МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«___» _____ 20___р.

РОБОЧА ПРОГРАМА

з дисципліни

«КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА МЕТОДИ КРИПТОАНАЛІЗУ»

ступінь вищої освіти – **магістр**

галузь знань – **12 Інформаційні технології**

спеціальність – **125 Кібербезпека та захист інформації**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. заняття (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	1	2	30	15	5	8	92	150	2
Заочна	1	2	8	4	-	-	138	150	2

Тернопіль - 2023

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 3 від 28 . 09 . 2023 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 2 від 02 . 10 . 2023 р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Криптографічні протоколи та методи криптоаналізу”

Дисципліна “Криптографічні протоколи та методи криптоаналізу”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 3	спеціальність – 125 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 2* *Заочна – 2*
Кількість змістових модулів – 3	ступінь вищої освіти – магістр	Лекції (год): *Денна – 30* *Заочна - 8* Практичні заняття (год): *Денна – 15* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 100* (в т.ч. тренінг, КПІЗ – 8 год.) *Заочна - 138* Індивідуальна робота (год): *Денна – 5*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета й завдання вивчення дисципліни “Криптографічні протоколи та методи криптоаналізу”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Криптографічні протоколи та методи криптоаналізу” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного криптографічного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу “Криптографічні протоколи та методи криптоаналізу» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи програмування», «Кібернетична безпека», «Системи та технології кібербезпеки», «Моніторинг та управління інформаційною безпекою», «Дискретна математика», «Криптографія»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є систематизація інформації щодо розроблення, впровадження та експлуатації криптографічних систем захисту інформації на об’єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик криптографічного захисту інформації.

У результаті вивчення навчальної дисципліни студент повинен:

– засвоїти основні фундаментальні поняття і закони криптографічного захисту інформації для їх використання в сучасних комп'ютерних системах;

– знати принципи побудови криптографічних протоколів та їх використання в задачах захисту інформації;

– використовувати основні математичний апарат та закони криптографії в професійній діяльності;

– вміти використовувати програмні засоби, які реалізують основні криптографічні протоколи;

– програмно реалізовувати криптографічні протоколи вирішення типових задач захисту інформації;

– проектувати різного рівня криптографічні системи захисту з врахуванням методів криптоаналізу;

– вміння використовувати методи та засоби криптографічного захисту даних.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Криптографічні протоколи та методи криптоаналізу». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Криптографічні протоколи та методи криптоаналізу» та формуванні у студентів цілісної системи теоретичних знань з курсу «Криптографічні протоколи та методи криптоаналізу».

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення практичних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

3. Програма навчальної дисципліни "Криптографічні протоколи та методи криптоаналізу"

Змістовий модуль 1. Криптографічні протоколи.

Тема 1. Сучасні симетричні та асиметричні криптосистеми.

Структура алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES. Структура алгоритму IDEA. Сімейство алгоритмів RC. Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля.

Тема 2. Поняття криптографічних протоколів. Їх опис.

Визначення криптографічного протоколу. Учасники протоколу. Вербальний опис. Математичний опис виконуваних операцій з вербальним описом дій учасників. Опис по кроках протоколу. Символічний опис. Опис у вигляді відображення послідовності дій.

Тема 3. Класифікація криптографічних протоколів.

Примітивні і прикладні криптографічні протоколи. Класифікація за кількістю учасників. Класифікація за кількістю переданих повідомлень. Класифікація за цільовим призначенням протоколу. За типом використовуваних криптографічних систем. За способом функціонування. Класифікація за надійністю.

Тема 4. Властивості, що визначають безпеку криптографічних протоколів.

Аутентифікація. Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення. Авторизація (довіреною третьою стороною). Властивості спільної генерації ключа. Конфіденційність. Анонімність. Захищеність від атак типу «відмова в обслуговуванні». Інваріантність відправника. Неможливість відмови від раніше вчинених дій. Безпечна тимчасова властивість.

Тема 5. Аналіз та моделювання криптографічних протоколів.

Моделювання і перевірка роботи протоколу з використанням мов опису і засобів перевірки, не розроблених для аналізу криптографічних протоколів. Створення експертних систем. Вироблення вимог до сімейства протоколів. Розробка формальних методів. Протоколи з посередником. Протоколи з арбітром. Самодостатні протоколи.

