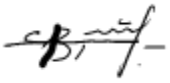
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

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 _____П.С.Венгерський

Силабус з навчальної дисципліни "Криптографічний аналіз", 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	**Криптографічний аналіз**
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/employee/trushevskyj-v-m 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/kryptohrafichnyy-analiz-kb
Інформація про дисципліну	Дисципліна “Криптографічний аналіз” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 8-му семестрі в обсязі 6-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетнтностей у галузі криптографічного аналізу, вивчення теоретичних та практичних основ щодо впровадження криптоаналітичних атак на шифри та виявленню їх вразливостей. Розглядаються поняття умовної та безумовної стійкості, теорія секретного зв’язку К. Шеннона, методи оцінки крипостійкості, основні принципи криптоаналізу симетричних та асиметричних криптосистем, вимоги щодо реалізації сучасних криптоалгоритмів.
Мета та цілі дисципліни	Метою курсу є вивчення базових принципів та методів проведення криптоаналізу, допоміжних методів та алгоритмів криптоаналізу, вміння застосовувати математичні методи для знаходження вразливостей криптосистем, оцінювати їх стійкість до різного виду криптоатак.
Література для вивчення дисципліни	*Основна* 1. Гапак О.М. Криптоаналіз. Криптографічні протоколи: посібник – Ужгород, 2021. – 93 с. 2. Гапак О.М., Балога С.І. Захист інформації в комп’ютерних системах: підручник.- Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021. – 184 с. 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. Стасюк М. Елементи математичних основ криптографії : навчальний посібник – Львів : ЛДУ БЖД, 2021. – 216 с.

	5. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120с. 6. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, 2020. – 943 p. 7. David Wong. Real-World Cryptography, Version 12, 2021 – 369 p. 8. Petrenko A. Applied Quantum Cryptanalysis, 2023 – 182 p. *Додаткова* 9. Вербіцький О.В. Вступ до криптології. Львів, 1998 – 247с. 10. Корченко О. Г. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. 11. Фільштінський В. А.,Бережний А. В. Математичні основи криптографії: конспект лекцій – Суми: Сумський державний університет, 2011. – 138 с. 12. Biham E. Differential Cryptanalysis of the Data Encryption Standard, 2011. – 197 p. 13. Becheikh R. Design and cryptanalysis of stream and block ciphers, 2019. – 180 p. 14. Douglas R. Stinson. Introduction to modern cryptography. Second Edition. 2015. – 576 p. 15. Douglas R. Stinson, Maura B. Paterson. Cryptography. Theory and Practice. Fourth Edition, 2019. – 580 p. 16. Schneier B. Applied cryptography, second edition, protocols, algorithms, and source code in C, 2015. – 792 p. 17. Stamp M., Low R. Applied Cryptanalysis: Breaking Ciphers in the Real World, 2007 – 422 p. 18. Swenson C. Modern Cryptanalysis: Techniques for Advanced Code Breaking. 1st Edition, 2008. – 264 p. 19. Xie T., Liu F. Differential Cryptanalysis on Hash Functions:Theory and Practice: Attack algorithms and source codes in visual C++, 2014. – 384 p. 20. Yan Y. Cryptanalytic Attacks on RSA, 2007. – 275 p.
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 110 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - математичні моделі шифрів та підходи до визначення їх надійності; - основні принципи криптоаналізу; - умовна та безумовна стійкість криптосистем; - класифікації атак на криптосистеми; - універсальні методи криптоаналізу; - допоміжні методи криптоаналізу - криптоаналіз класичних шифрів - криптоаналіз блокових шифрів (лінійний та диференціальний) - методи криптоаналізу сучасних потокових шифрів;

	- криптоаналіз асиметричних криптосистем - криптоаналіз геш-функції (Birthday paradox). - застосування нових технологій до криптоаналізу (нейронні мережі, генетичні алгоритми, квантові комп'ютери). **вміти:** - застосовувати основні методи криптоаналізу до розкриття шифрів; - оцінювати стійкість криптографічних алгоритмів; - проводи криптоаналіз зашифрованої інформації; - досліджувати слабкі та сильні сторони шифрів; - розв'язувати задачі криптоаналізу; - оцінювати ступінь програмних та апаратних засобів захисту інформації. **Курс забезпечує набуття таких компетентностей: 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 36, ПРН 37, ПРН 38, ПРН 40, ПРН 44, ПРН 45, ПРН 46, ПРН 47, ПРН 48.**
Ключові слова	Криптологія, криптографія, криптоаналіз, асиметрична криптосистема, симетрична криптосистема, класичні криптографічні алгоритми, статистичний криптоаналіз, частотний криптоаналіз, лінійний криптоаналіз, диференційний криптоаналіз, ймовірнісний криптоаналіз, умовна та безумовна стійкість, тести простоти, обчислювальна складність.
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; 9) Прикладна криптологія.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Індивідуальні завдання
Необхідне обладнання	Лабораторія з обладнаними робочими станціями. 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 • лабораторні роботи: 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 контролю	1. Задачі криптоаналізу. Криптографічна стійкість. Принцип Кергофа. 2. Методи класичного криптоаналізу. Криптоаналіз шифрів простої заміни. 3. Криптоаналіз поліалфавітних шифрів. Криптоаналіз Казискі. 4. Криптоаналіз шифру Віженера. Перший та другий методи Фрідмана. 5. Роторні криптосистеми. Криптоаналіз шифру Enigma. 6. Криптоаналіз афінних шифрів. 7. Основи теорії секретного зв'язку К. Шеннона. Поняття семантичної та безумовної стійкості. 8. Показати що шифр Віженера не є семантично стійким. 9. Ідеальна секретність. Вразливість шифру Two Times Pad. 10. Методи криптоаналізу потокових шифрів. 11. Криптостійкість шифру "Струмок". 12. Кореляційний криптоаналіз. 13. Криптоаналіз на основі регістрів зсуву. 14. Криптоаналіз блокових шифрів. 15. Лінійний та диференціальний криптоаналіз. 16. Важко розв'язні задачі. Задача факторизації. Алгоритм Полларда. 17. Важко розв'язні задачі. Задача дискретного логарифму. 18. Важко розв'язні задачі. Добування квадратного кореня за простим модулем. 19. Тестування простоти. Ймовірнісний тест Соловея-Штрассена. 20. Тестування простоти. Ймовірнісний тест Міллера-Рабіна. 21. Тест простоти Люка. 22. Криптоаналіз асиметричних систем. Атаки на RSA. 23. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні. 24. Елементи криптоаналізу геш-функцій. Парадокс днів народжень. Захист від колізій

	25. Основні види атак та загроз цифрового підпису. 26. Атаки на слабкі підписи. Атака на алгоритм підпису ЕльГамаля. 27. Еліптичні криптосистеми та їх стійкість. 28. Використання нових технологій у криптоаналізі.
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. Криптоаналіз. Основні поняття та приклади.** (Історія криптоаналізу та загальні відомості. Задачі криптоаналізу. Криптографічна стійкість. Теоретична та практична стійкість шифру. Абсолютна стійкість.)	лекція, самостійна робота	[1-8]	2 6	1 тиждень
	Тема 1. Криптоаналіз. Основні поняття та приклади. (Принцип Кергофа. Методи криптоаналізу)	лаб.	[1-8]	2	
2	**Тема 2. Методи класичного криптоаналізу.** (Частотний криптоаналіз, метод повного перебору. Криптоаналіз шифрів простої заміни)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 2. Методи класичного криптоаналізу. (Програмна реалізація криптоаналізу шифрів зсуву (шифр Ю. Цезаря)	лаб.	[1-8]	4	
3	**Тема 3. Криптоаналіз поліалфавітних шифрів. Шифр Віженера.** (Шифрування, дешифрування, криптоаналіз Казискі, перший та другий метод Фрідмана)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 3. Криптоаналіз поліалфавітних шифрів. Шифр Віженера. (Програмна реалізація шифрування, дешифрування та криптоаналізу Казискі та методів Фрідмана)	лаб.		2	
4	**Тема 4. Криптоаналіз роторних криптосистеми. Шифр Enigma.** (Роторні криптосистеми з одним та більше роторів. Основи криптоаналізу шифру Enigma)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 4. Криптоаналіз афінних шифрів. (Лінійний криптоаналіз афінних шифрів.)	лаб.	[1-8]	4	
5	**Тема 5. Основи теорії секретного зв'язку (К. Шеннона). Семантична та безумовна стійкість.** (Гра у підслуховування. Поняття семантичної та безумовної стійкості)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 5. Основи теорії секретного зв'язку (К. Шеннона). Семантична та безумовна стійкість. (Доведення семантичної стійкості шифрів. Показати, що шифр Віженера не є семантично стійким)	лаб.	[1-8]	2	

