МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол №9/24 від 29 серпня 2024 р.)

Завідувач кафедри .

Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни
“Криптографія та безпечний комунікаційний зв’язок”,
що викладається в межах ОПП Технології штучного інтелекту в кібербезпеці
другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів 2024 р.

Назва дисципліни	Криптографія та безпечний комунікаційний зв'язок
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Трушевський Валерій Миколайович, кандидат фіз.-мат. наук, доцент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	valeriy.trushevsky@lnu.edu.ua https://ami.lnu.edu.ua/en/employee/v-m-trushevskyy; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/course/kryptohrafiia-ta-bezpechnyy-komunikatsiynyy-zv-iazok
Інформація про дисципліну	Дисципліна "Криптографія та безпечний комунікаційний зв'язок" є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається у 1-му семестрі другого (магістерського) рівня освіти в обсязі 4.5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей у галузі застосування криптографічних методів до захисту комунікаційного зв'язку, вивчення принципів побудови сучасних симетричних та асиметричних криптографічних систем, криптографічних протоколів, криптографії на еліптичних кривих та застосування на практиці для забезпечення конфіденційності інформації.
Мета та цілі дисципліни	Метою курсу є вивчення принципів побудови сучасних симетричних та асиметричних криптосистем, криптографічних протоколів, розуміння ефективності та надійності алгоритмів шифрування для подальшого їх застосування на практиці з метою захисту комунікаційного зв'язку.
Література для вивчення дисципліни	*Основна* 1. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник. – Харків: ХПІ, 2023. – 658 с. 2. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с 3. Стасюк М. Елементи математичних основ криптографії : навчальний посібник – Львів : ЛДУ БЖД, 2021. – 216 с.

4. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с.
5. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. – 943 p.
6. David Wong. Real-World Cryptography, Version 12, 2021 – 369 p.

Додаткова

7. Вербіцький О.В. Вступ до криптології. Львів, 1998 – 247с.
8. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце у сучасному суспільстві, Одеса, 2003. – 80 с.
9. Корченко О. Г. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.
10. Остапов С. Е., Валь Л.О. Основи криптографії: Навчальний посібник. – Чернівці: Книги – XXI, 2008. – 188 с.
11. Фільштінський В. А.,Бережний А. В. – Суми: Сумський державний університет, 2011. – 138 с.
12. Douglas R. Stinson. Introduction to modern cryptography. Second Edition. 2015. – 576 p.
13. Douglas R. Stinson, Maura B. Paterson. Cryptography. Theory and Practice. Fourth Edition, 2019. – 580 p.
14. Bruce Schneier. Applied cryptography, second edition, protocols, algorithms, and source code in C, 2015. – 792 p.
15. Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger. A Course in Mathematical Cryptography, 2015. – 376 p.
16. Alko R. Meijer. Algebra for Cryptologists, 2016. – 301 p.
17. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2014. – 538 p.
18. Nigel P. Smart. Cryptography Made Simple, 2016. – 481 p.
19. Christof Paar · Jan Pelzl. Understanding Cryptography. A Textbook for Students and Practitioners, 2010. – 372 p.

Рекомендовані онлайн курси

20. https://www.coursera.org/learn/crypto
21. https://www.coursera.org/learn/crypto2
22. https://www.udacity.com/course/applied-cryptography--cs387
23. https://www.udemy.com/course/learn-modern-security-and-cryptography-by-coding-in-python/
24. https://www.udemy.com/course/conversation-on-cryptography-a-total-course-w-mike-meyers/
25. https://www.udemy.com/course/cryptography-learn-public-key-infrastructure-or-pki-from-scratch/
26. https://www.udemy.com/course/cryptography-past-present-and-future/
27. https://www.udemy.com/course/encryption-and-cryptography-for-professionals/

Обсяг курсу	Загальний обсяг: 135 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 71 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - принципи побудови сучасних симетричних криптосистем; - потокові шифри та генератори псевдовипадкових бітів; - асиметричні криптосистеми: RSA, ElGamal, Rabin, Diffie-Hellman; - еліптичні криптоситеми; - імовірнісне криптування; - електронний цифровий підпис: RSA, DSA, ElGamal; - мережеві криптографічні протоколи SSL/mTLS/TLS/SSH; - протоколи аутентифікації та ідентифікації; - керування ключами PKI; **вміти:** - застосовувати різні типи криптографічних систем в залежності від задачі; - використовувати бібліотеку OpenSSL; - створювати SSL сертифікати; - використовувати різні схеми електронного цифрового підпису; - шифрувати конфіденційні дані стандартними алгоритмами шифрування; - здійснювати проектування (розробку) систем, технологій і засобів захисту комунікаційного зв'язку при здійсненні професійної діяльності.
Ключові слова	Генератори псевдовипадкових бітів, асиметрична криптосистема, симетрична криптосистема, блокові шифри, потокові шифри, криптосистема з відкритим ключем, еліптичні криві, цифровий підпис, цифровий сертифіка, цифрова валюта, DSA, RSA, Diffie-Hellman, ElGamal, SSL/TLS/mTLS/SSH, OpenSSL, ECDSA, EdDSA
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Моделі та методи дискретної математики; 2) Застосування дискретної математики в криптології; 3) Обчислювальна геометрія та алгебра; 4) Програмування; 6) Застосування теорії ймовірностей в кібербезпеці; 7) Основи кібербезпеки; 8) Основи криптології.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Індивідуальні завдання
Необхідне обладнання	Лабораторія з обладнаними робочими станціями, з'єднаними в комп'ютерну мережу. IDE для програмування мовою C++, C#, Python або Java.

