Силабус курсу
КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА МЕТОДИ КРИПТОАНАЛІЗУ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Дисципліна циклу: вибіркова
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Михайло КАСЯНЧУК
Контактна інформація	kmm@wunu.edu.ua

Опис дисципліни

Метою дисципліни "Криптографічні протоколи та методи криптоаналізу" є формування у майбутніх фахівців умінь та компетенцій для забезпечення ефективного використання криптографічних протоколів та методів криптоаналізу, 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. / лаб	Тема	Результати навчання	Завдання
4/ -	Сучасні симетричні та асиметричні криптосистеми	Характеризують основні принципи симетричного й асиметричного шифрування. Пояснюють особливості алгоритмів (AES, DES, RSA, ECC тощо). Порівнюють переваги й недоліки різних типів криптосистем у практичних застосуваннях.	Поточне опитування
2 / 2	Поняття криптографічних протоколів. Їх опис.	Визначають сутність криптографічних протоколів і їх роль у забезпеченні безпеки. Уміють описувати структуру та етапи виконання протоколів. Розрізняють основні завдання, які реалізуються криптографічними протоколами (автентифікація, обмін ключами, підпис).	Поточне опитування

2 / -	Класифікація криптографічних протоколів.	Описують критерії класифікації протоколів (за завданням, моделлю обміну, криптографічною основою). Розрізняють протоколи автентифікації, розподілу ключів, підпису, шифрування та інші. Вміють наводити приклади протоколів для кожного класу.	Поточне опитування
2 / 2	Властивості, що визначають безпеку криптографічних протоколів.	Пояснюють поняття коректності, стійкості, конфіденційності, автентичності. Розуміють властивості незаперечності, стійкості до атак повторного використання, підробки та відмови. Уміють аналізувати, чи відповідає протокол вимогам безпеки.	Поточне опитування
2 / -	Аналіз та моделювання криптографічних протоколів	Використовують формальні методи опису протоколів (діаграми, моделі). Оцінюють стійкість протоколів до різних типів атак. Моделюють роботу протоколів у різних сценаріях взаємодії.	Поточне опитування
2 / 2	Протоколи електронного цифрового підпису.	Описують принцип роботи ЕЦП та його правову значущість. Аналізують популярні реалізації (RSA-PSS, DSA, ECDSA). Розуміють роль хешування та ключової інфраструктури.	Поточне опитування
2 / -	Протоколи, що ґрунтуються на симетричних криптосистемах.	Пояснюють принципи автентифікації й розподілу ключів на базі симетричного шифрування. Будують приклади протоколів (Needham–Schroeder, Kerberos). Аналізують обмеження симетричних протоколів у великих мережах.	Поточне опитування
2 / 2	Протоколи, що ґрунтуються на асиметричних криптосистемах	Розуміють роль відкритих ключів у побудові безпечних протоколів. Описують приклади протоколів (Diffie–Hellman, TLS). Пояснюють переваги асиметричних протоколів у масштабованих системах.	Поточне опитування
2 / -	Квантовий розподіл ключів.	Пояснюють принципи квантової криптографії. Описують протоколи BB84, E91 та їх реалізації. Аналізують переваги та обмеження квантового підходу.	Поточне опитування
2 / 2	Протокол розподілу ключів за допомогою	Розуміють принципи ECC та їх використання у криптографії.	Поточне опитування

	еліптичних кривих	Описують протокол ECDH та його застосування в сучасних системах. Оцінюють переваги ECC над RSA у швидкодії та безпеці.	
2 / -	Вступ до криптоаналізу. Криптоаналітичні атаки.	Визначають мету криптоаналізу та види атак. Розуміють підхід «безпеки за відсутності секретності алгоритму». Розрізняють атаки за повним текстом, відкритим текстом, вибраним текстом.	Поточне опитування
2 / 2	Атаки на протоколи	Вміють ідентифікувати вразливості в протоколах. Описують атаки «людина посередині», повторні атаки, підробку повідомлень. Оцінюють вплив цих атак на реальні системи.	Поточне опитування
2 / -	Криптоаналіз симетричних криптосистем.	Пояснюють базові методи криптоаналізу блочних і потокових шифрів. Виконують прості приклади аналізу на малих ключах і блоках. Оцінюють стійкість алгоритмів DES, AES до сучасних атак.	Поточне опитування
2 / 2	Диференційний (різницевий) криптоаналіз	Розуміють суть методу аналізу різниць у вхідних даних. Виконують приклади атаки на спрощені шифри. Усвідомлюють роль диференційного аналізу в оцінці безпеки сучасних блокових шифрів.	Поточне опитування
2 / -	Криптоаналіз асиметричних криптосистем.	Розуміють уразливості RSA, ECC, ElGamal. Описують методи факторизації та знаходження дискретного логарифма. Аналізують сучасні загрози для асиметричних алгоритмів (у т. ч. квантові атаки).	Поточне опитування

Рекомендовані джерела інформації

1. Stallings, W., & Brown, L. Computer Security: Principles and Practice (4th ed.). Pearson. 2022. 384 p.
2. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2021. – 128 p.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. 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/
5. 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.

6. 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.
7. 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.
8. 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, 2022. P. 13-36.
9. Nykolaychuk Ya.M., Yakymenko I.Z., Vozna N.Ya., and Kasianchuk M.M. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis.* 2022, Vol. 58, No. 4, P.611-618.
10. 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.
11. 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.
12. 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 і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач освіти може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне з оцінок, отриманих за виконання та захист лабораторних робіт.	Підсумкова письмова робота за темами №1-15.	Оцінка за виконання та представлення одного вибраного завдання тренінгу	Оцінка за виконаний і представлений реферат на вибрану тему.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання

За шкалою університету	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)