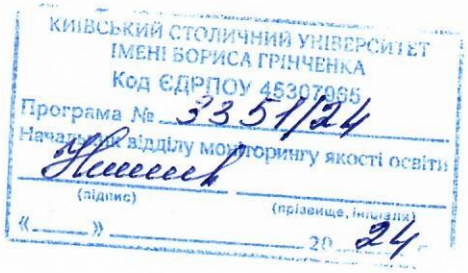
Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2024

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем



2023 – 2024 навчальний рік

Розробник:

Жданова Юлія Дмитрівна, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління Київського столичного університету імені Бориса Грінченка.

Викладач:

Жданова Юлія Дмитрівна, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління Київського столичного університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 03.01.2024 р. № 1

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2023 р.

Керівник освітньої програми ___ (підпис) Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2023 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4/120	
Курс	1	
Семестр	2	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	32	
Модульний контроль	8	
Самостійна робота	80	
Семестровий контроль	-	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Математичні методи криптографії» є нормативним документом Київського столичного університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Математичні методи криптографії» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Мета:

- надання знань, умінь, компетенцій в області математичних методів, які необхідні для розробки і використання криптографічних перетворень;
- засвоєння студентами фундаментальних знань в області теорії і практики математичних методів розробки сучасних криптоалгоритмів та криптопротоколів;
- набуття навичок практичного застосування законів та методів основних розділів математики, які необхідні для розробки і використання криптографічних перетворень.

Завдання: отримання теоретичних знань та формування практичних умінь з проектування та дослідження систем інформаційної та кібербезпеки та набуття наступних компетентностей:

Інтегральна компетентність – Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності:

ЗК 3: здатність до абстрактного мислення, аналізу та синтезу.

Фахові компетентності:

ФК 8: здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

мати уяву: про об’єкти абстрактної алгебри, теорії чисел, теорії скінченних полів, алгебраїчної геометрії; про математичні методи формування псевдовипадкових послідовностей, про математичні принципи функціонування криптографічних систем;

знати:

- основні поняття криптографії;
- типи і види криптографічних перетворень;
- елементи абстрактної алгебри;
- елементи теорії чисел;
- елементи теорії скінчених полів;
- елементи алгебраїчної геометрії;
- математичні методи формування криптоалгоритмів.

вміти:

- користуватися методами, методами абстрактної алгебри;
- застосовувати апарат теорії чисел;
- застосовувати апарат теорії скінчених полів;
- застосовувати апарат алгебраїчної геометрії.

та досягти наступних програмних результатів навчання:

РН 3: провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;

РН 4: застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;

РН 13: досліджувати, розробляти, впроваджувати та використовувати методи і засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Змістовий модуль 1. Вступ до курсу. Алгебраїчні методи криптографії					
Тема 1. Вступ до курсу Математичні методи криптографії	14	2	2		10
Тема 2. Основні алгебраїчні структури, що застосовуються у криптографії	14	2	2		10
Модульний контроль 1	2				
Разом за змістовим модулем 1	**30**	**4**	**4**		**20**
Змістовий модуль 2. Теоретико-числові методи криптографії Математичні моделі криптоалгоритмів					
Тема 3. Теоретико-числові методи криптографії	14	2	2		10
Тема 4. Математичні моделі криптоалгоритмів	14	2	2		10
Модульний контроль 2	2				
Разом за змістовим модулем 2	**30**	**4**	**4**		**20**
Змістовий модуль 3. Многочлени над скінченними полями. Лінійні рекурентні послідовності над полем *GF*(2)					
Тема 5. Многочлени над скінченними полями	14	2	2		10
Тема 6. Лінійні рекурентні послідовності над полем GF(2)	14	2	2		10
Модульний контроль 3	2				
Разом за змістовим модулем 3	**30**	**4**	**4**		**20**
Змістовий модуль 4. Алгоритми дискретного логарифмування. Методи алгебраїчної геометрії					
Тема 7. Алгоритми дискретного логарифмування	14	2	2		10
Тема 8. Методи алгебраїчної геометрії в криптографії	14	2	2		10
Модульний контроль 4	2				
Разом за змістовим модулем 4	**30**	**4**	**4**		**20**
Усього годин	**120**	**16**	**16**		**80**

5. Програма навчальної дисципліни

Змістовий модуль 1. Вступ до курсу. Алгебраїчні методи криптографії

Тема 1. Вступ до курсу.

Значення криптографії в інформаційному суспільстві. Базові поняття. Конфіденційність, автентичність, цілісність. Історичні етапи розвитку криптографії та їх характеристика. Приклади історичних шифрів. Модель К Шеннона криптосистеми з секретним ключем. Проблематика криптографії. Завдання та сучасні застосування криптографії. Математичні концепції, які лежать в основі криптографічних перетворень інформації. Математичні моделі в криптографії. Класифікація криптографічних методів. Класифікація криптографічних систем. Короткі відомості про криптоаналіз. Види атак на симетричні і асиметричні криптосистеми.

Тема 2. Основні алгебраїчні структури, що застосовуються у криптографії

Поняття алгебраїчної структури. Ізоморфізм алгебраїчних структур. Групи і підгрупи.

Циклічні групи. Порядок елемента групи. Групи підстановок.

Кільця і поля. Скінченні поля. Скінченні поля на базі кілець класів лишків за даним модулем. Характеристика поля. Число елементів скінченного поля. Примітивні елементи скінченного поля. Структура скінченного поля.

