів Інтернет-МЕМ (ЕОТ) і заходів для блокування технічних каналів витоку інформації з використанням пасивних засобів (ТСПІ)?

2 Методи, способи і засоби добування ІзОД.

3 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах?

4 Який загальний порядок обстеження систем електроживлення і заземлення?

5 Основні вимоги до систем електроживлення та заземлення об'єктів інформаційної діяльності.

6 Який порядок вимірювання опору заземлення?

7 Чи задовольняє норми опору заземлення об'єкта, якщо воно виміряно в умовах Р = 730 мм; т = + 30 °С; Н = 90 % і становить: 1,5 Ом; 2,3 Ом; 3,6 Ом; 4,1 Ом?

4 ЗАХИСТ МЕРЕЖІ WI-FI

4.1 Теоретичні відомості до лабораторної роботи

Стандарт Wi-Fi розроблений на основі IEEE 802.11 (Institute of Electrical and Electronics Engineers), використовується для широкосмугових бездротових мереж зв'язку. Спочатку технологія Wi-Fi була орієнтована на організацію точок швидкого доступу в Інтернет (hotspot) для мобільних користувачів. Переваги бездротового доступу очевидні, а технологія Wi-Fi спочатку стала стандартом, якого дотримуються виробники мобільних пристроїв. Поступово мережі Wi-Fi стали використовувати малі і великі офіси для організації внутрішніх мереж і підмереж, а оператори створювати власну інфраструктуру надання бездротового доступу в Інтернет на основі технології Wi-Fi. Таким чином, в даний час мережі Wi-Fi поширені повсюдно і часто мають зони покриття цілих районів міста.

З точки зору безпеки, слід враховувати загрози, властиві провідним мережам, і середовище передачі сигналу. У бездротових мережах отримати доступ до інформації, що передається, набагато простіше, ніж в провідних мережах, так само, як і вплинути на канал передачі даних. Досить помістити відповідний пристрій в зоні дії мережі.

Загрози інформаційній безпеці, що виникають при використанні Wi-Fi мереж, можна умовно поділити на два класи:

- прямі – загрози інформаційній безпеці, що виникають при передачі інформації по бездротовому інтерфейсу IEEE 802.11;
- непрямі – загрози, пов'язані з наявністю на об'єкті і поруч з об'єктом великої кількості Wi-Fi-мереж.

При прямій загрозі радіоканал передачі даних, який використовується в Wi-Fi, потенційно схильний до втручання з метою порушення конфіденційності, цілісності та доступності інформації. У Wi-Fi передбачені як аутентифікація, так і шифрування, але ці елементи захисту мають свої вади.

Шифрування значно знижує швидкість передачі даних, і найчастіше воно свідомо відключається адміністратором для оптимізації трафіку. Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований за рахунок вад в

алгоритмі розподілу ключів RC4. Це дещо пригальмувало розвиток Wi-Fi ринку і викликало створення інститутом IEEE робочої групи 802.11i для розроблення нового стандарту, що враховує вади WEP, що забезпечує 128-бітове AES шифрування і аутентифікацію для захисту даних. Wi-Fi Alliance в 2003 р. представив свій власний проміжний варіант цього стандарту – WPA (Wi-Fi Protected Access). WPA використовує протокол цілісності часових ключів TKIP (Temporal Key Integrity Protocol). Також в ньому використовується метод контрольної суми MIC (Message Integrity Code), яка дозволяє перевіряти цілісність пакетів. У 2004 р. Wi-Fi Alliance випустили стандарт WPA2, який являє собою поліпшений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування: TKIP і AES. WPA2 забезпечує більш високий рівень захисту мережі, так як TKIP дозволяє створювати ключі довжиною до 128 біт, а AES – до 256 біт.

Загроза блокування інформації в каналі Wi-Fi практично залишена без уваги при розробленні технології. Само по собі блокування каналу не є небезпечним, так як зазвичай Wi-Fi мережі є допоміжними, проте блокування може являти собою лише підготовчий етап для атаки "людина посередині", коли між клієнтом і точкою доступу з'являється третій пристрій, який перенаправляє трафік між ними через себе. Таке втручання дозволяє видаляти, спотворювати або нав'язувати неправдиву інформацію.

Чужинцями (RogueDevices, Rogues) називаються пристрої, які дають змогу несанкціонованого доступу до корпоративної мережі, зазвичай в обхід механізмів захисту, визначених політикою безпеки. Заборона на використання пристроїв бездротового зв'язку не захистить від бездротових атак, якщо в мережі, навмисне чи ні, з'явиться чужинець. У ролі чужинця може виступати все, що має дротові і бездротові інтерфейси: точки доступу (включаючи програмні), сканери, проектори, ноутбуки з обома ввімкненими інтерфейсами.

Некоректно сконфігуровані пристрої, пристрої зі слабкими і недостатньо довгими ключами шифрування, які використовують уразливі методи аутентифікації – саме такі пристрої піддаються атакам у першу чергу. Відповідно до звітів аналітиків, більша частина успішних зламів відбувається якраз через неправильні

налаштування точок доступу і програмного забезпечення клієнта. Досить підключити неправильно налаштовану точку доступу до мережі для зламу останньої. Налаштування "за замовчуванням" не включають шифрування і аутентифікацію або використовують ключі, прописані в керівництві і тому всім відомі. Малоймовірно, що користувачі досить серйозно будуть стурбовані безпечною конфігурацією пристроїв. Саме такі привнесені точки доступу і створюють основні загрози захищеним мережам.

Некоректно налаштовані пристрої користувачів – загроза небезпечніша, ніж некоректно сконфігуровані точки доступу. Це пристрої користувачів і вони не конфігуруються спеціально з метою безпеки внутрішньої мережі підприємства. До того ж вони знаходяться як за периметром контрольованої зони, так і всередині нього, дозволяючи зловмисникові проводити всілякі атаки, а саме поширювати шкідливе програмне забезпечення або просто забезпечуючи зручну точку входу.

Про захищеності WEP вже не йдеться. Інтернет повний спеціального і зручного у використанні програмного забезпечення для зламу цього стандарту, яке збирає статистику трафіку до тих пір, поки її не стане достатньо для відновлення ключа шифрування. Стандарти WPA і WPA2 також мають ряд вад різного ступеня небезпеки, що дозволяють їх злам. Поки що немає інформації про успішні атаки на WPA2-Enterprise (802.1x).

Якість роботи Wi-Fi мережі як радіоефіру залежить від багатьох факторів. Один з них – інтерференція радіосигналів, яка може значно знизити пропускну здатність будь-якого пристрою, що випромінює на тій же частоті сигнал достатньої потужності. Це можуть бути як сусідні точки доступу, так і мікрохвильовки. Цю особливість можуть також використовувати зловмисники як атаки відмови в обслуговуванні або для підготовки атаки "людина посередині", заглушаючи легітимні точки доступу і залишаючи свою з таким же SSID.

4.2 Способи захисту бездротової мережі Wi-Fi

4.2.1 Модифікація SSID та шифрування мережного трафіку

Пристрої, які координують роботу бездротових мереж, передають в ідентифікатор бездротової мережі (Service Set Identifier – SSID). За умовчанням як SSID мережі використовується найменування мережного пристрою. Знаючи вид використовуваного обладнання, зловмисник може скористатися відомими вадами даного пристрою. Для запобігання цьому необхідно змінити SSID на нейтральне значення.

При забороні на трансляцію SSID для підключення до бездротової мережі потрібно вказати її найменування вручну. При установленні імені мережного пристрою, який використовується за умовчанням, можна створити зловмисникові додаткові проблеми. Розглянемо, як підключитися до прихованої точки доступу.

Крім підключення до ресурсів мережі, зловмисник також має можливість перехоплення трафіку, що генерується в процесі її роботи. Сучасні мережні пристрої підтримують широкий спектр можливостей шифрування, заснованих на технології WPA (Wi-Fi Protected Access) і її модифікаціях (WPA2, WPA-PSK і т. д.). Використання технології WPA не тільки дозволяє забезпечити шифрування мережного трафіку в бездротовій мережі, але і запобігти несанкціонованому підключенню до неї: для підключення до бездротової мережі, захищеної з використанням WPA, клієнт повинен вказати ключ доступу, встановлений адміністратором. В рамках мережного пристрою є можливість визначити список фізичних адрес (MAC-адрес), які матимуть доступ до бездротової мережі (або навпаки – яким буде заборонений доступ до бездротової мережі). Визначивши фільтр за MAC-адресами, з'являється можливість обмежити доступ до бездротової мережі навіть без використання алгоритмів шифрування. Використовуйте WPA2-PSK-CCMP з паролем від 12 символів a-z (2000+ років перебору на ATI-кластері).

4.2.2 Захист від зміни настроювань бездротової мережі та фільтрація пристроїв за MAC-адресою

Для установлення настроювань, що визначають порядок функціонування бездротової мережі, будь-який пристрій, яке координує її роботу, надає адміністратору консоль управління. Для входу в консоль управління використовується ім'я користувача і пароль. Спочатку як ім'я користувача і пароль використовуються деякі стандартні значення, які можуть бути відомі в тому числі і зловмисникові. Отримавши доступ до консолі управління, зловмисник може змінити настроювання роботи бездротової мережі довільним чином.

Увімкнення цієї функції дозволить підключати до роутера тільки ті пристрої, MAC адреси яких прописані в настройках і дозволені. Це дуже ефективний захист, але якщо ви часто підключаєте нові пристрої, то буде не дуже зручно кожен раз заходити в настроювання роутера і прописувати MAC адреси пристрою. Для початку потрібно дізнатися MAC адреси пристроїв, яким ви хочете дозволити підключення до Wi-Fi мережі. Їх можна подивитися в настройках, докладніше читайте тут. Якщо це телефон або планшет, то можна подивитися адресу в налаштуваннях, в розділі «Про телефон». А якщо він вже увімкнений до роутера, то всю необхідну інформацію можна дізнатися на вкладці «DHCP» – «DHCP Clients List».

Для відключення служби WPS (QSS) переходимо на вкладку «QSS», у вас вона може називатися ще «WPS» або якось схоже. І натискаємо кнопку «Disabled QSS». QSS, або WPS – це технологія, яка дозволяє напівавтоматично створювати бездротове Wi-Fi з'єднання між роутером і пристроєм, який потрібно підключити до мережі.

Розшифровується так: WPS – Wi-Fi Protected Setup; QSS – Quick Security Setup. Досить перебрати 10000 комбінацій PIN і WPS (QSS) буде зламана. Дану функцію необхідно обов'язково відключити.

Література [7, с. 334 – 344; 8 с. 339 – 346; 2, с. 28 – 43; 1, с. 39 – 51].

Контрольні питання

1 Які канали витоку інформації можливі при роботі ТСПІ?

2 Методи, способи і засоби добування ІзОД.

3 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах.

4 Порядок перевірки стану і оцінки ефективності застосування технічних засобів захисту ІзОД від витоку за рахунок ПЕМВН ПЕОМ.

5 Порядок перевірки стану і оцінки ефективності застосування засобів захисту інформації телекомунікаційних систем.

6 Як змінюються розміри КЗ при застосуванні засобів ТЗІ?

7 Які акти і протоколи відпрацьовуються комісією з категорування при оцінці ефективності застосування технічних засобів захисту ІзОД?

8 Основні критерії прийняття рішення про відповідність заходів захисту ІзОД на об'єкті вимог керівних документів з ТЗІ.

5 ПОБУДОВА ШИФРОТВІРНИХ ПРИСТРОЇВ СИМЕТРИЧНИХ ПОТОКОВИХ СИСТЕМ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ І ЇХ КРИПТОАНАЛІЗ

5.1 Постановка завдання лабораторної роботи

Побудувати потокову криптосистему за принципом комбінування трьох лінійних регістрів зсуву зі зворотнім зв'язком (РЗЗЗ) різної розрядності з довільним правилом введення нелінійності для формування 10 символів двійкової псевдовипадкової послідовності (ПВП). Кожен з використовуваних РЗЗЗ повинен генерувати двійкову ПВП з максимальним періодом, тобто бути асоційованим з примітивним поліномом (многочленом), ступінь якого дорівнює розрядності РЗЗЗ.

Вибір примітивних поліномів заданого ступеня може бути здійснено, виходячи з визначення примітивності полінома.

Примітивним поліномом f(x) степеня k називається незвідний поліном, для якого виконується умова

$$\forall\ j = 1,\ldots,2^k - 1 : x^j + 1 \neq 0 (\mathrm{mod}\ f(x)), \qquad (5.1)$$

тобто повинен існувати не рівний нулю залишок від ділення хоча б одного з поліномів вигляду $x^j + 1$ (де $j = 1,\ldots,2^k - 1$) на поліном f(x).

При цьому критерієм незвідности многочлена f(x) степеня k є подільність на нього без залишку многочлена $x^n + 1$, де $n = 2^k - 1$, тобто повинна виконуватися умова

$$x^n + 1 = 0 (\mathrm{mod}\ f(x)). \qquad (5.2)$$

Слід зазначити, що не всякий многочлен, який не зводиться, є в той же час примітивним. Наприклад, многочлен $f(x) = x^4+x^3+x^2+x+1$ є незвідним (тобто ділить многочлен $p(x)= x^{15} + 1$ без залишку), але не є примітивним, оскільки має місце співвідношення $x^5 + 1 = (x^4+x^3+x^2+x+1)(x+1)$, тобто залишок від ділення $x^5+ 1$ на f(x) дорівнює 0 (у даному випадку $j = 5$). Тому на основі цього полінома можна сформувати лінійну рекурентну двійкову послідовність з періодом $2^4 - 1 = 15$ символів.

Для перевірки умов (5.1), (5.2) можна скористатися, наприклад, стандартними функціями програмного середовища MATLAB. Для цього необхідно в командному вікні MATLAB (Command Window) в режимі прямих обчислень задати відповідні поліноми шляхом перерахування їх коефіцієнтів перед змінною x в порядку спадання ступенів x, а потім використовувати стандартну функцію [q,r] = deconv(p,f), де p,f відповідно поліном-ділене і поліном-дільник, а q,r – відповідно частка і залишок від ділення p f. Наприклад, для згаданого вище випадку ділення полінома $p(x) = x^5 + 1$ на поліном $f(x) = (x^4+x^3+x^2+x+1)$, програма роботи в середовищі MATLAB і результат роботи цієї програми будуть виглядати таким чином:

```
>> p = [1 0 0 0 0 1];
>> f = [1 1 1 1 1];
```

```
>> [q,r] = deconv(p,f)
q = 1    -1
r = 0     0     0     0     0     2
```

Як видно з запису, часткою від розподілу p(x) на f(x) буде поліном q(x) = x + 1, а залишок поліному r(x) = 0.

Слід також взяти до уваги, що двійковий поліном, який не зводиться (а значить, і примітивний), ступінь свободи k в ролі коефіцієнта при нульовому x обов'язково має одиницю. Цей факт дозволяє істотно звузити безліч поліномів заданого ступеня k-претендентів на володіння властивістю незвідності (і, відповідно, примітивності).

При цьому слід мати на увазі, що якщо поліном f(x) ступіня k є примітивним, то примітивним також буде і поліном, додатковий до цього, а саме, поліном $p(x) = x^k \cdot f(1/x)$. Наприклад, як випливає з таблиці 16.2 зазначеного джерела, поліном $f(x) = x^{17}+x^3+$ є примітивним, тому примітивним також буде додатковий до даного поліном.

$p(x) = x^{17}+x^{14}+1$, оскільки $p(x) = x^{17} \cdot f(1/x) = x^{17} \cdot (x^{-17}+x^{-3}+1) = x^{17}+x^{14}+1$.

5.2 Алгоритм розв'язання завдання 2 лабораторної роботи

Використовуючи алгоритм Берлекемпа-Мессі, побудувати РЗЗЗ, на основі якого сформована псевдовипадкова послідовність (ПВП) символів (гамма-шифру), якщо відомі перші її 2k = 8 членів (таблиця 5.2). Перевірити правильність отриманого результату (побудованого регістра) шляхом формування на ньому перших восьми елементів ПСП при заданому початковому стані регістра і зіставленні отриманого ПСП з наведеною у вихідних даних послідовністю.

Вказівка до розв'язання завдання

Сутність алгоритму Берлекемпа-Мессі зводиться до визначення структури РЗЗЗ (типу наявних у ньому зворотних зв'язків), якщо передбачувана розрядність регістра дорівнює k.

Так, якщо $h_0, h_1,\ldots,h_n$ – символи (біти) однорідної ЛРП, асоційованої з мінімальним многочленом степеня k, то шуканий

мінімальний многочлен m(x) дорівнює многочлену, подвійному до многочлена $g_{2K}(x)$ степеня r, сформованого відповідно до нижче поданих послідовностей кроків j при j = 2k. Тут

$$r = \left\lfloor k + 0{,}5 - \frac{m_{2K}}{2} \right\rfloor, \tag{5.3}$$

де m_{2K} – деяке ціле число, отримане на кроці j = 2k;

|y| – найбільше ціле число, яке не перевищує y.

Відповідно до даного алгоритму для j = 0,…,2k визначаються многочлени $g_j(x)$, $I_j(x)$ над полем GF(q) (у нашому випадку q = 2), цілі числа m_j і елементи $b_j \in GF(q)$ наступним чином.

Для j = 0 записують

$$g_0 l(x) = 1,\ I_0(x) = x,\ m_0 = 0, \tag{5.4}$$

після чого рекурсивно обчислюємо значення, де b_j – коефіцієнт при x^j у множенні вигляду $g_j(x)G(x)$,

$$G(x) = \sum_{i=0}^{2k-1} h_i x^i \quad - \tag{5.5}$$

многочлен над полем GF(q), асоційований з першими 2k членами ЛРП;

$$g_{j+1}(x) = g_j(x) - b_j I_j(x), \tag{5.6}$$

$$I_{j+1}(x) = \begin{cases} b_j^{-1} x g_j(x), & \text{если } b_j \neq 0,\ m_j \geq 0; \\ x I_j(x) & \text{в іншому випадку,} \end{cases} \tag{5.7}$$

$$m_{j+1} = \begin{cases} -m_j, & \text{если } b_j \neq 0, m_j \geq 0; \\ m_j + 1 & \text{в іншому випадку.} \end{cases} \tag{5.8}$$

У формулі (5.8) b_j^{-1} – елемент, обернений елементу b_j ($b_j^{-1} \in GF(2)$). В даному випадку $b_j^{-1} = 1$ як при $b_j = 1$, так і $b_j = 0$.

5.3 Методика вирішення типового прикладу

Нехай перші вісім членів лінійної рекурентної послідовності, що відповідає шуканій многочленом, мають вигляд: 1, 1, 0, 0, 1, 0, 1, 1. G(x) = 1+x+x4+ x6+ x7.

Тоді, згідно з формулою (5.5), отримаємо G(x) = 1+x+x4+ x6+ x7. Результати подальших розрахунків, згідно з формулами (5.6) - (5.8), помістимо у таблиці 5.1.

Таблиця 5.1 – Результати розрахунків

j	$g_j(x)$	$I_j(x)$	m_j	b_j
0	1	X	0	1
1	$1 + x$	X	0	0
2	$1 + x$	x^2	1	1
3	$1 + x + x^2$	$x + x^2$	-1	1
4	1	$x^2 + x^3$	0	1
5	$1 + x^2 + x^3$	X	0	0
6	$1 + x^2 + x^3$	x^2	1	0
7	$1 + x^2 + x^3$	x^2	2	0
8	$1 + x^2 + x^3$		3	

Так, на кроці j = 0 з урахуванням (5.5) знаходимо $g_0(x)G(x) = 1(1+x+x^4+ +x^6+ x^7)$, звідки $b_0 = 1$ – коефіцієнт при $x^0 = 1$ (значення (5.4) і b_0 заносимо у перший рядок таблиці). Далі на кроці j = 1 маємо: $g_1(x) = g_0(x) - b_0 I_0(x) = 1 – 1 \cdot x = 1 – x = 1+x$ (символ “–” можна замінити на “+”, тобто, з точки зору арифметики, в полі це ролі не відіграє, оскільки важливе значення коефіцієнта ступеня x^j);

$$I_1(x) = b_0^{-1} x g_0(x) = 1 \cdot x \cdot 1 = x;$$

визначимо b_1:

$$g_1(x)G(x) = (1+x)(1+x+x^4+\ldots) = 1+x+ x^4\ldots\ x+x^2+ x^4\ldots = 1+x+x+\ldots= \\ = 1+x(1+1) = =1+\ldots+ x^2+\ldots,$$

тобто $b_1 = 0$, так як коефіцієнт при x^1 дорівнює 1 + 1 = 0, оскільки складання здійснюється за правилами двійкової арифметики.

На кроці j = 2 отримаємо

$$g_2(x) = g_1(x) – b_1I_1(x) = (1+x) – 0\cdot x^2 = 1+x;$$

$$I_2(x) = xI_1(x);$$

визначимо b_2:

$$g_2(x)G(x) = (1+x)(1+x+x^4+\ldots) = 1+x+ x^4\ldots\ x+x^2+ \ldots,$$

тобто $b_2 = 1$, так як коефіцієнт при x^2 дорівнює 1; $m_2 = m_1+1 = 1$.

Інші значення розрахованих параметрів отримують аналогічно. Таким чином, видно, що шуканий РЗЗЗ асоційований з примітивним поліномом, додатковим по відношенню до поліному $f(x) = x^3+ x^2 + 1$. Відповідно до поняття додатковості додатковим до отриманого в результаті розрахунків поліному буде поліном $f(x) = x^3 + x + 1$, а, отже, структура самого регістру має вигляд, як на рисунку 5.1.

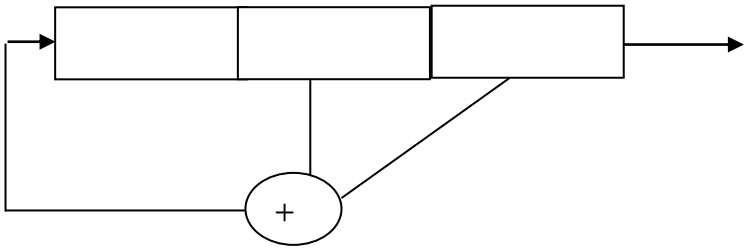

Рисунок 5.1 – Структура регістру

Перевіримо коректність отриманого результату шляхом формування на даному регістрі символів ПСП для початкового стану регістра 0 1 1 (так як відповідно до вихідних даних першими трьома символами ПСП є 1 1 0). В результаті отримаємо наступні вісім символів ПСП: 1 1 0 0 1 0 1 1, що

збігається з вихідними даними, а, значить, свідчить на користь правильності виконаного завдання.

Слід зазначити, що з таблиці 5.1 видно, що для визначення структури даного регістра достатньо знати шість елементів вихідної послідовності.

Таблиця 5.2 – Варіанти вихідних даних

Номер варіанта	Значення символів ЛРП	Номер варіанта	Значення символів ЛРП
1	10010011	12	10011110
2	11101011	13	10110010
3	00010011	14	10100101
4	11101011	15	10001001
5	10001100	16	00011110
6	11010110	17	00101001
7	11110001	18	00110101
8	10111101	19	10101100
9	01001101	20	01111010
10	11011110	21	10101111
11	10110001	22	11110111

Література [1, с. 334 – 344; 2 с. 339 – 346; 3, с. 28 – 43; 4, с. 39 – 51].

Контрольні питання

1 Який захисний контур називається багаторівневим захистом?

2 Покажіть модель багаторівневого захисту та стисло опишіть її особливості.

3 Наведіть схему моделі обчислювальної системи з безпечною обробкою інформації.

4 Стисло опишіть зовнішні системи охорони.

5 Традиційні системи охорони.

6 Ультразвукові системи та системи переривання променя.

7 Телевізійні, радіолокаційні, мікрохвильові та інші системи охорони.

8 Засоби контролю та керування доступом (коди паролів).

9 Які канали витоку інформації можливі при роботі ТСПІ?

10 Методи, способи і засоби добування ІзОД.

11 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах.

12 З якою метою проводиться категорування об'єктів інформаційної діяльності?

13 Правила і порядок оцінки оптичної захищеності об'єкта інформаційної діяльності.

14 Правила і порядок оцінки акустичної захищеності об'єкта інформаційної діяльності.

15 Які акти і протоколи відпрацьовуються комісією з категорування об'єктів інформаційної діяльності?

16 Основні критерії прийняття рішення про відповідність заходів захисту ІзОД на об'єкті вимог керівних документів з ТЗІ.

6 РОЗРАХУНОК ПАРАМЕТРІВ ПРОТОКОЛУ АУТЕНТИФІКАЦІЇ З НУЛЬОВОЮ ПЕРЕДАЧЕЮ ЗНАНЬ ФЕЙГЕ – ФІАТА – ШАМІРА

6.1 Теоретичні відомості до лабораторної роботи

Спочатку вибирають випадкове значення модуля N, який є добутком двох великих простих чисел. Даний модуль повинен мати довжину не менше 1024 біт. Це значення надається групі користувачів, яким належить доводити свою автентичність. В процесі аутентифікації беруть участь дві сторони. Сторона А, яка доводить свою автентичність та має рішення $X^2 = V(\mathrm{mod}\ N)$, та протилежна V за модулем n сторона, тобто$V \cdot V^{-1} = 1(\mathrm{mod}\ N)$.

Нагадаємо, що критерієм існування у деякого цілого числа, а оберненого йому за модулем числа n, є виконання умови (a, N) = 1.