Тема 6. Протоколи електронного цифрового підпису.

Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

Змістовий модуль 2. Протоколи розподілу криптографічних ключів.

Тема 7. Протоколи, що ґрунтуються на симетричних криптосистемах.

Протокол Барроуза. Протокол Нідхема-Шредера. Протокол Kerberos. Протокол розподілу ключів по паралельних каналах.

Тема 8. Протоколи, що ґрунтуються на асиметричних криптосистемах.

Протокол обміну ключами Діффі-Хелмана. Триразовий протокол рукостискання. Протокол MQV (Менезес-Кью-Ванстоун).

Тема 9. Квантовий розподіл ключів.

Протокол BB84. Протокол B92. Протокол E91 (EPR). Протокол розподілу ключів, що грунтується на кодуванні через часові зсуви. Протокол на основі квантового прямого безпечного зв'язку. Протокол на основі методу довірених кур’єрів.

Тема 10. Протокол розподілу ключів за допомогою еліптичних кривих.

Протокол Діффі-Хелмана. Опис протоколу. Приклад застосування. Приклади програмної реалізації.

Змістовий модуль 3. Методи криптоаналізу.

Тема 11. Вступ до криптоаналізу. Криптоаналітичні атаки.

Вступ. Основні поняття криптоаналізу. Криптоаналіз шифру Цезаря. Типи криптостійких систем шифрування. Поняття про атаки на алгоритми шифрування та їх класифікація. Метод повного перебору. Моделі оцінки безпеки. Типи атак на алгоритми шифрування. Ідеальний шифр, принципи побудови та властивості. Безумовно стійкі та практично (обчислювально) стійкі шифри.

Тема 12. Атаки на протоколи.

Класи криптоаналітичних атак. Атаки на схеми зашифрування. Пасивні атаки. Активні атаки. Пасивні шахраї. Активні шахраї. Підміна. Повторне нав’язування повідомлення. Атака відображенням. Затримка передачі повідомлення. Комбінована атака. Атака з паралельними сеансами. Атака з використанням спеціально підібраних текстів. Атака «противник в середині». Атака з відомим сеансовим ключем. Атака з невідомим спільним ключем. Атака вичерпного пошуку та словникова атака. Атака на основі парадоксу днів народження. Атака на основі застосування таблиць передобчислень.

Тема 13. Криптоаналіз симетричних криптосистем.

Універсальні методи криптоаналізу. Атака по ключам. Частотний аналіз. Методи криптоаналізу блочних шифрів. Методи криптоаналізу потокових шифрів. Криптоаналіз по побічним каналам. Стійкість сучасних стандартів симетричного шифрування. Криптоаналіз методом «зустрічі посередині».

Тема 14. Диференційний (різницевий) криптоаналіз.

Сутність диференційного криптоаналізу. Диференційні властивості підстановки блокового шифру DES. Механізм відновлення бітів ключа при знанні вхідних різниць підстановки. Операція додавання ключа. Різниці у цикловій функції блокового шифру DES. Складність диференційного криптоаналізу блокового шифру DES..

Тема 15. Криптоаналіз асиметричних криптосистем.

Криптоаналіз асиметричних криптосистем. Криптоаналіз геш-функцій. Рішення завдання факторизації. Рішення задачі дискретного логарифма. Квантові обчислення.

4. Структура залікового кредиту дисципліни “Криптографічні протоколи та методи криптоаналізу”

4.1 Структура залікового кредиту дисципліни “Криптографічні протоколи та методи криптоаналізу” для ДФН

