МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA–технологій факультету №6

МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

з навчальної дисципліни "Прикладна криптологія"
обов'язкових компонент
освітньої програми першого рівня вищої освіти

"Кібербезпека (безпека інформаційних та комунікаційних систем)"

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол № 7 від 30.08.2023

СХВАЛЕНО
Вченою радою факультету №6
Протокол № 7 від 25.08.2023

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол № 7 від 29.08.2023

Розглянуто на засіданні кафедри кібербезпеки та DATA–технологій факультету №6 (протокол №8 від 15.08.2023)

Розробник: професор кафедри протидії кібербезпеки та DATA–технологій факультету, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №5						
Тема №1. Криптосистеми з секретним ключем	105	30		30	45	**залік**
Всього за семестр №5	**105**	**30**		**30**	**45**	
Семестр №6						
Тема №2. Криптосистеми з публічним ключем	85	20		20	45	**екз.**
Тема №3. Криптографічні протоколи	24	4		6	14	
Тема №4. Цифрова стеганографія	26	6		4	16	
Всього за семестр №6	**135**	**30**		**30**	**75**	
Всього за дисципліною	**240**	**60**		**60**	**120**	

2. Методичні вказівки до лабораторних занять

Тема №1. Криптосистеми з секретним ключем

Лабораторне заняття 1.1. Шифри заміни

Навчальна мета заняття: засвоїти принцип роботи шифрів заміни

Кількість годин: 2 год.

Навчальні питання

Вступ

1. Шифр Цезаря
2. Модулярний (афінний) шифр

Висновки

Література:

1. Матеріали лекції 1.
2. [3, с. 23-24].
3. [11, с. 17-18].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.2. Атаки на шифри заміни

Навчальна мета заняття: засвоїти техніки криптоаналізу шифрів заміни

Кількість годин: 2 год.

Навчальні питання

1. Атака повного перебору (brute force) на шифр заміни
2. Атака на шифр заміни із підрахунком частот літер

Література:

1. Матеріали лекції і керівництва до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.3. Шифр Віженера. Одноразовий блокнот

Навчальна мета заняття: засвоїти принцип роботи складних шифрів заміни

Кількість годин: 2 год.

Навчальні питання

1. Загальне визначення шифру складної заміни (багатоабетковий шифр)
2. Формальне визначення шифру складної заміни

Література:

1. Матеріали лекції 1, 2.
2. [3, с. 24-26].
3. [11, с.–с. 19-20].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.4. Атаки на шифр Віженера

Навчальна мета заняття: засвоїти техніку криптоаналізу шифра Віженера

Кількість годин: 4 год.

Навчальні питання

1. Ранжуванням літер за частотою використання в українських текстах
2. Атака на шифр Віженера

Література:

1. Матеріали лекції 1,2 і керівництва до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.5. Симетричний алгоритм шифрування AES

Навчальна мета заняття: засвоїти принцип роботи алгоритму шифрування AES

Кількість годин: 2 год.

Навчальні питання

1. Функціональність програми CrypTool 1
2. Аналіз візуалізації алгоритму шифрування AES

Література:

1. Матеріали лекції 10.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.6. Криптосистеми з секретним ключом у фреймворку OpenSSL

Навчальна мета заняття: перевірити теоретичні відомості про особливості роботи симетричних алгоритмів шифрування на практиці

Кількість годин: 4 год.

Навчальні питання

1. Інсталяція на ознайомлення із фреймворком OpenSSL
2. Дослідження особливостей реалізації симетричних алгоритмів шифрування

Література:

1. Матеріали лекції 10 і керівництво до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.7. Симетричний алгоритм шифрування Triple-DES в режимі CBC

Навчальна мета заняття: засвоїти принцип роботи алгоритму шифрування Triple-DES в режимі CBC

Кількість годин: 2 год.

Навчальні питання

1. Функціональність програми CrypTool 1
2. Аналіз роботи симетричного алгоритму шифрування Triple-DES в режимі CBC

Література:

1. Матеріали лекції 10.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.8. Гешування

Навчальна мета заняття: ознайомитися із безпечністю алгоритмів гешування

Кількість годин: 2 год.

Навчальні питання

1. Демонстрація гешування у програми CrypTool 1
2. Аналіз гешування із фреймворком OpenSSL

Література:

1. Матеріали лекції 13.

2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.9. Засоби генерації простору словникових ключів

Навчальна мета заняття: навчитися користуватися інструментами генерації парольних словників для криптоаналізу шифртексту

Кількість годин: 4 год.

Навчальні питання

1. PassphraseGen.
2. Crunch.
3. CUPP.
4. Mentalist.
5. Passphrase-wordlist

Література:

1. Керівництво до практичних і лабораторних занять.
2. https://securityonline.info/passphrasegen/
3. https://tools.kali.org/password-attacks/crunch
4. https://kali.tools/?p=151
5. https://securityonline.info/mentalist-create-wordlist/
6. https://securityonline.info/passphrase-wordlist/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 1.10. Засоби криптоаналізу дайджестів геш-функцій

Навчальна мета заняття: ознайомитися із засобами криптоаналізу дайджестів геш-функцій

Кількість годин: 6 год.