Вибране значення V є відкритим ключем для А. Потім обчислюють найменше значення S, для якого

$$(S)^2=V^{-1}\ (\mathrm{mod}\ n),\ \text{або}\ S = \mathrm{sqrt}(V^{-1}))(\mathrm{mod}\ N). \qquad (6.1)$$

Дане значення S є секретним ключем для А. Після виконання цих підготовчих заходів дії сторін А та В такі:

а) сторона А вибирає деяке випадкове число *r*, (*r* < *N)* і обчислює

$$x = r^2 \pmod N, \qquad (6.2)$$

а потім відправляє отримане значення x стороні *B;*

б) сторона *B* посилає *A* випадковий біт *b;*

в) якщо *b = 0*, тоді *A* відправляє *r* стороні *B,* якщо *b = 1*, то *A* відправляє стороні *B*

$$y = rs(\mathrm{mod} N); \qquad (6.3)$$

г) якщо *b* = 0, сторона *B* перевіряє, що $x = r^2 \pmod N$, щоб упевнитися, що *A* знає sqrt(x);

д) якщо *b* = 1, сторона *B* перевіряє, що $x = y^2 \cdot V \pmod N$, щоб бути упевненою, що *A* знає $\mathrm{sqrt}(V^{-1})$.

Дійсно, з урахуванням (6.1) і (6.3) маємо

$$x = r2s2V(\mathrm{mod} N) = r2V\text{-}1(\mathrm{mod} N) = r2(\mathrm{mod} N),$$

що відповідає (6.2).

Виконані етапи утворюють один цикл протоколу НПЗ, званий акредитацією. Сторони А і В повторюють цей цикл l раз при різних випадкових значеннях r і b до тих пір, поки значення не стане S.

Якщо сторона А не знає значення S, вона, в принципі, може вибрати таке значення r, яке дозволить їй «обдурити» сторону, якщо В відправить їй b = 0. Якщо В відправить А значення b = 1, сторона А також, в принципі, не знаючи S, може вибрати таку r, яка виступала б як rS і дозволила б «обдурити» В. Проте в обох випадках така невідповідність неможлива, оскільки для сторони стало б очевидно, що сторона А при b = 0 і b = 1 використовує різні значення r. Ймовірність того, що А «обдурить» В в одному циклі, дорівнює 0,5, а ймовірність невідповідності в l циклах становить 0,5.

Розглянемо тепер паралельну схему аутентифікації з НПЗ, яка дозволяє збільшити кількість акредитацій, що виконуються за один цикл, і тим самим зменшити тривалість процесу аутентифікації.

Сутність даної схеми полягає в наступному. Після того, як згенеровано число N = pq, де p, q – прості числа, що зберігаються в секреті, формується безліч $M = \{V_i\}$ $(i = 1,\ldots,m)$ квадратичних відрахувань за модулем N шляхом зведення в квадрат за модулем N чисел 1, 2,..., N-1. Потім визначається $M' = \{V_i'\}_{i=1}^{k}$, $M' \subset M$, де для елементів V_i' множини M' виконується умова $(V_i', n) = 1$. При цьому k = (p-1)(q-1)/4. Отриманий рядок взаємно простих чисел, квадратичних відрахувань по модулю, є відкритим ключем сторони A.

Потім обчислюються такі найменші значення S_i, що $S_i = sqrt(V_i'^{-1})(mod n)$, тобто для яких правдиве співвідношення $(S_i)^2 = (V_i'^{-1})(mod n)$. Рядок чисел $S_i\,(i = \overline{1,k})$ при заданому k є секретним ключем сторони A.

Після цього виконуються такі дії (власне протокол):

а) сторона вибирає, як і у разі спрощеного варіанта протоколу аутентифікації з НПЗ, випадкове число r, яке не перевищує N, обчислює $x = r^2 (\mathrm{mod}\ N)$ і відправляє x стороні B;

б) сторона B відправляє A деякий випадковий двійковий рядок з k біт: $b_1, b_2, \ldots, b_k$;

в) сторона A обчислює $y = r \prod_{i=1}^{k} S_i^{b_i} (\mathrm{mod}\ N)$ і отримане значення відправляє стороні B;

г) сторона B перевіряє, що $x = y^2 \prod_{i=1}^{k} (V_i'^{\,b_i}) (\mathrm{mod}\ N)$; сторони повторюють цей протокол стільки раз, поки B не впевниться, що A знає $S_i\,(i = \overline{1,k})$.

При цьому ймовірність обману стороною сторони дорівнює $\left(\frac{1}{2}\right)^{kl}$.

Очевидно, що надійність даної схеми аутентифікації визначається трудомісткістю розв'язання задачі розкладання модуля N на прості множники p і q, оскільки, дізнавшись ці значення, зловмисник має можливість легко обчислити значення функції Ейлера від N, щоб потім також досить легко визначити

секретний ключ виходячи з відкритого, і, володіючи секретним ключем, мати можливість виступати від імені легального користувача.

6.2 Постановка завдання до лабораторної роботи

Розрахувати параметри одного циклу паралельного протоколу аутентифікації з нульовою передачею знань для k = 4 і значень p, q таких, що pq = N, заданих в таблиці варіантів вихідних даних (таблиця 6.2). Значення випадкового числа r вибрати самостійно, а випадкові двійкові рядки, які висилаються, перевіряються (аутентифікуючою) стороною (B), для парних і непарних номерів варіантів дорівнюють відповідно [0110] і [1010]. Визначити ймовірність обману сторони, що аутентифікує, при заданому значенні кількості циклів аутентифікації.

Розв'язання типового прикладу. Нехай N = 35, p = 5, q = 7. Підносячи до квадрата за модулем 35 числа 1, ..., 34, сформуємо множину M квадратичних відрахувань за модулем 35: M = {1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30}, тобто

$x^2 = 1 (\mathrm{mod}\ 35)$ має рішення x = 1, 6, 29, 34;
$x^2 = 4 (\mathrm{mod}\ 35)$ має рішення x = 2,12, 23, 33;
$x^2 = 9 (\mathrm{mod}\ 35)$ має рішення x = 3, 17, 18, 32;
$x^2 = 11 (\mathrm{mod}\ 35)$ має рішення x = 9, 16, 19, 26;
$x^2 = 14 (\mathrm{mod}\ 35)$ має рішення x = 7, 28;
$x^2 = 15 (\mathrm{mod}\ 35)$ має рішення x = 15, 20;
$x^2 = 16 (\mathrm{mod}\ 35)$ має рішення x = 4, 11, 24, 31;
$x^2 = 21 (\mathrm{mod}\ 35)$ має рішення x = 14, 21;
$x^2 = 25 (\mathrm{mod}\ 35)$ має рішення x = 5, 30;
$x^2 = 29 (\mathrm{mod}\ 35)$ має рішення x = 8, 13, 22, 27.
$x^2 = 30 (\mathrm{mod}\ 35)$ має рішення x = 10, 25.

Визначимо множину $M' \subset M$ квадратичних відрахувань, для яких виконується умова (V, N) = 1. Потужність множини M' дорівнює (5 –1)(7 – 1)/4 = 6, тобто $M' = \{1, 4, 9, 11, 16, 29\}$.

Для елементів множини M′ обчислимо обернені величини за модулем 35, а також їх квадратні корені за модулем 35. Отримані результати зведемо в таблиці 6.1.

Таблиця 6.1 – Результати обчислення обернених величин за модулем 35

V_i'	$V_i'^{-1}$	$S = sqrt(V_i'^{-1})$
1	1	1
4	9	3
9	4	2
11	16	4
16	11	9
29	29	8

Наприклад, визначимо обернену величину для V5′ = 16, розв'язавши рівняння 16y = 1(mod35). Рішенням є y = 16φ(35) - - 1(mod35) = 11. Тут φ(35)= φ(7·5)=(7–1)·(5–1)=24.

Обчислення квадратних коренів величин $V_i^{'-1}$ означає визначення таких величин $S_i = sqrt(V_i^{'-1})(\text{mod}35)$, що $(S_i)^2 = V_i^{'-1}(\text{mod}35)$.

Наприклад, S5=9, так як 92 = 11(mod35), а S6=8, що слідує з порівняння 82 = 64 = 29(mod35). Оскільки за умовою k = 4, то з шести чисел множини M' виберемо, наприклад, значення V_2', V_4', V_5', V_6', тоді відкритим ключем є рядок чисел [4, 11, 16, 29], а відповідний йому особистий ключ є рядком чисел S2, S4, S5, S6, тобто [3, 4, 9, 8].

Сам протокол аутентифікації полягає в наступному.

Сторона А вибирає деяке випадкове число, наприклад, r = 16, і обчислює x = 16^2mod35 = 11, після чого дане значення відправляється стороні В.

Сторона надсилає стороні А деякий випадковий двійковий рядок $[b_1, b_2, b_3, b_4] = [1, 1, 0, 1]$, використовуючи який, сторона А обчислює значення

$$y = r \cdot (S_1^{b_1} \cdot S_2^{b_2} \cdot S_3^{b_3} \cdot S_4^{b_4})(\text{mod}\, N) = 16 \cdot (3^1 \cdot 4^1 \cdot 9^0 \cdot 8^1)\text{mod}35 = 31,$$

а потім відправляє отримане значення стороні В. Сторона В обчислює

$$x = y^2 \cdot (V'^{b_1}_1 \cdot V'^{b_2}_2 \cdot V'^{b_3}_3 \cdot V'^{b_4}_4)(\mathrm{mod}\, N) = 31^2 \cdot (4^1 \cdot 11^1 \cdot 16^0 \cdot 29^1) \mathrm{mod} 35 = 11$$

і переконується в тому, що сторона А є тим, за кого вона себе видає.