Критерії оцінювання (окремо для кожного виду навчальної діяльності)

Оцінювання проводиться за 100-бальною шкалою. 70 балів нараховують за виконання 7 лабораторних завдань та 30 балів – за оволодіння теоретичним матеріалом курсу (2 модульні контролі по 15 балів)

Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.

Література. Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.

Політика виставлення балів. Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.

Критерії оцінювання знань студентів	**Бали рейтингу**	**Макс. к-сть балів**
1. Бали поточної успішності за виконання індивідуальних завдань		
Критерії оцінювання (7*10 бали)	**70 балів**	
Студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час захисту індивідуальних завдань, глибоко та всебічно розкриває зміст теоретичних питань. Реалізоване програмне забезпечення пройшло перевірку на плагіат та повністю виконує умову завдання.	**10**	
Студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час захисту індивідуальних завдань, в основному розкриває зміст теоретичних питань. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації. Реалізоване програмне забезпечення містить окремі несуттєві неточності та незначні помилки.	**9-5**	
Студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час захисту лабораторного завдання, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності, програмна реалізація індивідуального завдання частково виконана.	**4-1**	

Студент не виконав індивідуальне завдання та не володіє матеріалом.	**0**
2. Модульний контроль	
Критерії оцінювання (2*15 бали)	**30**
Протягом семестру проводиться **2 модульних контролі**. Кожен модуль містить **15 тестових питань.**	
***Критерії оцінювання вирішення тестів (15*1 бали)*:**	
Відповідь вірна	**1**
Відповідь невірна	**0**
Загальна кількість балів по завершенні вивчення дисципліни	**100**

Додаткові бали / або зарахування певних тем можна отримати за результатами **неформального та/або інформального навчання за** тематикою даної дисципліни. Визнання та зарахування результатів такого навчання відбувається у відповідності до наданих документів про неформальне та/або інформальне навчання.
Жодні форми порушення академічної доброчесності не толеруються.

Питання до модульних контролів

1. Сучасні блокові шифри. Шифри підстановки та транспозиції. Блокові шифри як групові математичні перестановки. Компоненти сучасного блокового шифру.
2. Складені шифри. Розсіювання та перемішування. Раунди. Два класи складених шифрів.
3. Атаки на блокові шифри. Диференціальний та лінійний криптографічні аналізи.
4. Принципи побудови шифру ГОСТ 28147-89.
5. Принципи побудови шифру DES. Подвійний та потрійний DES.
6. Принципи побудови шифру AES. Аналіз та безпека Шифру AES.
7. Режими шифрування блокових шифрів: ECB, CBC, PCBC, CFB, OFB, CRT, GCM
8. Національний стандарт шифрування “Калина” (ДСТУ 7624:2014)
9. Загальні відомості про потокові шифри.
10. Генератори псевдовипадкових чисел: лінійний конгруентний генератор, метод Фібоначчі з запізненням, генератор BBS, генератор на основі регістрів зсуву.
11. Потоковий шифр A5. Криптографічна стійкість потокового шифру A5.
12. Потоковий шифр RC4. Криптографічна стійкість потокового шифру RC4.
13. Потокові шифри WEP 802.11b, WPA 802.11i, WPA2, WPA3.
14. Принцип побудови сучасних потокових шифрів eStream.
15. Потоковий шифр “Струмок”.
16. Криптосистеми з відкритим ключем. Концепція. Ефективність. Надійність.
17. Алгоритм рюкзака Merkle–Hellman.
18. Криптосистема RSA. Коректність, ефективність, надійність.
19. Протокол обміну ключем Diffie-Hellman.
20. Криптосистема ElGamal.
21. Еліптичні криптосистеми. Операції над точками еліптичних кривих.
22. Алгоритм Діффі-Хелмана на еліптичних кривих.
23. Криптографічні хеш функції: основні властивості, принцип роботи.
24. Криптографічні хеш функції: Парадокс днів народжень.
25. Стандарт цифрового підпису ECDSS
26. Цифровий підпис на основі RSA.
27. Стандарт цифрового підпису DSS.
28. Цифровий підпис на основі ElGamal.
29. Протоколи ідентифікації та аутентифікації.
30. Мережеві криптографічні протоколи mTLS/TLS.
31. Криптографічний протокол SSH.
32. Цифровий сертифікат. Інфраструктура відкритих ключів PKI.

