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 № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни "Прикладна криптологія", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Прикладна криптологія**
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	Хохлачова Юлія Євгенівна, кандидат техн. наук, професор кафедри кібербезпеки, Трушевський Валерій Миколайович, кандидат фіз.-мат. наук, доцент кафедри кібербезпеки
Контактна інформація викладачів	yuliia.khokhlachova@lnu.edu.ua https://ami.lnu.edu.ua/employee/khokhlachova-yu-ye 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/prykladna-kryptolohiia-kb
Інформація про дисципліну	Дисципліна “Прикладна криптологія” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 5-му семестрі в обсязі 7-х 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 інформації, вивчення принципів побудови сучасних симетричних та асиметричних криптографічних систем шифрування, криптографічних протоколів та їх застосування на практиці для забезпечення конфедиційності інформації.
Мета та цілі дисципліни	Метою курсу є вивчення принципів побудови сучасних симетричних та асиметричних криптосистем, розуміння ефективності та надійності алгоритмів шифрування для подальшого їх застосування на практиці з метою захисту інформації.
Література для вивчення дисципліни	*Основна* 1. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації: підручник – К.: ЦП «Компринт», 2021. – 296 с. 2. Гаврилова А.А., Хохлачова Ю.Є., Погорелов В.В. Аналіз застосування гібридних криптокодових конструкцій для підвищення рівня стійкості геш-кодів до злому: стаття - Безпека інформації. Том 28 № 2 (2022). С. 87-101.

3. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник. – Харків: ХПІ, 2023. – 658 с.
4. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с
5. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник – К.: НАУ, 2023. – 312.
6. Стасюк М. Елементи математичних основ криптографії : навчальний посібник – Львів : ЛДУ БЖД, 2021. – 216 с.
7. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с.
8. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. – 943 p.
9. David Wong. Real-World Cryptography, Version 12, 2021 – 369 p.

Додаткова

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

Рекомендовані онлайн курси

23. https://www.coursera.org/learn/crypto
24. https://www.coursera.org/learn/crypto2

	25. https://www.udacity.com/course/applied-cryptography--cs387 26. https://www.udemy.com/course/learn-modern-security-and-cryptography-by-coding-in-python/ 27. https://www.udemy.com/course/conversation-on-cryptography-a-total-course-w-mike-meyers/ 28. https://www.udemy.com/course/cryptography-learn-public-key-infrastructure-or-pki-from-scratch/ 29. https://www.udemy.com/course/cryptography-past-present-and-future/ 30. https://www.udemy.com/course/encryption-and-cryptography-for-professionals/
Обсяг курсу	Загальний обсяг: 210 годин. Аудиторних занять: 80 год., з них 32 год. лекцій та 48 год. лабораторних робіт. Самостійної роботи: 130 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - принципи побудови сучасних симетричних криптосистем (AES, Калина); - потокові шифри та генератори псевдовипадкових бітів; - асиметричні криптосистеми: RSA, ElGamal, Rabin, Diffie-Hellman; - еліптичні криптоситеми; - електронний цифровий підпис: RSA, DSA, ElGamal; - Пртоколи ідентифікації та аунтефікації; - протокол передачі даних SSL/TLS; - сертифікати та керування ключами, моделі PKI **вміти:** - застосовувати різні типи криптографічних систем в залежності від задачі; - використовувати бібліотеку OpenSSL; - використовувати різні схеми електронного цифрового підпису; - шифрувати конфіденційні дані стандартними алгоритмами шифрування; - здійснювати проектування (розробку) систем, технологій і засобів кіберзахисту при здійсненні професійної діяльності. **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КЗ 7, КФ 1, КФ 5, КФ 7, КФ 9, КФ 10; та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 7, ПРН 8, ПРН 9, ПРН 16, ПРН 22, ПРН 27, ПРН 31, ПРН 33, ПРН 34, ПРН 44, ПРН 45, ПРН 46, ПРН 47, ПРН 48.**
Ключові слова	Генератори псевдовипадкових бітів, асиметрична криптосистема, симетрична криптосистема, блокові шифри, потокові шифри, криптосистема з відкритим ключем, цифровий підпис, цифровий сертифіка, цифрова валюта, A5, DES, DSS, RSA, Diffie-Hellman, ElGamal, RSA, SSL/TLS/mTLS, OpenSSL, ECDSS, eStream, WEP, WPA.
Формат курсу	Очний
Теми	Теми подані у схемі курсу нижче
Підсумковий контроль, форма	Іспит 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) Математичні основи криптографії.
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. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **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 незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття 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 практичного 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.
Питання до іспиту	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 DES. Подвійний та потрійний DES. 5. Принципи побудови шифру AES. Аналіз та безпека Шифру AES. 6. Національний стандарт шифрування "Калина" (ДСТУ 7624:2014) 7. Загальні відомості про потокові шифри.