Отримані результати зведемо в таблицю 6.2.

Таблиця 6.2 – Варіанти вихідних даних

Номер варіант	p	q	Число циклів аутентифікаці	Номер варіант	p	q	Число циклів аутентифікаці
1	3	1	4	14	1	3	5
2	3	1	5	15	3	7	4
3	3	1	6	16	3	1	3
4	5	7	4	17	3	1	6
5	7	3	5	18	5	1	6
6	3	1	6	19	1	3	5
7	19	3	6	20	7	3	4
8	13	3	5	21	1	3	3
9	5	3	4	22	3	7	4
10	3	7	3	23	1	3	5
11	3	5	4	24	3	7	6
12	11	5	5	25	1	3	5
13	17	3	6	26	3	1	4

Література [1, с. 334 – 344; 2 с. 339 – 346; 3, с. 28 – 43; 4, с. 39 – 51].

Контрольні питання

1 Методи, способи і засоби добування ІзОД.

2 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах.

3 Який загальний порядок підготовки об'єктів захисту до категорування?

4 Перелік основних документів з ТЗІ, які відпрацьовуються при підготовці об'єкта захисту до категорування.

5 Основні заходи, що проводяться при підготовці об'єктів захисту до категорування.

6 З якою метою проводиться категорування об'єктів інформаційної діяльності?

7 Які основні критерії визначення готовності об'єкта захисту до обстеження і атестування?

8 Основний зміст інструкції щодо забезпечення безпеки ІзОД на об'єкті ЕОТ.

7 ПРОТИДІЯ ШКІДЛИВИМ ПРОГРАМАМ

7.1 Теоретичні відомості до лабораторної роботи

Коректна робота персонального комп'ютера в більшій мірі залежить не від надійності антивірусної програми, а від користувачів, які працюють на ньому.

Розглянемо рекомендації та мінімальні вимоги для забезпечення безпечної роботи персонального комп'ютера.

Перелік необхідних дій для безпечної роботи ПК:

а) не встановлювати стороннє програмне забезпечення (ПЗ), яке написано і випущено невідомою торговою маркою або не є масовим.

Приклади: Vksaver; Crack-програми; агенти збору повідомлень; нерегламентовані антивіруси; нерегламентовані браузери; прискорювачі роботи ПК;

б) при інсталяції програм завжди вибирайте ручне установлення. Тим самим ви можете запобігти інсталяції додаткової програми, яка може встановлюватися як «бонус» до основної програми.

Приклад: до програми інсталяції торрент клієнта інсталятор встановлює вам додатковий браузер в разі, якщо ви вибираєте швидке установлення і т. д.;

в) не відвідувати непопулярні, нерегламентовані інтернет-ресурси.

Такі інтернет-ресурси, як правило, містять шкідливе ПЗ. У разі відвідування подібних web-сайтів у жодному разі не клікати маніпулятором по спливаючих вікнах (сам сайт може викликати

довіру, але сам власник сайту через брак фінансових коштів або просто лінощі не піклувався про додаткову перевірку на наявність вірусів розміщуваної реклами).

Для перегляду даних про власника домену необхідно на сайті http://who.is ввести адресу сайту, в якому ви сумніваєтеся, або запідозрили, що даний ресурс – не оригінальний сайт організації. Наприклад, введемо адресу сайту університету залізничного транспорту kart.edu.ua, у відповідь отримуємо інформацію про сайт організації, яка наведена у таблиці 7.1;

Таблиця 7.1 – Інформація про сайт о університету залізничного транспорту kart.edu.ua

% This is the Ukrainian Whois query server #B.	
% The Whois is subject to Terms of use	
% See https://hostmaster.ua/services/	
%	
% % .UA whois	
% Domain Record:	
% ==========	
domain:	kart.edu.ua
admin-c:	KSSA2-UANIC
tech-c:	KSSA1-UANIC
status:	OK-UNTIL 20150614113410
nserver:	ns.bestnet.kharkov.ua
nserver:	ns.kart.edu.ua
remark:	Kharkov's State Academy of Railway Transport
created:	0-UANIC 20020530000000
changed:	UARR168-UANIC 20150113150507
source:	UANIC
% Glue Record:	
% ==========	
nserver:	ns.kart.edu.ua
ip-addr:	193.105.7.142
% Administrative Contact:	
% ==========	
nic-handle:	KSSA2-UANIC
organization:	Academy of Railway Transport, ICC, head

Продовження таблиці 7.1

address:	2.224, Feuerbach sq, 7
address:	61050 KHARKOV
address:	UA
phone:	+380 (57) 7322872
fax-no:	+380 (57) 7322872
e-mail:	ktim@kart.edu.ua
url:	http://kart.edu.ua
org-id:	AUTO 2400
mnt-by:	NONE
changed:	KSSA2-UANIC 20120404122830
source:	UANIC
% Technical Contact:	
% ================	
nic-handle:	KSSA1-UANIC
organization:	Academy of Railway Transport, ICC, admin
address:	Room 2.224, Feuerbach sq, 7
address:	61050 Kharkovskaya KHARKOV
address:	UA
phone:	+38 (057) 7322872
fax-no:	+38 (057) 7322872
e-mail:	postmaster@kart.edu.ua
url:	http://kart.edu.ua
org-id:	AUTO 2396
mnt-by:	NONE
changed:	KSSA1-UANIC 20100515120938
source:	UANIC
% % .UA whois	
% Query time: 12 msec	

г) не відкривати посилання, які надсилаються вам в соціальних мережах, програмах-месенджерах (Skype, Viber, ICQ), повідомлення електронною поштою. Навіть, якщо це повідомлення від ваших друзів;

д) не підключати свій флеш-носій до неперевірених або невідомих комп'ютерів (наприклад, центр друку фотографій; коли

ви хочете скопіювати фотографії для друку, використовуйте компакт-диск);

е) встановити антивірусну програму, яка входить в топ кращих антивірусів (у мережі зустрічається багато псевдо-антивірусів. Це віруси, які мають вигляд антивірусу і імітують роботу антивірусу);

ж) працювати на комп'ютері з правами доступу – користувач. Коли вірус проникає на персональний комп'ютер, він привласнює права поточного користувача і якщо ці права обмежені, вірус не може завдати великої шкоди. Отже, не використовувати користувача з правами – адміністратора (всі права на доступ) в повсякденній роботі з комп'ютером. В консолі управління користувачами створити користувача для щоденної роботи з ПК, а користувача з адміністративними правами використовувати в крайніх випадках для настроювання ОС і інсталяції нового програмного забезпечення;

и) усіх носіїв, що підключаються, завжди перевіряти на наявність комп'ютерних вірусів;

к) відключити автозавантаження носіїв інформації для запобігання самовільному запуску програм за допомогою файлу autoran.inf, як зображено на рисунку 7.1.