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Тренінг, КПІЗ	Контрольні заходи
Змістовий модуль 1. **Криптографічні протоколи.**						
Тема 1. Сучасні симетричні та асиметричні криптосистеми**.**	2	1	6	-	2	Поточне опитування
Тема 2. Поняття криптографічних протоколів. Їх опис.	2	1	6	-		Поточне опитування
Тема 3. Класифікація криптографічних протоколів**.**	2	1	6	-		Поточне опитування
Тема 4. Властивості, що визначають безпеку криптографічних протоколів**.**	2	1	6	-		Поточне опитування
Тема 5. Аналіз та моделювання криптографічних протоколів.	2	1	6	1		Поточне опитування
Тема 6. Протоколи електронного цифрового підпису.	2	1	7	-		Поточне опитування
Змістовий модуль 2. **Протоколи розподілу криптографічних ключів**						
Тема 7. Протоколи, що ґрунтуються на симетричних криптосистемах.	2	1	6	-	3	Поточне опитування
Тема 8. Протоколи, що ґрунтуються на асиметричних криптосистемах**.**	2	1	6	-		Поточне опитування
Тема 9. Квантовий розподіл ключів	2	1	6	-		Поточне опитування
Тема 10. Протокол розподілу ключів за допомогою еліптичних кривих	2	1	6	2		Поточне опитування
Змістовий модуль 3. **Методи криптоаналізу.**						
Тема 11. Вступ до криптоаналізу. Криптоаналітичні атаки**.**	2	1	6	-	3	Поточне опитування
Тема 12. Атаки на протоколи**.**	2	1	6	-		Поточне опитування
Тема 13. Криптоаналіз симетричних криптосистем**.**	2	1	6	-		Поточне опитування
Тема 14. Диференційний (різницевий) криптоаналіз**.**	2	1	6	-		Поточне опитування
Тема 15. Криптоаналіз асиметричних криптосистем**.**	2	1	7	2		Поточне опитування
Разом	30	15	92	5	8	

4.2 Структура залікового кредиту дисципліни "Криптографічні протоколи та методи криптоаналізу" для ЗФН

	Кількість годин		
	Лекції	Практичні заняття	Самостійна робота
Змістовий модуль 1. **Криптографічні протоколи.**			
Тема 1. Сучасні симетричні та асиметричні криптосистеми**.**	0,5	-	9
Тема 2. Поняття криптографічних протоколів. Їх опис.	0,5	-	9
Тема 3. Класифікація криптографічних протоколів**.**	0,5	-	9
Тема 4. Властивості, що визначають безпеку криптографічних протоколів**.**	0,5	1	9
Тема 5. Аналіз та моделювання криптографічних протоколів.	0,5	-	9
Тема 6. Протоколи електронного цифрового підпису.	0,5	1	9
Змістовий модуль 2. **Протоколи розподілу криптографічних ключів**			
Тема 7. Протоколи, що ґрунтуються на симетричних криптосистемах.	0,5	-	9
Тема 8. Протоколи, що ґрунтуються на асиметричних криптосистемах**.**	0,5	-	9
Тема 9. Квантовий розподіл ключів	1	-	9
Тема 10. Протокол розподілу ключів за допомогою еліптичних кривих	0,5	1	9
Змістовий модуль 3. **Методи криптоаналізу**			
Тема 11. Вступ до криптоаналізу. Криптоаналітичні атаки**.**	0,5	-	9
Тема 12. Атаки на протоколи**.**	0,5	-	10
Тема 13. Криптоаналіз симетричних криптосистем**.**	0,5	1	9
Тема 14. Диференційний (різницевий) криптоаналіз**.**	0,5	-	10
Тема 15. Криптоаналіз асиметричних криптосистем**.**	0,5	-	10
Разом	8	4	138

5. Тематика практичних занять.

5.1 Тематика практичних занять для ДФН.

Практичне заняття №1

Тема: Сучасні симетричні та асиметричні криптосистеми.

Мета: Вивчення та дослідження сучасних симетричних та асиметричних криптосистем.

Питання для обговорення:

1. Структура алгоритму DES. Функція шифрування алгоритму DES.
2. Генерація підключів алгоритму DES.
3. Режими роботи алгоритму DES.
4. Структура алгоритму IDEA.
5. Сімейство алгоритмів RC.
6. Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування.
7. Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна.
8. Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля.

Література: 1-15.

Практичне заняття № 2

Тема: Поняття криптографічних протоколів. Їх опис та класифікація.

Мета: Вивчення та дослідження поняття криптографічних протоколів, їх опису та класифікації.

Питання для обговорення:

1. Визначення криптографічного протоколу. Учасники протоколу.

2. Вербальний опис. Математичний опис виконуваних операцій з вербальним описом дій учасників.
3. Опис по кроках протоколу. Символічний опис.
4. Опис у вигляді відображення послідовності дій.
5. Примітивні і прикладні криптографічні протоколи.
6. Класифікація за кількістю учасників.
7. Класифікація за кількістю переданих повідомлень.
8. Класифікація за цільовим призначенням протоколу.
9. Класифікація за типом використовуваних криптографічних систем. Класифікація за способом функціонування.
10. Класифікація за надійністю.