	8. Генератори псевдовипадкових чисел: лінійний конгруентний генератор, метод Фібоначчі з запізненням, генератор BBS, генератор на основі регістрів зсуву. 9. Потоковий шифр A5. Криптографічна стійкість потокового шифру A5. 10. Потоковий шифр RC4. Криптографічна стійкість потокового шифру RC4. 11. Потокові шифри WEP 802.11b, WPA 802.11i, WPA2, WPA3. 12. Принцип побудови сучасних потокових шифрів eStream. 13. Потоковий шифр “Струмок”. 14. Криптосистеми з відкритим ключем. Концепція. Ефективність. Надійність. 15. Алгоритм рюкзака Merkle–Hellman. 16. Криптосистема RSA. Коректність, ефективність, надійність. 17. Протокол обміну ключем Diffie-Hellman. 18. Криптосистема ElGamal. 19. Еліптичні криптосистеми. Операції над точками еліптичних кривих. 20. Алгоритм Діффі-Хелмана на еліптичних кривих. 21. Стандарт цифрового підпису ECDSS 22. Цифровий підпис на основі RSA. 23. Стандарт цифрового підпису DSS. 24. Цифровий підпис на основі ElGamal. 25. Протоколи ідентифікації та аутентифікації. 26. Криптографічні протоколи mTLS/TLS 27. Цифровий сертифікат. Інфраструктура відкритих ключів PKI 28. Використання бібліотеки OpenSSL для генерації ключів та сертифікатів
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література**	**Завдання, год.**	**Термін виконання**
1	**Тема 1. Принципи побудови сучасних симетричних криптографічних систем** (Компоненти сучасного блокового шифру, Розсіювання та перемішування, атаки на блокові шифри. Шифрування DES)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень
2	**Тема 1. Принципи побудови сучасних симетричних криптографічних систем. Режими шифрування.** (Режими зв’язування блоків: ECB, CBC, PCBC, CFB, OFB, CRT, GCM)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
3	**Тема 2. Шифри не Фейстеля, AES.** (Математичні основи побудови алгоритму AES, структура раундів, аналіз та безпека шифру)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень

4	**Тема 2. Шифри не Фейстеля, AES.** (Використання криптографічної бібліотеки для шифрування використовуючи різні режими AES, порівняння режимів шифрування CBC та ECB на прикладі шифрування зображень)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
5	**Тема 3. Національний стандарт шифрування "Калина" (ДСТУ 7624:2014)** (Основні характеристики. Ключі та кількість раундів. Схеми шифрування та дешифрування)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень
6	**Тема 3. Національний стандарт шифрування "Калина" (ДСТУ 7624:2014)** (Порівняння з шифром AES. Режими роботи "Калина")	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
7	**Тема 4. 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 лаб.	[1-10]	2 8 2	1 тиждень
8	**Тема 4. Потокові шифри та генератори псевдовипадкових чисел.** (Потокові шифри WEP 802.11b, WPA 802.11i, WPA2, WPA3)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
9	**Тема 5. 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)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень
10	**Тема 5. Сучасні потокові шифри eStream. Потоковий шифр "Струмок"(ДСТУ 8845:2019).** (Порівняльний аналіз результатів оцінки швидкодії потокових та блокових шифрів.)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
11	**Тема 6. 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)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень

12	**Тема 6. Асиметричні криптосистеми.** (Застосування криптосистеми RSA для обміну зашифрованими файлами, порівняльний аналіз симетричних та асиметричних криптосистем)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
13	**Тема 7. 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. Електронні гроші.)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень
14	**Тема 8. Основи криптографії на еліптичних кривих.** (Операції над точками еліптичних кривих. Алгоритм Діффі-Хелмана на еліптичних кривих. Стандарт цифрового підпису ECDSS)	лекція, самостійна робота лаб.	[1-10]	2 8 4	1 тиждень
15	**Тема 9. Протоколи ідентифікації та аутентифікації.** (Аутентифікація на основі паролю. Встановлення аутентифікації на основі запиту-відповіді на основі використання симетричного шифру, функцій ключового хешування, асиметричного шифру, цифрового підпису, біометрична аутентифікація)	лекція, самостійна робота лаб.	[1-10]	2 8 2	1 тиждень
	Тема 10. Криптографічні протоколи mTLS/TLS/SSL. **(**Схеми роботи протоколів mTLS та TLS. Вдосконалення версій протоколів TLS 1.1 – TLS 1.3**)**	лаб.	[1-10]	2	
16	**Тема 11. 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 лаб.	[1-10]	2 10 2	1 тиждень