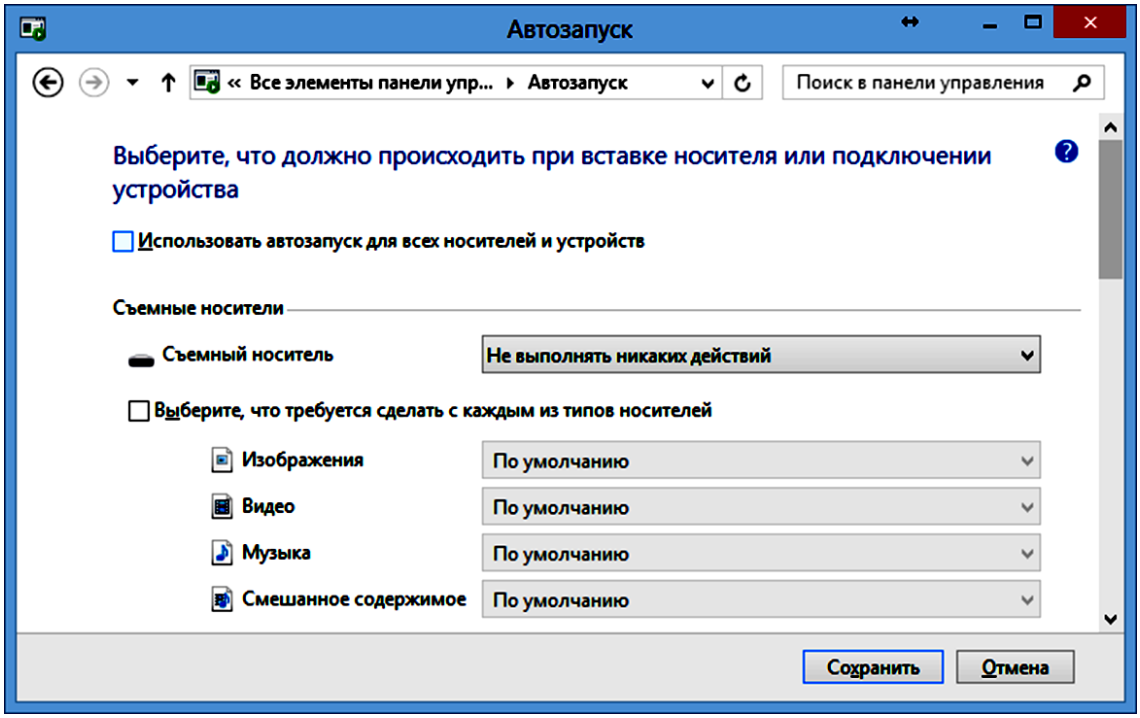

Рисунок 7.1 – Панель автозавантаження носіїв інформації

7.2 Хід виконання лабораторної роботи

Після встановлення антивірусної програми та відключення автозавантаження носіїв інформації треба встановлювати пакети оновлень операційної системи. Розробники ОС постійно відстежують вади у своєму продукті і випускають пакет оновлень, який усуває їх. Вади, як правило, знаходять «просунуті» хакери, які за допомогою них отримують віддалений доступ до системи. Як правило, необхідно встановлювати оновлення з позначкою «Оновлення безпеки Windows».

1 Оновлювати базу сигнатур «Антивірусне програмне забезпечення». Так як за хвилину в світі розробляється близько шістьох вірусів, то важливо показати роботу антивіруса.

2 Перевірити список програм і служб, що завантажуються з операційною системою. Необхідно відобразити весь список програм і служб, прочитати їх назву і опис. Проаналізувати непотрібні і сумнівні пункти в даному списку. Як правило, віруси записують в автозавантаження команди старту служб і програм. Як правило, в автозавантаженні мають перебувати тільки служби і програми від компанії Microsoft і програми, яким ви довіряєте (наприклад Skype).

3 Періодично користуватися пасивними антивірусними програмами (Dr. Web Curent IT, Kaspersky Virus Removal Tool) для сканування на наявність вірусів всієї системи. Дана дія дозволить вам протестувати ваш поточний антивірус на коректність роботи. Припустимо, що є віруси Х і У. Перший антивірус виявляє та знешкоджує тільки вірус Х, другий антивірус може знайти і знешкодити тільки вірус У. Тобто у кожної антивірусної програми свої бази сигнатур. Ще одна причина користуватися другим пасивним антивірусом – це загроза ураження вірусом вашого поточного антивірусу, тобто коли ваш антивірус змінюється «троянською програмою» і не функціонує в повному обсязі.

Розглянемо обидві програми. Dr. Web Curent IT зображено на рисунку 7.2.

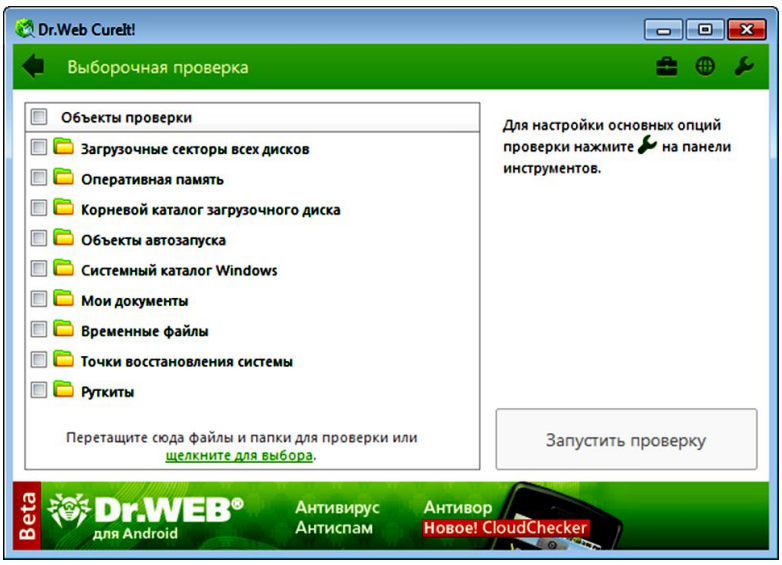

Рисунок 7.2 – Програма Dr. Web Curent IT

На офіційному сайті Dr. Web необхідно завантажити програму Dr. Web Curent IT. Посилання на сайт: http://www.freedrweb.com/cureit/. Програма є безкоштовною, її призначення – пошук вірусів і їх усунення. Дана програма є пасивною, тобто вона на працює в режимі моніторингу і не відстежує віруси в реальному часі. Вона запускається і зупиняється користувачем. Запускаємо програму і вибираємо об'єкти перевірки.

Після перевірки програма видасть список загроз і запропонує їх знешкодити.

Друга популярна програма це – Kaspersky Virus Removal Tool. Безкоштовна утиліта для «лікування» комп'ютера від вірусів і інших загроз допоможе вам виявити і знешкодити їх. Працює за таким же принципом що і програма Dr. Web Curent IT. Для кращого результату необхідно просканувати заражений комп'ютер двома програмами, так як немає гарантії, що з однією з них є повні бази сигнатур. Посилання на сайт для завантаження: http://www.kaspersky.ru/antivirus-removal-tool.

4 Сканування системи в безпечному режимі або без завантаження ОС. Якщо код вірусу знаходиться в системному файлі в занедбаному стані, ОС даний вірус не видалити. Дані режими дозволяють сканувати всі системні файли ОС, завантажувальний сектор диска, а також у разі їх виявлення знешкодити їх. Як приклад можна скористатися дистрибутивом

Dr.Web LiveCD або USB. Це незалежна від вашої системи самостійна операційна система, яка завантажується з завантажувального диска або флеш-носія. Програма сканує вашу ОС, всі системні файли, завантажувальні сектори, емулює запуск системних процесів. Після виявлення система знешкоджує заражені об'єкти.

Для застосування даної програми вам знадобиться змінний носій – CD або USB. На офіційному сайті Dr / Web посилання: http://www.freedrweb.com/livedisk/ викачуємо програму Dr.Web LiveCD (USB). Ми розглянемо варіант з USB-носієм. Запускаємо програму, підключаємо до комп'ютера вільний USB-носій. У програмі вибираємо даний USB-накопичувач і натискаємо кнопку Створити DR. Web LiveUSB. Після закінчення даної операції перезавантажуємо комп'ютер і систему завантажуємо з USB-носія.

Завантажується ОС, заснована на Linux-системі. У даній системі багато можливостей: від файлового менеджера до підключення до Інтернету, запусків перевірки на наявність шкідливих програм. Після завершення сканування програма запропонує перезавантажити комп'ютер.

5 Перевірити запущені процеси у вашій ОС. Як правило, процеси програмних вірусів запущені з довільною назвою, наприклад qr5s3u6fr.exe – якщо ви знайдете подібне ім'я в запущених процесах, швидше за все ваш комп'ютер заражений. Інший розповсюджений сигнал про те, що ваш комп'ютер заражений вірусом – це повільна робота всієї системи незалежно від того, чи навантажений комп'ютер або в процесі простою. Як правило, ваш системний процес заражений троянською програмою і ресурси ПК повністю зосереджені для виконання даного процесу. Для виявлення імені процесу в диспетчері завдань необхідно подивитися ім'я процесу і його завантаженість, простежити динаміку.

6 Не завантажувати і не запускати з глобальної мережі Інтернет виконувані файли (exe, bat, cmd, com і т.д.). Тобто якщо ви шукаєте драйвер до пристрою, він повинен бути з розширенням «.inf».

7 Звертати особливу увагу на файли, що знаходяться в архіві, а також в архіві з паролем. Дані файли не скануються антивірусом.

Література [1, с. 334 – 344; 2 с. 339 – 346; 3, с. 28 – 43; 4, с. 39 – 51].

Контрольні питання

1 Яке місце займає рахист інформації у сучасних інформаційних технологіях?

2 Найважливіші категорії службового ПЗ, що відносять до захисту інформації?

3 Як розповсюджуються віруси типу «Червь-вирусы»?

4 Що з нижчевказаного відносять до елементів політики безпеки?

5 Якими діями «зловмисник» відрізняється від «порушника»?

6 Для чого необхідна модель поведінки потенційного порушника?

7 Класи безпеки. Суть та стисла характеристика.

8 Які основні поняття використовуються при описі елементарної моделі захисту?

9 Наведіть вираз для визначення елементарного захисту, розкрийте його фізичний сенс.

10 Наведіть умову міцності перешкоди з виявленням та блокуванням несанкціонованого доступу.

11 Наведіть та проаналізуйте формулу для розрахунку міцності перешкоди з властивостями виявлення та блокування.