Література: 1-15.

Практичне заняття №3

Тема: Властивості, що визначають безпеку криптографічних протоколів, аналіз і моделювання їх роботи.

Мета: Вивчення та дослідження властивостей, що визначають безпеку криптографічних протоколів, аналіз та моделювання їх роботи.

Питання для обговорення:

1. Аутентифікація. Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення.
2. Авторизація (довіреною третьою стороною).
3. Властивості спільної генерації ключа. Конфіденційність. Анонімність.
4. Захищеність від атак типу «відмова в обслуговуванні». Інваріантність відправника.
5. Неможливість відмови від раніше вчинених дій. Безпечна тимчасова властивість.
6. Моделювання і перевірка роботи протоколу з використанням мов опису і засобів перевірки, не розроблених для аналізу криптографічних протоколів.
7. Створення експертних систем.
8. Вироблення вимог до сімейства протоколів.
9. Розробка формальних методів.
10. Протоколи з посередником. Протоколи з арбітром. Самодостатні протоколи.

Література: 1-15.

Практичне заняття № 4

Тема: Протоколи електронного цифрового підпису. Протоколи, що ґрунтуються на симетричних криптосистемах.

Мета: Вивчення та дослідження протоколів електронного цифрового підпису та протоколів, що ґрунтуються на симетричних криптосистемах.

Питання для обговорення:

1. Поняття електронного цифрового підпису.
2. Електронний цифровий підпис в системах RSA та Ель–Гамаля.
3. Алгоритм DSA.
4. Система Шнорра.
5. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.
6. Протокол Барроуза.
7. Протокол Нідхема-Шредера.
8. Протокол Kerberos.
9. Протокол розподілу ключів по паралельних каналах.

Література: 1-15.

Практичне заняття № 5

Тема: Протоколи, що ґрунтуються на асиметричних криптосистемах. Квантовий розподіл ключів.

Мета: Вивчення та дослідження протоколів, що ґрунтуються на симетричних криптосистемах та квантового розподілу ключів.

Питання для обговорення:

1. Протокол обміну ключами Діффі-Хелмана.

2. Триразовий протокол рукостискання.
3. Протокол MQV (Менезес-Кью-Ванстоун).
4. Протокол BB84.
5. Протокол B92.
6. Протокол E91 (EPR).
7. Протокол розподілу ключів, що грунтується на кодуванні через часові зсуви.
8. Протокол на основі квантового прямого безпечного зв'язку.
9. Протокол на основі методу довірених кур'єрів

Література: 1-15.

Практичне заняття №6

Тема: Протокол розподілу ключів за допомогою еліптичних кривих. Вступ до криптоаналізу. Криптоаналітичні атаки.

Мета: Вивчення та дослідження протоколів розподілу ключів за допомогою еліптичних кривих**.** Вступ до криптоаналізу. Криптоаналітичні атаки

Питання для обговорення:

1. Протокол Діффі-Хелмана.
2. Опис протоколу.
3. Приклад застосування.
4. Приклади програмної реалізації.
5. Вступ. Основні поняття криптоаналізу. Криптоаналіз шифру Цезаря.
6. Типи криптостійких систем шифрування.
7. Поняття про атаки на алгоритми шифрування та їх класифікація. Метод повного перебору.
8. Моделі оцінки безпеки.
9. Типи атак на алгоритми шифрування.
10. Ідеальний шифр, принципи побудови та властивості.
11. Безумовно стійкі та практично (обчислювально) стійкі шифри.

Література: 1-15.

Практичне заняття № 7

Тема: Атаки на протоколи. Криптоаналіз симетричних криптосистем.

Мета: Вивчення та дослідження атак на криптографічні протоколи та методів криптоаналізу симетричних криптосистем.