	33. Використання бібліотеки OpenSSL для генерації ключів та сертифікатів.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1-2	**Тема 1. Сучасні блокові шифри. Принципи побудови шифрів Фейстеля (DES та ГОСТ 28147-89).** (Шифри підстановки та транспозиції. Блокові шифри як групові математичні перестановки. Компоненти сучасного блокового шифру. Складені шифри. Розсіювання та перемішування. Раунди. Два класи складених шифрів. Атаки на блокові шифри, ГОСТ 28147-89, Подвійне та потрійне шифрування DES. Режими зв'язування блоків: ECB, CBC, PCBC, CFB, OFB, CRT)	лекція, самостійна робота	[1-6]	4 10	2 тижні
		лаб.	[1-6]	4	
3	**Тема 2. Шифри не Фейстеля, AES.** (Математичні основи побудови алгоритму AES, структура раундів, програмна реалізація шифрування, дешифрування AES, режими зв'язування блоків: ECB, CBC, PCBC, CFB, OFB, CRT, GCM)	лекція, самостійна робота		2 5	1 тиждень
		лаб.	[1-6]	2	
4	**Тема 3. Атаки на блокові шифри.** (Диференціальний та лінійний криптографічні аналізи, аналіз та безпека шифру AES. Використання криптографічної бібліотеки для шифрування використовуючи різні режими AES, порівняння режимів шифрування CBC та ECB на прикладі шифрування зображень.)	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
5	**Тема 4. Національний стандарт шифрування "Калина" (ДСТУ 7624:2014)** (Основні характеристики. Ключі та кількість раундів. Схеми шифрування та дешифрування. Псевдокод процедури шифрування "Калина", розгортання ключів, Порівняння з шифром AES. Режими роботи "Калина")	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
6-7	**Тема 5. Потокові шифри та генератори псевдовипадкових чисел.** (Властивості ГПВЧ, лінійний конгруентний генератор, метод Фібоначчі з запізненням, генератор BBS, генератор на основі регістрів зсуву. Синхронні та самосихронізуючі потокові шифри, потокові шифри A5, A5/1, A5/2, A5/3, RC4, CSS, WEP 802.11b, WPA 802.11i, WPA2, WPA3)	лекція, самостійна робота	[1-6]	4 10	2 тижні
		лаб.	[1-6]	4	

8	**Тема 6. Сучасні потокові шифри eStream. Потоковий шифр “Струмок”(ДСТУ 8845:2019).** (Потокові шифри: Salsa 20, Snow 2.0, Snow 3G, Sosemanuk, Trivium, Grain. Специфікація алгоритму шифрування “Струмок”, базові компоненти шифру. Порівняльний аналіз результатів оцінки швидкодії потокових та блокових шифрів)	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
9-10	**Тема 7. Асиметричні криптосистеми.** (Основні завдання, односторонні функції, проблеми симетричних криптосистем, концепція криптосистем з відкритим ключем. Криптосистема Меркла-Хелмана, протокол обміну ключем Діффі-Геллмана, RSA, знаходження таємного ключа RSA, коректність, ефективність, надійність, схема Ель-Гамаля, криптосистема Рабіна, Імовірнісне криптування на основі RSA)	лекція, самостійна робота	[1-6]	4 7	2 тижні
		лаб.	[1-6]	4	
11	**Тема 8. Основи криптографії на еліптичних кривих.** (Арифметичні операції в скінченному полі Галуа $G(2^8)$, Операції над точками еліптичних кривих. Алгоритм Діффі-Хелмана на еліптичних кривих. Стандарт цифрового підпису ECDSS)	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
12	**Тема 9. Криптографічні хеш-функції. Цілісність даних та аунтефікація повідомлень.** (Основні властивості. Принцип роботи криптографічних хеш-функцій. Парадокс днів народжень. Захист від колізій. Дайджест повідомлення.)	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
13	**Тема 10. Цифровий підпис. Алгоритми цифрового підпису.** (Схема цифрового підпису. Алгоритм цифрового підпису RSA. Цифровий підпис Ель-Гамаля. Стандарт цифрового підпису DSS. Генерування ключа, підписування і верифікація. Класифікація атак на схеми цифрового підпису. Особливі схеми цифрового підпису. Стандарт цифрового підпису ECDSS. Електронні гроші.)	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
14	**Тема 11. Протоколи ідентифікації та аутентифікації.** (Аунтефікація на основі паролю. Атаки. Встановлення аутентичності на основі запиту-відповіді на основі використання симетричного шифру, функцій ключового хешування, асиметричного шифру, цифрового підпису. Підтвердження з нульовим розголошенням. Протокол Фіата-Шаміра. Протокол Фуйге-Фіата-Шаміра. Протокол Кіскатера-Гійу. Біометрична аутентифікація.)	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
15	**Тема 12. Криптографічні мережеві протоколи mTLS/TLS/SSL/SSH.** **(**Схеми роботи протоколів mTLS та TLS. Вдосконалення версій протоколів TLS 1.1 – TLS 1.3**)**	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	

16	**Тема 13. Сертифікати. Інфраструктура відкритих ключів PKI.** **(**Структура та типи сертифікатів, генерування сертифікатів та ключів за допомогою бібліотеки OpenSSL. Центр розподілу ключів. Інфраструктура відкритих ключів. Режими роботи.**)**	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	