12 Наведіть та проаналізуйте формулу для розрахунку міцності перешкоди з урахуванням можливої відмови системи контролю.

13 Наведіть та проаналізуйте формулу для розрахунку міцності багатокільцевого захисту при використанні неконтрольованих перешкод.

14 Наведіть та проаналізуйте формулу для розрахунку міцності багатокільцевого захисту з контрольованими перешкодами.

15 Наведіть та проаналізуйте формулу для розрахунку сумарної міцності дублюючих перешкод.

8 ОРГАНІЗАЦІЯ ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ (OPENVPN)

8.1 Теоретичні відомості до лабораторної роботи

OpenVPN – вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим вихідним кодом для створення зашифрованих каналів типу «точка-точка» або «сервер-клієнти» між комп'ютерами. Вона дозволяє встановлювати з'єднання між комп'ютерами, що знаходяться за NAT і мережним екраном, без необхідності зміни їх налаштувань. OpenVPN була створена Джеймсом Йонаном (James Yonan) і розповсюджується під ліцензією GNU GPL.

Для забезпечення безпеки керуючого каналу і потоку даних OpenVPN використовує бібліотеку OpenSSL. Це дозволяє задіяти весь набір алгоритмів шифрування, доступних в даній бібліотеці. Також може використовуватися пакетна авторизація HMAC, для забезпечення більшої безпеки, і апаратне прискорення для поліпшення продуктивності шифрування. Ця бібліотека використовує OpenSSL, а точніше, протоколи SSLv3 / TLSv1 [2]. OpenVPN використовується в операційних системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU / Linux, Apple Mac OS X, QNX, Microsoft Windows, Android.

OpenVPN пропонує користувачеві кілька видів аутентифікації:

- встановлений ключ – найпростіший метод;
- сертифікатна аутентифікація – найбільш гнучкий в настроюваннях метод.

За допомогою логіна і пароля – може використовуватися без створення клієнтського сертифіката (серверний сертифікат все одно потрібен).

OpenVPN проводить всі мережні операції через TCP або UDP транспорт. TCP забезпечує кращу надійність передачі даних, однак критикується за великі затримки в порівнянні з UDP, який виграє в швидкості за рахунок відсутності підтвердження доставки пакетів. Також можлива робота через більшу частину проксі-серверів, включаючи HTTP, SOCKS, через NAT і мережні фільтри. Сервер може бути настроєний на призначення мережних

настроювань клієнту. Наприклад: IP-адреса, настроювання маршрутизації і параметри з'єднання. OpenVPN пропонує два різних варіанти мережних інтерфейсів, використовуючи драйвер TUN / TAP. Можливо створити тунель мережного рівня, званий TUN, і канального рівня – TAP, здатний передавати Ethernet-трафік. Також можливе використання бібліотеки компресії LZO для стиснення потоку даних. Використовуваний порт 1 194 виділений Internet Assigned Numbers Authority для роботи даної програми. Версія 2.0 дозволяє одночасно контролювати кілька тунелів, на відміну від версії 1.0, що дозволяла створювати тільки один тунель на один процес.

Використання в OpenVPN стандартних протоколів TCP і UDP дозволяє йому стати альтернативою IPsec в ситуаціях, коли інтернет-провайдер блокує деякі VPN протоколи.

8.2 Настроювання OpenVPN сервера на Windows

1 Викачуємо OpenVPN з сайту OpenVPN відповідно до розрядності системи.

Посилання: http://openvpn.net/index.php/open-source/downloads.html

2 Запускаємо установку, на 3-му кроці активуємо неактивні пункти. Наступний крок – шлях для установки. Щоб полегшити собі подальше життя, встановлюємо ПЗ в корінь диска C.

3 Створюємо каталог для ключів і сертифікатів, назвемо його "ssl".

4 У папці easy-rsa створюємо файл vars.bat.

```
set HOME=C:\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf
set KEY_DIR=C:\OpenVPN\ssl
set KEY_SIZE=1024
set KEY_COUNTRY=UA
set KEY_PROVINCE=Kiev
set KEY_CITY=Kiev
set KEY_ORG=test_org
set KEY_EMAIL=root@localhost
set KEY_CN=test
set KEY_NAME=test
set KEY_OU=test
set PKCS11_MODULE_PATH=test
set PKCS11_PIN=1234
```

5 Копіюємо файли index.txt.start і serial.start в папку ssl, і перейменовуємо, відповідно, в index.txt і serial.

6 Запускаємо командний рядок, переходимо шляхом C: \ OpenVPN \ Easy-RSA.

7 Запускаємо vars.bat та clean-all.b:

```
c:\OpenVPN\easy-rsa>vars.bat
c:\OpenVPN\easy-rsa>set HOME=C:\OpenVPN\easy-rsa
c:\OpenVPN\easy-rsa>set KEY_CONFIG=openssl-1.0.0.cnf
c:\OpenVPN\easy-rsa>set KEY_DIR=C:\OpenVPN\ssl
c:\OpenVPN\easy-rsa>set KEY_SIZE=1024
c:\OpenVPN\easy-rsa>set KEY_COUNTRY=UA
c:\OpenVPN\easy-rsa>set KEY_PROVINCE=Kiev
c:\OpenVPN\easy-rsa>set KEY_CITY=Kiev
c:\OpenVPN\easy-rsa>set KEY_ORG=test
c:\OpenVPN\easy-rsa>set KEY_EMAIL=root@localhost
c:\OpenVPN\easy-rsa>set KEY_CN=test
c:\OpenVPN\easy-rsa>set KEY_NAME=test
c:\OpenVPN\easy-rsa>set KEY_OU=test
c:\OpenVPN\easy-rsa>set PKCS11_MODULE_PATH=test
c:\OpenVPN\easy-rsa>set PKCS11_PIN=1234
c:\OpenVPN\easy-rsa>_
```

```
c:\OpenVPN\easy-rsa>clean-all.bat
Скопировано файлов:         1.
Скопировано файлов:         1.

c:\OpenVPN\easy-rsa>
```

8 Запускаємо vars.bat.

9 Запускаємо build-ca.bat. Так як вся інформація про сервер у нас вже заповнена, все залишаємо без змін.

10 Запускаємо vars.bat, build-dh.bat та vars.bat.

```
c:\OpenVPN\easy-rsa>build-dh.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.....++*++*++*
```

11 Створюємо серверний ключ `build-key-server.bat OpenVPN` .

Важливо! Вказуємо параметр "common name" – пишемо ім'я нашого VPN-сервера.

Всі інші параметри залишаємо за замовчуванням, на всі питання відповідаємо yes.

```
c:\OpenVPN\easy-rsa>build-key-server.bat OpenVPN
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..++++++
.......++++++
writing new private key to 'C:\OpenVPN\ssl\OpenVPN.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UA]:
State or Province Name (full name) [Kiev]:
Locality Name (eg, city) [Kiev]:
Organization Name (eg, company) [test]:
Organizational Unit Name (eg, section) [test]:
Common Name (eg, your name or your server's hostname) [test]:OpenVPN
Name [test]:
Email Address [root@localhost]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UA'
stateOrProvinceName   :PRINTABLE:'Kiev'
localityName          :PRINTABLE:'Kiev'
organizationName      :PRINTABLE:'test'
organizationalUnitName:PRINTABLE:'test'
commonName            :PRINTABLE:'OpenVPN'
name                  :PRINTABLE:'test'
emailAddress          :IA5STRING:'root@localhost'
Certificate is to be certified until May 19 19:23:45 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

12 Запускаємо vars.bat.

13 Приступаємо до створення конфіга сервера. В папці config створюємо файл OpenVPN.ovpn:

```
port 1194
proto udp
dev tun
dev-node "vpn"
dh C:\\OpenVPN\\ssl\\dh1024.pem
ca C:\\OpenVPN\\ssl\\ca.crt
cert C:\\OpenVPN\\ssl\\OpenVPN.crt
key C:\\OpenVPN\\ssl\\OpenVPN.key
server 192.168.15.0 255.255.255.0
cipher DES-CBC
status C:\\OpenVPN\\log\\openvpn-status.log
log C:\\OpenVPN\\log\\openvpn.log
verb 2
mute 20
max-clients 100
keepalive 10 120
client-to-client
comp-lzo
persist-key
persist-tun
```

14 Перейменовуємо TAP-інтерфейс в "vpn":

15 Запускаємо службу. Якщо все зробили правильно, мережний інтерфейс буде підключений.

16 Далі, перед тим як створювати клієнтські ключі, очищаємо вміст файла index.txt та build-key.bat user1. Вказуємо параметр "common name"

```
c:\OpenVPN\easy-rsa>build-key.bat user1
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................
.++++++
.....................................++++++
writing new private key to 'C:\OpenVPN\ssl\user1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UA]:
State or Province Name (full name) [Kiev]:
Locality Name (eg, city) [Kiev]:
Organization Name (eg, company) [test]:
Organizational Unit Name (eg, section) [test]:
Common Name (eg, your name or your server's hostname) [test]:OpenVPN
Name [test]:
Email Address [root@localhost]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UA'
stateOrProvinceName   :PRINTABLE:'Kiev'
localityName          :PRINTABLE:'Kiev'
organizationName      :PRINTABLE:'test'
organizationalUnitName:PRINTABLE:'test'
commonName            :PRINTABLE:'OpenVPN'
name                  :PRINTABLE:'test'
emailAddress          :IA5STRING:'root@localhost'
Certificate is to be certified until May 19 19:32:03 2023 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

17 Створюємо конфіг клієнта. Якщо на боці клієнта Windows, потрібен файлик з розширенням .ovpn, якщо Linux і ін. - .conf. Вміст у них однаковий:

```
client
proto udp
dev tun
ca ca.crt
dh dh1024.pem
cert user1.crt
key user1.key
remote 192.168.80.128 1194
cipher DES-CBC
user nobody
group nogroup
verb 2
mute 20
keepalive 10 120
comp-lzo
persist-key
persist-tun
float
resolv-retry infinite
nobind
```

У пункті "remote" вказуємо ip-адресу нашого сервера.