Питання для обговорення:

1. Класи криптоаналітичних атак. Атаки на схеми зашифрування.
2. Пасивні атаки. Активні атаки. Пасивні шахраї. Активні шахраї.
3. Підміна. Повторне нав'язування повідомлення.
4. Атака відображенням. Затримка передачі повідомлення.
5. Комбінована атака. Атака з паралельними сеансами.
6. Атака з використанням спеціально підібраних текстів. Атака «противник в середині».
7. Атака з відомим сеансовим ключем. Атака з невідомим спільним ключем. А
8. така вичерпного пошуку та словникова атака.
9. Атака на основі парадоксу днів народження. Атака на основі застосування таблиць передобчислень.
10. Універсальні методи криптоаналізу. Атака по ключам.
11. Частотний аналіз. Методи криптоаналізу блочних шифрів.
12. Методи криптоаналізу потокових шифрів.
13. Криптоаналіз по побічним каналам.
14. Стійкість сучасних стандартів симетричного шифрування.
15. Криптоаналіз методом «зустрічі посередині»

Література: 1-15.

Практичне заняття №8

Тема: Диференційний (різницевий) криптоаналіз. Криптоаналіз асиметричних криптосистем.

Мета: Вивчення та дослідження диференційного (різницевого) крипто аналізу та криптоаналізу асиметричних криптосистем**.**

Питання для обговорення:

1. Сутність диференційного криптоаналізу.
2. Диференційні властивості підстановки блокового шифру DES.
3. Механізм відновлення бітів ключа при знанні вхідних різниць підстановки.
4. Операція додавання ключа.
5. Різниці у цикловій функції блокового шифру DES.
6. Складність диференційного криптоаналізу блокового шифру DES.
7. Криптоаналіз асиметричних криптосистем.
8. Криптоаналіз геш-функцій.
9. Рішення завдання факторизації.
10. Рішення задачі дискретного логарифма.
11. Квантові обчислення.

Література: 1-15.

5.2 Тематика практичних занять для ЗФН.

Практичне заняття №1

Тема: Властивості, що визначають безпеку криптографічних протоколів, аналіз і моделювання їх роботи.

Мета: Вивчення та дослідження властивостей, що визначають безпеку криптографічних протоколів, аналіз та моделювання їх роботи.

Питання для обговорення:

1. Аутентифікація. Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення.
2. Авторизація (довіреною третьою стороною).
3. Властивості спільної генерації ключа. Конфіденційність. Анонімність.
4. Захищеність від атак типу «відмова в обслуговуванні». Інваріантність відправника.
5. Неможливість відмови від раніше вчинених дій. Безпечна тимчасова властивість.
6. Моделювання і перевірка роботи протоколу з використанням мов опису і засобів перевірки, не розроблених для аналізу криптографічних протоколів.
7. Створення експертних систем.
8. Вироблення вимог до сімейства протоколів.
9. Протоколи з посередником. Протоколи з арбітром. Самодостатні протоколи.

Література: 1-15.

Практичне заняття № 2

Тема: Протоколи електронного цифрового підпису. Протоколи, що ґрунтуються на симетричних криптосистемах.

Мета: Вивчення та дослідження протоколів електронного цифрового підпису та протоколів, що ґрунтуються на симетричних криптосистемах.

Питання для обговорення:

1. Поняття електронного цифрового підпису.
2. Електронний цифровий підпис в системах RSA та Ель–Гамаля.
3. Алгоритм DSA.
4. Система Шнорра.
5. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.
6. Протокол Барроуза.
7. Протокол Нідхема-Шредера.
8. Протокол Kerberos.
9. Протокол розподілу ключів по паралельних каналах.

Література: 1-15.

Практичне заняття №3

Тема: Протокол розподілу ключів за допомогою еліптичних кривих. Вступ до криптоаналізу. Криптоаналітичні атаки.

Мета: Вивчення та дослідження протоколів розподілу ключів за допомогою еліптичних кривих**.** Вступ до криптоаналізу. Криптоаналітичні атаки

Питання для обговорення:

1. Протокол Діффі-Хелмана.
2. Опис протоколу.
3. Приклад застосування.
4. Приклади програмної реалізації.
5. Вступ. Основні поняття криптоаналізу. Криптоаналіз шифру Цезаря.
6. Типи криптостійких систем шифрування.
7. Поняття про атаки на алгоритми шифрування та їх класифікація. Метод повного перебору.
8. Моделі оцінки безпеки.
9. Типи атак на алгоритми шифрування.
10. Ідеальний шифр, принципи побудови та властивості.
11. Безумовно стійкі та практично (обчислювально) стійкі шифри.

Література: 1-15.

Практичне заняття №4

Тема: Диференційний (різницевий) криптоаналіз. Криптоаналіз асиметричних криптосистем.

