Силабус курсу

Криптографічні протоколи та методи криптоаналізу

Ступінь вищої освіти – магістр
Освітня програма «Кібербезпека»

Дні занять: _____, _____, ауд. ____; _____, _____, ауд. ____
Консультації: _____ _____, ауд. ____

Рік навчання: I,**Семестр:** II

Кількість кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП д.т.н., професор, професор кафедри кібербезпеки **Михайло КАСЯНЧУК**

Контактна інформація kmm@wunu.edu.ua, +38 (0352) 47 50 50 *6501

Опис дисципліни

Метою дисципліни "Криптографічні протоколи та методи криптоаналізу" є формування 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.

Структура курсу

Години (лек. / сем.)	Тема	Результати навчання	**Завдання**
2 / 1	**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.	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання

2 / 1	**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.	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**Тема 7.** Протоколи, що ґрунтуються на симетричних криптосистемах.	Протокол Барроуза. Протокол Нідхема-Шредера. Протокол Kerberos. Протокол розподілу ключів по паралельних каналах.	Тести, задачі, питання
2 / 1	**Тема 8.** Протоколи, що ґрунтуються на асиметричних криптосистемах	Протокол обміну ключами Діффі-Хелмана. Триразовий протокол рукостискання. Протокол MQV (Менезес-Кью-Ванстоун).	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**Тема 10.** Протокол розподілу ключів за допомогою еліптичних кривих	Протокол Діффі-Хелмана. Опис протоколу. Приклад застосування. Приклади програмної реалізації.	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**Тема 12.** Атаки на протоколи	Класи криптоаналітичних атак. Атаки на схеми зашифрування. Пасивні атаки. Активні атаки. Пасивні шахраї. Активні шахраї. Підміна. Повторне нав’язування	Тести, задачі, питання

		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.	
2 / 1	**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».	Тести, задачі, питання
2 / 1	**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.	Тести, задачі, питання
2 / 1	**Тема 15.** Криптоаналіз асиметричних криптосистем.	Криптоаналіз асиметричних криптосистем. Криптоаналіз геш-функцій. Рішення завдання факторизації. Рішення задачі дискретного логарифма. Квантові обчислення.	Тести, задачі, питання

Літературні джерела

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.

Політика оцінювання

- **Політика щодо дедлайнів та перескладання**: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності**: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
- **Політика щодо відвідування**: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

аліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
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 студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом