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 № від 2023 р.)

Завідувач кафедри .
Венгерський П.С.

Силабус з навчальної дисципліни "Криптографія та безпечний комунікаційний зв'язок", що викладається в межах ОПП Кібербезпека другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека

Львів 2023 р.

Назва дисципліни	Криптографія та безпечний комунікаційний зв'язок
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
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
Викладачі дисципліни	Трушевський Валерій Миколайович, доцент кафедри кібербезпеки
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 в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна "Криптографія та безпечний комунікаційний зв'язок" є вибірковою дисципліною з спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається у IX-му семестрі в обсязі 4-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 комунікаційного зв'язку, вивчення принципів побудови сучасних симетричних та асиметричних криптографічних систем, криптографічних протоколів, криптографії на еліптичних кривих та застосування на практиці для забезпечення конфедиційності 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	1. Берегуляк І.Я. Класичні методи криптування. Львівський університет, 1997. 2. Вербіцький О.В. Вступ до криптології. Львів, 1998. 3. Гапак О. М. Криптоаналіз. Криптографічні протоколи. Ужгород, 2021. 4. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце у сучасному суспільстві, Одеса, 2003. 5. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування, Житомир, 2014.

	6. Козіна Г.Л. Криптографія від історії до сучасних стандартів, Запоріжжя, 2020 7. Остапов С.Е., Валь Л.О. Основи Криптографії, Чернівці, 2008. 8. Щур Н.О., Покотило О.А. Основи криптології, Житомир, 2021. 9. Фільштінський В.А., Бережний А.В. Математичні основи криптографії, Суми, 2011. 10. державний університет, 2011. – 138 с. 11. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. 12. Douglas R. Stinson, Maura B. Paterson. Cryptography. Theory and Practice. Fourth Edition, 2019. 13. David Wong. Real-World Cryptography, Version 12, 2021. 14. Douglas R. Stinson. Introduction to modern cryptography. Second Edition. 2015. 15. Bruce Schneier. Applied cryptography, second edition, protocols, algorithms, and source code in C, 1996. 16. Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger. A Course in Mathematical Cryptography, 2010. 17. Alko R. Meijer. Algebra for Cryptologists, 2016. 18. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2014. 19. Nigel P. Smart. Cryptography Made Simple, 2016. 20. Christof Paar · Jan Pelzl. Understanding Cryptography. A Textbook for Students and Practitioners, 2010. **Онлайн курси** 1. https://www.coursera.org/learn/crypto 2. https://www.coursera.org/learn/crypto2 3. https://www.udacity.com/course/applied-cryptography--cs387 4. https://www.udemy.com/course/learn-modern-security-and-cryptography-by-coding-in-python/ 5. https://www.udemy.com/course/conversation-on-cryptography-a-total-course-w-mike-meyers/ 6. https://www.udemy.com/course/cryptography-learn-public-key-infrastructure-or-pki-from-scratch/ 7. https://www.udemy.com/course/cryptography-past-present-and-future/ 8. https://www.udemy.com/course/encryption-and-cryptography-for-professionals/
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - принципи побудови сучасних симетричних криптосистем. AES; - потокові шифри та генератори псевдовипадкових бітів; - асиметричні криптосистеми: RSA, ElGamal, Rabin, Diffie-Hellman; - еліптичні криптоситеми; - імовірнісне криптування; - електронний цифровий підпис: RSA, DSA, ElGamal;