Мета: Вивчення та дослідження диференційного (різницевого) крипто аналізу та криптоаналізу асиметричних криптосистем**.**

Питання для обговорення:

1. Сутність диференційного криптоаналізу.
2. Диференційні властивості підстановки блокового шифру DES.
3. Механізм відновлення бітів ключа при знанні вхідних різниць підстановки.
4. Операція додавання ключа.
5. Різниці у цикловій функції блокового шифру DES.
6. Складність диференційного криптоаналізу блокового шифру DES.
7. Криптоаналіз асиметричних криптосистем.
8. Криптоаналіз геш-функцій.
9. Рішення завдання факторизації.
10. Рішення задачі дискретного логарифма.
11. Квантові обчислення.

Література: 1-15.

6. Комплексне практичне індивідуальне завдання (КПІЗ).

Індивідуальне завдання з курсу “Криптографічні протоколи та методи криптоаналізу” виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є оволодіння навиками використання стеганографічних методів при вирішенні конкретних задач кібербезпеки. Студенти повинні дослідити та застосувати криптографічні протоколи за одним із варіантів:

1. Протокол доведення з нульовим пізнанням.
2. Протокол обміну ключами.
3. Протокол для проблеми криптографів, що обідають.
4. Протокол Діффі - Геллмана на еліптичних кривих.
5. Протокол Signal.
6. Протоколи таємного голосування.
7. Протокол CCMP.
8. Протокол HOTP.
9. Протокол HTTPS.
10. Протокол Kerberos.
11. Протокол KMIP.
12. Протокол MIKEY.
13. Протокол OCRA.
14. Протокол Off-the-Record Messaging.

15. Протокол OMEMO.
16. Протокол SCRAM.
17. Протокол SDES.
18. Протокол SSL.
19. Протокол Subresource Integrity.
20. Протокол Transport Layer Security.
21. Протокол Wi-Fi Protected Setup.
22. Протокол ZRTP.
23. Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести.
24. Криптографічно безпечні генератори псевдовипадкових послідовностей.
25. Випадкові числа. Генератори випадкових чисел.
26. Генератори псевдовипадкових послідовностей.
27. Використання стандартних функцій мов програмування високого рівня. Конгруентний генератор псевдовипадкових чисел.
28. Лінійні регістри зі зворотним зв'язком (LFSR). Модифіковані LFSR.
29. Криптографічно стійкі датчики випадкових чисел.
30. Системно-теоретичний підхід отримання випадкових чисел.
31. Складнісно-теоретичний підхід отримання випадкових чисел.
32. Інформаційно-теоретичний підхід отримання випадкових чисел.
33. Рандомізований підхід отримання випадкових чисел.
34. Генератори справжніх випадкових чисел. Відхилення та кореляції.
35. Розподіл випадковості за допомогою односторонньої хеш-функції.
36. Статистичні тести для псевдовипадкових чисел.
37. Метод криптоаналізу «метод зустрічі посередині».
38. Поліграмний шифр Хілла і дослідження методів його криптоаналізу.
39. Аналіз криптографічної стійкості AES.
40. Лінійний криптоаналіз.
41. Сутність та вимоги до протоколів автентифікації.
42. Аналіз методів криптографічного аналізу криптоперетворень в циклічних групах та підгрупах.
43. Аналіз відомих вразливостей банків та нанесених втрат.
44. Порівняльний аналіз стійкості асиметричних крипто перетворень.
45. Вимоги до засобів генерування та застосування ключів та ключової інформації.
46. Класифікація та оцінка стійкості криптоперетворень в групі точок еліптичних кривих.
47. Порівняльний аналіз методів криптографічного аналізу симетричних шифрів.
48. Сутність та вразливості симетричних крипто перетворень.
49. Аналіз вразливостей блокових шифрів.
50. Класифікація та оцінка вразливості відомих методів криптоаналізу відносно блокових симетричних шифрів.
51. Порівняльний аналіз методів криптоаналізу симетричних шифрів.
52. Вимоги до криптостійкості блокових шифрів.

Виконання КПІЗ є одним із обов’язкових складових модулів залікового кредиту.