6	**Тема 6. Вразливість шифру Two Times Pad.** (Надійність шифру одноразового блокноту та вразливість Two Times Pad)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 6. Вразливість шифру Two Time Pad. (Недоліки шифру одноразового блокноту. Ідеальна секретність, доведення безумовної стійкості)	лаб.	[1-8]	2	
7	**Тема 7. Методи криптоаналізу потокових шифрів** **(**Криптоаналіз та стійкість потокових шифрів. Криптостійкісь алгоритму "Струмок"**)**	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 7. Методи криптоаналізу потокових шифрів (Кореляційний криптоаналіз. Криптоаналіз на основі регістрів зсуву.)	лаб.	[1-8]	4	
8	**Тема 8. Криптоаналіз блокових шифрів.** (Лінійний криптоаналіз симетричних шифрів, Криптоаналіз блокових шифрів методом ітерацій, циклічні групи, приклади груп)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 8. Криптоаналіз блокових шифрів. **(**Диференціальний криптоаналіз симетричних шифрих. Криптоаналіз AES**)**	лаб.	[1-8]	2	
9	**Тема 9. Важко розв'язні задачі. Задача факторизації.** (Задачі факторизації та дискретного логарифму. Добування квадратного кореня за простим модулем.)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 9. Важко розв'язні задачі. Задача факторизації. (Програмна реалізація задачі факторизації. Алгоритм Полларда.)	лаб.	[1-8]	4	
10	**Тема 10. Первісні корені. Квадратичні лишки. Тестування простоти.** (Псевдопрості числа. Мала теорема Ферма. Сито Ератосфена. Ймовірносний тест Соловея-Штрассена. Ймовірнісний тест Міллера-Рабіна, тест простоти Люка. Проблема генерування простих чисел для криптосхеми DSA)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 10. Первісні корені. Квадратичні лишки. Тестування простоти. (Програмна реалізація алгоритмів тестування на простоти на основі теореми Ферма. Тести простоти параметрів асиметричних криптосистем. Сертифікат простоти Прата. Тест простоти AKS)	лаб.	[1-8]	2	1 тиждень
11	**Тема 11. Криптоаналіз асиметричних криптосистем.**	лекція, самостійна	[1-8]	2 8	1 тиждень

	(Атаки на криптосистему RSA, атаки на ЦЕП RSA) **Тема 12. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні** (Постановка завдання. Метод “крок немовляти, крок велетня”. Схема обчислення ключа доступу)	робота			
	Тема 11. Криптоаналіз асиметричних крптосистем. (Атаки на RSA використовуючи функцію Ейлера. Витік експоненти, Обчислювальна складність.) **Тема 12. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні** (Алгоритм обчислення порядку.)	лаб.	[1-8]	4	
12	**Тема 13. Елементи криптоаналізу геш-функцій.** (Оцінка параметрів хеш-функції для застосування в задачах криптології. Прррблема колізій та боротьба з ними. Криптографічна сіль. Birthday paradox.)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 13. Елементи криптоаналізу геш-функцій. (Криптографічна хеш-функція Blake. Криптоаналіз алгоритма DSA на базі хеш-функції Blake)	лаб.	[1-8]	4	
13	**Тема 14. Основні види атак та загроз цифрового підпису.** (Атака на основі відомого відкритого ключа, атака на основі відомих підписаних повідомлень, проста атака з вибором підписаних повідомлень. Атаки на слабкі підписи.)	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 14. Основні види атак та загроз цифрового підпису. (Спрямована атака з вибором повідомлень, адаптивна атака з вибором повідомлень, атака на зв'язаних ключах. Основні вивди загроз. Атака на алгоритм підпису ЕльГамаля)	лаб.	[1-8]	2	1 тиждень
14	**Тема 15. Еліптичні криптосистеми та їх стійкість.** (Основи криптографії на еліптичних кривих. Алгоритм Діффі-Хелмана та його стійкість.) **Тема 16. Використання нових технологій у криптоаналізі.** **(**Нейронні мережі, генетичні алгоритми**)**	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 15. Еліптичні криптосистеми та їх стійкість. (Стандарт цифрового підпису ECDSS, криптоаналіз еліптичних криптосистем.)	лаб.	[1-8]	4	

	Тема 16. Використання нових технологій у криптоаналізі. **(**Квантові комп’ютери.**)**				