Навчальні питання

1. John the ripper.
2. Hashcat.
3. Hashtopolis.

Література:

1. Керівництво до практичних і лабораторних занять.
2. https://kali.tools/?p=747
3. https://hashcat.net/hashcat/
4. https://github.com/s3inlc/hashtopolis

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №2. Криптосистеми з публічним ключем

Лабораторне заняття 2.1. Елементи теорії чисел

Навчальна мета заняття: перевірити релевантні для криптосистем з публічним ключом положення теорії чисел.

Кількість годин: 6 год.

Навчальні питання

1. Прості числа
2. Основна теорема арифметики
3. Знаходження найбільшого спільного дільника (алгоритм Евкліда)

Література:

1. Матеріали лекції 14.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.2. Криптосистема з обміну ключами Diffie-Hellman

Навчальна мета заняття: засвоїти принцип роботи криптосистеми Diffie-Hellman з обміну ключами

Кількість годин: 2 год.

Навчальні питання

1. Демонстрація Diffie-Hellman Key Exchange в CrypTool 1

Література:

1. Матеріали лекції 16.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.3. Асиметричний криптографічний алгоритм RSA

Навчальна мета заняття: засвоїти принцип роботи криптографічного алгоритму RSA

Кількість годин: 4 год.

Навчальні питання

1. Аналіз роботи асиметричного криптографічного алгоритму RSA в CrypTool 1
2. Демонстрація цифрового підпису

3. RSA в фреймворке OpenSSL

Література:

1. Матеріали лекції 17.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.4. Криптосистеми з публічним ключом у фреймворку OpenSSL

Навчальна мета заняття: перевірити теоретичні відомості про особливості роботи симетричних алгоритмів шифрування на практиці

Кількість годин: 4 год.

Навчальні питання

1. Інфраструктура відкритих ключів (PKI)
2. Створення підписаного повідомлення
3. Налаштування веб-серверу з автентифікацією клієнтів за допомогою сертифікатів

Література:

1. Матеріали лекції 20 і керівництво до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.5. Криптосистеми на еліптичних кривих

Навчальна мета заняття: перевірити теоретичні відомості про особливості роботи криптосистем на еліптичних кривих

Кількість годин: 4 год.

Навчальні питання

1. Демонстрація Point addition on elliptic curves в CrypTool 1.
2. Elliptic Curve scalar multiplication.

Література:

1. Матеріали лекції 20 і керівництво до лабораторних занять.
2. https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/modk-mul.html

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Криптографічні протоколи

Лабораторне заняття 3.1. Криптографічний протокол SSL/TLS

Навчальна мета заняття: засвоїти принцип роботи криптографічного протоколу SSL/TLS

Кількість годин: 2 год.

Навчальні питання

1. Протокол SSL/TLS
2. Testing TLS/SSL encryption
3. Аналіз SSL/TLS у Wireshark

Література:

1. Керівництво до практичних і лабораторних занять
2. https://n0where.net/testing-tlsssl-encryption

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 3.2. Протокол Network Authentication

Навчальна мета заняття: засвоїти принцип роботи криптопротоколу із Network Authentication

Кількість годин: 2 год.

Навчальні питання

1. Демонстрація Network Authentication в CrypTool 1

Література:

1. Матеріали лекції 23.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 3.3. Протокол шифрування електронної пошти S/MIME

Навчальна мета заняття: засвоїти принцип роботи протоколу Secure E-Mail with S/MIME

Кількість годин: 2 год.

Навчальні питання

1. Демонстрація Secure E-Mail with S/MIME в CrypTool 1

Література:

1. Матеріали лекції 23.
2. https://www.cryptool.org/en/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №4. Цифрова стеганографія

Лабораторне заняття 4.1. Метод модифікації найменшого значущого біта

Навчальна мета заняття: засвоїти принцип роботи методу модифікації найменшого значущого біта

Кількість годин: 4 год.

Навчальні питання

1. Теоретичні відомості
2. Практичне застосування утиліти OpenStego

Література:

1. Керівництво до практичних і лабораторних занять
2. https://www.youtube.com/watch?v=yNo58UiIMKU
3. https://www.openstego.com/

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Дистанційний курс University of Maryland by Jonathan Katz "Криптографія". https://www.coursera.org/course/cryptography.
2. Остапов С.Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
3. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві : Навч. посібник. – Одеса: ОНАЗ ім. О. С. Попова, 2003. – 80 с.
4. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. - К.: ДУІКТ, 2006. - 126 с.
5. Кузнецов О.О. Стеганографія : навчальний посібник / О.О. Кузнецов, С.П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

Допоміжна

6. Henk C.A. van Tilborg, FUNDAMENTALS OF CRYPTOLOGY. A Professional Reference and Interactive Tutorial. Eindhoven University of Technology. The Netherlands. KLUWER ACADEMIC PUBLISHERS, Boston/Dordrecht/London.
7. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.

Інформаційні ресурси

8. https://www.coursera.org/course/cryptography
9. https://www.coursera.org/course/crypto
10. https://www.coursera.org/course/crypto2
11. https://www.cryptool.org/en/