7. Самостійна робота

№ п/п	Тематика
1	Криптографічні атаки по стороннім каналам.
2	Криптографічні вразливості: недостатній аналіз розробленого алгоритму, застосування застарілих перетворень та некоректне застосування перетворень.
3	Атака розширення довжини на конструкцію Меркля-Дамгарда.
4	Застосування слабкого протоколу управління ключами.
5	Рекомендації щодо застосування криптографічних протоколів.

6	Криптографія на основі ідентифікаторів.
7	Інфраструктура відкритих ключів. Центр сертифікації ключів. Кореневий центр сертифікації.
8	Кроссертифікація. Сертифікат X.509 v3.
9	Список відкликаних сертифікатів. Причини відкликання сертифікату.
10	Протокол OCSP (Online Certificate Status Protocol).
11	Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення.
12	Методи бінарного відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії та властивості.
13	Вимоги, методи та засоби оцінки нерозрізнюваності, необоротності та непередбачуваності псевдовипадкових чисел (бітів).
14	Визначення та вимоги до випадкових послідовностей чисел(бітів).
15	Поняття та вимоги до псевдовипадкової послідовності.
16	Порівняльний аналіз властивостей випадкових та псевдовипадкових послідовностей.
17	Оцінка необоротності генераторів псевдовипадкових чисел.
18	Методи та механізми автентифікації і імітозахисту в радіосистемах, критерії та показники оцінки властивостей.
19	Модель загроз порушення справжності (автентичності).
20	Модель взаємної недовіри та взаємного захисту.
21	Особливості автентифікації в радіосистемах.
22	Критерії та показники оцінки якості імітозахисту.

8. Організація та проведення тренінгу з дисципліни “Криптографічні протоколи та методи криптоаналізу”

№п/п	Вид роботи	Порядок проведення тренінгу
1	Огляд сучасних комп’ютерних систем для реалізації криптографічних протоколів	− розгляд сучасних засобів проектування криптографічних протоколів; − вивчення можливостей проектування криптографічних протоколів в різних програмних середовищах.
2	Розгляд процесу проектування системи для генерації електронного цифрового підпису	− постановка задачі; − опис технічного завдання; − проектування схеми для генерації електронного цифрового підпису
3	Розв’язування наскрізних задач, що охоплюють усі розділи дисципліни «Криптографічні протоколи та методи криптоаналізу»	− опис наскрізної задачі; − розбиття задачі на окремі підзадачі; − об’єднання розв’язаних підзадач в єдине ціле з метою вирішення усієї задачі.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Застосування методів, засобів та алгоритмів для реалізації та дослідження криптографічних протоколів та методів криптоаналізу.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "Криптографічні протоколи та методи криптоаналізу" використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання практичних завдань;
– ректорська контрольна робота;
– комплексне практичне індивідуальне заняття (КПІЗ).

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни "Криптографічні протоколи та методи криптоаналізу" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Семестр 2 – залік %

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ)
30%	40%	30%
1. Усне опитування на заняттях: 4 заняття по 6 балів – max 24 балів. 2. Письмова робота – max 52 бали. 3. Практичне завдання: 4 практичних завдання по 6 балів – max 24 бали.	1. Усне опитування на заняттях: 4 заняття по 6 балів – max 24 бали. 2. Письмова робота – max 52 балів. 3. Практичне завдання: 4 практичних завдання по 6 балів – max 24 бали.	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Виконання завдань на тренінгах – max 30 балів

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1-15
2	Методичні вказівки до виконання практичних робіт (електронний варіант)	1–15
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-15
4	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, Nod32, FoxitReader, AdobeReader, WinRAR, WinZip, MathCAD, MatLab, DjVu Viewer, Total Commander, C#, C++, MASM32, Java Server Pages, Servlets, EJB, Java Server Faces, JavaFX,	1-15

	BC3.0, .NET Framework, PHP, Visual C++, Symbian C++, ARIS, MS Project, IBM Rational, GPSS World, Visual Web Developer 2016 Express, SWI Prolog, Microsoft Project, Spider Project, Primavera Project Planner, SQL Server 2015 Enterprise, Visio Professional 2016, Project Professional 2016, Expression Studio 2, Visual Studio 2015, Visual Studio™ 2015, Visual Studio Team System 2015	

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
3. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
4. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
5. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
6. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.
10. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
11. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
12. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С.63-71.

13. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С.65-73.

14. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.

15. Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. 2020. № 6. С. 33-39