18 Склад "клієнтського" набору в даному випадку:

user1.conf и

user1.ovpn - тільки но створили вручну

user1.crt и

user1.key - в папці "ssl", створили в п. 20

ca.crt и

dh1024.pem - однакові для сервера та всіх клієнтів, також знаходятся в папці "ssl".

8.3 Настроювання OpenVPN клієнта на Windows

1 Перевірити дату і час! При неправильній даті-часі підключення не буде встановлено. Викачуємо клієнта.

Посилання:
http://swupdate.openvpn.org/community/releases/openvpn-install-2.3.2-I003-i686.exe

2 Встановлюємо OpenVPN клієнт.

Після встановлення не запускаємо.

Переходимо в директорію зі встановленою програмою, в папку "config".

3 Розпаковуємо архів з особистими ключами. Весь його вміст копіюємо в папку "config".

4 Переходимо до настроювання ярлика програми.

Натискаємо правою кнопкою мишки по ярлику "OpenVPN GUI", вибираємо властивості.

На вкладці "Ярлик", в полі "Об'єкт" в самому кінці дописуємо

```
--connect "имя_вашей_конфигурации.ovpn"
```

Тобто весь рядок повинен виглядати так:

"C:\Program Files\OpenVPN\bin\openvpn-gui.exe" --connect "test.ovpn", тільки замість test.ovpn, ім'я вашої конфігурації.

5 Переходимо на вкладку "Сумісність". Там ставимо галочку навпроти "Виконувати цю програму від імені адміністратора ".

6 Натискаємо "ОК", запускаємо OpenVPN з щойно створеного ярлика. Чекаємо закриття вікна.

Після закриття вікна поруч з годинником повинен з'явитися значок. Якщо він зеленого кольору, з'єднання встановлено.

Завдання на лабораторну роботу:

а) створити програмний сервер VPN в Windows.

б) призначити IP адресу підмережі = 192.168. [Ваш варіант] .0 / 24;

в) створити ключі і сертифікати для клієнтів VPN;

г) підключити клієнта до сервера VPN за допомогою створених ключів.

Література [1, с. 334 – 344; 2 с. 339 – 346; 3, с. 28 – 43; 4, с. 39 – 51].

Контрольні питання

1 З чого складається суть шифру методом перестановок?

2 Проаналізуйте перетворення методом перестановок за допомогою таблиці.

3 Дайте стислий опис шифру перестановки, який використовує геометричну фігуру (наприклад, прямокутник). Вкажіть умови вибору розміру боків прямокутника.

4 Дайте стислий опис шифру “Поворотна перестановка”. Вкажіть алгоритм шифрування.

5 Наведіть приклад використання “шифру вертикальної перестановки”.

6 Дайте стислий опис шифру перестановки, який використовує маршрути Гамільтона.

7 Методи, способи і засоби добування ІзОД.

8 Методи, способи і засоби технічного захисту ІзОД в мережах електрозв'язку, обчислювальних комплексах і комп'ютерах.

9 Який загальний порядок категорування об'єктів?

10 Основний зміст робіт з категорування об'єктів.

11 Порядок контролю документації на об'єкт, що атестується.

12 Який порядок призначення комісії з категорування?

13 Представники яких спеціальностей повинні призначатися до складу комісії з категорування?

14 Які дані потрібні для використання програми шифрування за допомогою першого алгоритму?

СПИСОК ЛІТЕРАТУРИ

1 Мірошник М. А. Інформаційно-управляючі системи та організації паралельних обчислень: Навч. посібник / С. В. Лістровий, О. С. Лістрова, М. А. Мірошник. – Харків: Діса плюс, 2015. – 324 с.

2 Дибкова Л. М. Інформатика і комп'ютерна техніка: Навч.посібник. – 2-ге вид., перероб. – К.: Академвидав, 2007. – 415 с.

3 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. – СПб.: Питер, 2007.

4 Новиков О. М., Грайворонский М. В. Захист інформації в комп’ютерних системах і мережах. – К.: ВНV, 2007. – 380 с.

5 Богуш В. М., Мухачов В. А. Криптографічні застосування елементарної теорії чисел: Навч. посібник [Держ. ун-т інформаційно-комунікаційних технологій]. – К.: ДУІКТ, 2006. – 126 с.

6 Башлий Н. П. Современные сетевые технологии: Учеб. пособие. – М.: Горячая линия-Телеком, 2006. – 334 с.

7 Злобін Г. Г., Рикалюк Р. Є. Архітектура та апаратне забезпечення ПЕОМ: Навч. посібник. – К.: Каравела, 2006. – 301 с.

8 Михеев Е. В. Практикум по информационным технологиям в профессиональной деятельности: Учеб. пособие. – 5-е изд., стереотип. – М.: Изд. центр «Академия», 2006. – 254 с.

9 Филин С. А. Информационная безопасность: Учеб. пособие. – М.: Альфа-Пресс, 2006. – 410 с.

10 Практикум по информатике и информационным технологиям: Учеб. пособие / Н. Угринович, Л. Босова, Н. Михайлова. – 4-е изд. – М.:Бином, 2006. – 394 с.

11 Программирование WEB-страниц / С. В. Глушаков, И. А. Жакин, Т. С. Хачиров. – Ростов н/Д.: Феникс, Харьков: Фолио, 2006. – 390 с.

12 Борисов М. В. Основы информатики и вычислительной техники: Учеб. пособие. – Ростов н/Д.: Феникс, 2006. – 541 с.

13 Попов В. Б. Основны информационных и телекоммуникационных технологий: Сетевые информационные технологии: Учеб. пособие. – М.: Финансы и статистика, 2005. – 218 с.

14 Шеховцова В. А. Операційні системи: Підручник. – К.: BHV, 2005. – 576 с.

15 Защита информации в телекоммуникационных системах / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – К.: МК-Пресс, 2005. – 279 с.

16 Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник для студ. Ч. 1. Криптографічний захист інформації / І. Д. Горбенко, Т. О. Гріненко [Харк. нац. ун-т радіоелектрон]. – Харків, 2004. – 368 с.

17 Маккарти Т. IT-безопасность: стоит ли рисковать корпорацией? / Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2004. – 208 с.

18 Скляров Д. Искуство взлома и защиты информации. – СПб.: БХВ-Петербург, 2004. – 288 с.

19 Скембрей Дж., Мак-Клар Ст. Секреты хаккеров. Безопасность Windows – готовые решения / Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 512 с.

20 Кибернетический подход к проектированию систем защиты информации / В. Гарбарчук, З. Зинович, А. Свиц [Укр. акад. инф-ки, Волын. гос. ун-т им. Л. Украинки, Любл. политехн. ун-т]. – К.; Луцк; Люблин, 2003. – 658 с.

21 Прокофьев И. В. Защита информации в компьютерных сетях: Учеб. пособие. – М.: Логос, 2003. – 264 с.

22 Пройдуков Э. М., Теплицкий Л. А. Англо-русский толковый словарь по вычислительной технике, Интернету и программированию. – 3-е изд., испр. и доп. – М.: Русская Редакция, 2002. – 640 с.

23 Гарнаев А. А. Excel, VBA, Internet в экономике и финансах. – СПб.: БХВ-Петербург, 2002. – 796 с.

24 Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. – М.: Российск. гос. гуманит. ун-т, 2002. – 399 с.

25 Вебер Р. Энциклопедия пользователя. Сборка, конфигурирование, настройка, модернизация и разгон ПК. – М., DiaSoft, 2001.

26 Бондаренко М. Ф., Кривуля Г. Ф. Проектирование и диагностика компьютерных систем и сетей. – Харьков, 2000.