	- принципи побудови цифрової валюти; - протоколи аунтефікації та ідентифікації; - керування ключами; - протокол передачі даних SSL/TLS **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. **Курс забезпечує набуття таких компетентностей: КЗ 1, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КФ 1, КФ 2, КФ 5, КФ 9, КФ 10; та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 6, ПРН 7, ПРН 13, ПРН 14, ПРН 23, ПРН 26, ПРН 27, ПРН 28, ПРН 31, ПРН 34, ПРН 47.**		
Ключові слова	Генератори псевдовипадкових бітів, асиметрична криптосистема, симетрична криптосистема, блокові шифри, потокові шифри, криптосистема з відкритим ключем, цифровий підпис, цифровий сертифіка, цифрова валюта, DSA, RSA, Diffie-Hellman, ElGamal, SSL/TLS, OpenSSL, ECDSA, EdDSA		
Формат курсу	Змішаний Проведення лекцій, лабораторних робіт і консультацій.		
Теми	**Теми**	**Лек.**	**Лаб.**
	Модуль 1		
	Змістовий модуль 1. Принципи побудови сучасних симетричних криптографічних систем		
	1. Сучасні блокові шифри. Шифри підстановки та транспозиції. Блокові шифри як групові математичні перестановки. Компоненти сучасного блокового шифру	1	
	2. Складені шифри. Розсіювання та перемішування. Раунди. Два класи складених шифрів	2	
	3. Атаки на блокові шифри. Диференціальний криптографічний аналіз.	1	2
	4. Лінійний криптографічний аналіз	1	2
	5. Принципи побудови алгоритму AES	2	2
	6. Аналіз та безпека Шифру AES	2	2
	Змістовий модуль 2. Потокові шифри та генератори псевдовипадкових бітів		
	1. Загальні відомості про потокові шифри	2	
	2. Принципи використання генераторів псевдовипадкових чисел під час потокового шифрування	1	2
	3. Потоковий шифр A5	1	
	4. Криптографічна стійкість потокового шифру A5	1	2
	5. Потоковий шифр RC4	1	2
	6. Криптографічна стійкість потокового шифру RC4	1	2
	Разом за модуль 1	**16**	**16**
	Модуль2		
	Змістовий модуль 3. Асиметричні криптографічні системи шифрування		

	1. Криптосистеми з відкритим ключем. Концепція. Ефективність. Надійність	1	
	2. Алгоритм рюкзака Merkle–Hellman		1
	3. Криптосистема RSA. Коректність, ефективність, надійність.	1	2
	4. Протокол обміну ключем Diffie-Hellman	1	
	5. Криптосистема Шаміра	1	1
	6. Криптосистема ElGamal	1	1
	7. Криптосистема Rabin	1	1
	8. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні	1	1
	9. Імовірнісне криптування на основі RSA	1	1
	10. Еліптичні криптосистеми. ECIES	1	
	11. Криптографічні хеш-функції	1	
	Змістовий модуль 4. Застосування сучасних криптосистем		
	1. Цифровий підпис на основі RSA	1	
	2. Цифровий підпис на основі DSA	1	1
	3. Цифровий підпис на основі ElGamal		1
	4. Система Шнора	1	1
	5. ECDSA (Elliptic Curve Digital Signature Algorithm)	1	
	6. Цифровий підпис на основі Rabin		1
	7. EdDSA (Edwards-curve Digital Signature Algorithm)		1
	8. Цифровий підпис на основі ElGamal		1
	9. Криптографічні протоколи		
	10. Застосування криптографічних систем на прикладі протоколу SSL/TLS. Цифровий сертифікат	1	
	11. Бібліотека OpenSSL	1	2
	Разом за модуль 2	**16**	**16**
	Разом	**32**	**32**
Підсумковий контроль, форма	Залік у кінці семестру		
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Лабораторні роботи		
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 • залік: 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 екзамену	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. 4. Диференціальний криптографічний аналіз. 5. Лінійний криптографічний аналіз. 6. Принципи побудови алгоритму AES. 7. Аналіз та безпека Шифру AES. 8. Загальні відомості про потокові шифри. 9. Принципи використання генераторів псевдовипадкових чисел під час потокового шифрування. 10. Потоковий шифр A5. 11. Криптографічна стійкість потокового шифру A5. 12. Потоковий шифр RC4. 13. Криптографічна стійкість потокового шифру RC4. 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 Шаміра. 19. Криптосистема ElGamal. 20. Криптосистема Rabin. 21. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні. 22. Імовірнісне криптування на основі RSA. 21. Еліптичні криптосистеми. ECIES. 22. Цифровий підпис на основі RSA. 23. DSA. 24. Цифровий підпис на основі ElGamal. 25. Система Шнора. 26. ECDSA (Elliptic Curve Digital Signature Algorithm). 27. Цифровий підпис на основі Rabin. 28. EdDSA (Edwards-curve Digital Signature Algorithm). 29. Цифровий підпис на основі ElGamal. 30. Застосування криптографічних систем на прикладі протоколу SSL/TLS. Цифровий сертифікат. 31. Захист даних на диску. 32. Цифрова валюта. 33. Бібліотека OpenSSL. 34. Криптографічні хеш-функції.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.