Скінченновимірні векторні простори**.**

Змістовий модуль 2. Теоретико-числові методи криптографії
Математичні моделі криптоалгоритмів

Тема 3. Теоретико-числові методи криптографії

Подільність цілих чисел. Найбільший спільний дільник, Найменше спільне кратне. Взаємно прості числа. Алгоритм Евкліда. Лінійні діофантові рівняння з двома невідомими. Прості числа і основна теорема арифметики.

Конгруентність цілих чисел. Модульна арифметика. Обчислення мультиплікативного оберненого за модулем. Функція Ейлера. Теорема Ейлера. Мала теорема Ферма.

Лінійні конгруенції. Системи лінійних конгруенцій. Китайська теорема про остачі.

Алгебраїчні конгруенції другого степеня за простим модулем. Алгоритм Шенкса-Тонеллі.

Алгебраїчні конгруенції другого степеня за модулем складеного числа, що є добутком двох простих чисел**.**

Тема 4. **Математичні моделі криптоалгоритмів**

Моделі шифрів класичної криптографії.

Комп'ютерні симетричні криптоалгоритми: DES, AES.

Комп'ютерні асиметричні криптоалгоритми: RSA, DSA. Криптосистема RSA. Атаки на RSA. Проблема факторизації великих чисел. Вимоги до параметрів RSA. Цифровий підпис RSA

Цифровий підпис DSA. Загальносистемні параметри КС. Формування ЦП згідно з DSA. Ключове рівняння. Формування і перевірка цифрового підпису DSA Стандарти цифрового підпису.

Змістовий модуль 3. Многочлени над скінченними полями
Лінійні рекурентні послідовності над полем *GF*(2)

Тема 5. Многочлени над скінченними полями.

Кільце многочленів над алгебраїчною структурою. Операції над многочленами. Алгоритми ділення многочленів. Алгоритм Евкліда для многочленів. Розкладання в кільці многочленів. Незвідні многочлени. Многочлени над скінченними полями. Алгоритм Берлекемпа розкладання многочлена на незвідні множники над скінченним полем.

Тема 6. Лінійні рекурентні послідовності над полем *GF*(2)

Лінійні рекурентні послідовності над скінченним полем. Регістри зсуву з лінійним зворотним зв'язком. Лінійна рекурентна послідовність, що генерується РЗЛЗЗ. Запис станів двійкового регістру через супроводжуючу матрицю. Анулюючі та мінімальні многочлени послідовностей над полем *GF*(2). Алгоритм Берлекемпа-Мессі пошуку найкоротшого РЗЛЗЗ для даної двійкової послідовності.

Змістовий модуль 4. Алгоритми дискретного логарифмування
Методи алгебраїчної геометрії в криптографії

Тема 7. Алгоритми дискретного логарифмування

Первісні корені та їх властивості. Індекси (дискретні логарифми). Задача дискретного логарифмування в скінченному полі. Криптосистема EG.

Алгоритми дискретного логарифмування: алгоритм Сільвера-Полліга-Хеллмана; алгоритм Шенкса (алгоритм малого та великого кроку); ρ-алгоритм Полларда.

Тема 8. Методи алгебраїчної геометрії в криптографії

Еліптичні криві та їх властивості. Групова операція на множині точок еліптичної кривої. Еліптичні криві над скінченним полем. Визначення порядку групи точок еліптичної кривої над скінченним полем.

Знаходження точки еліптичної кривої над $GF(2^n)$.
Методи обчислення скалярного добутку на еліптичній кривій.
Задача дискретного логарифмування в групі точок еліптичної кривої.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

6.1 Система оцінювання навчальних досягнень студентів

Поточний контроль здійснюється в балах під час оцінювання знань та вмінь студента з кожного практичного заняття, опитування теорії, результатів самостійної роботи.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2	2	2
Відвідування практичних занять	1	2	2	2	2	2	2	2	2
Робота на практичному занятті	10	2	20	2	20	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Макс. кількість балів за видами поточного контролю (МВ)			54		54		54		54
Максимальна кількість балів: 216									
Розрахунок коефіцієнта: 216/100=2,16									

6.2 Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Вступ до курсу. Алгебраїчні методи криптографії.		**20**	**5**
1	- виконання завдань відповідно до теми; - опрацювання фахових видань.	20	5
Змістовий модуль 2. Теоретико-числові методи криптографії Математичні моделі криптоалгоритмів		**20**	**5**
2	Безпека криптосистема RSA - виконання завдань відповідно до теми; - опрацювання фахових видань.	20	5
Змістовий модуль 3. Многочлени над скінченними полями. Лінійні рекурентні послідовності над полем *GF*(2)		**20**	**5**
3	Сучасні потокові шифри: - виконання завдань відповідно до теми; - опрацювання фахових видань.	20	5
Змістовий модуль 4. Алгоритми дискретного логарифмування. Методи алгебраїчної геометрії		**20**	**5**
3	Алгоритми еліптичної криптографії - виконання завдань відповідно до теми;	20	5

	- опрацювання фахових видань.		
	Разом	80	20

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

6.3 Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, за виконання домашніх завдань, за виконання завдань самостійної роботи, за модульну контрольну роботу. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – виконання тестових завдань в середовищі MOODLE. Модульна контрольна робота оцінюється у 25 балів.

6.4 Форми проведення семестрового контролю та критерії оцінювання

Семестровий (підсумковий) контроль знань студентів здійснюється після завершення вивчення навчального матеріалу дисципліни у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Підсумкова семестрова (залікова) рейтингова оцінка студента є сумою підсумкових фактичних оцінок студента за змістовими модулями.

6.5. Орієнтовний перелік питань для самоконтролю

Змістовий модуль 1. Вступ до курсу. Алгебраїчні методи криптографії

1. Значення криптографії в інформаційному суспільстві.
2. Конфіденційність, автентичність, цілісність.
3. Модель К Шеннона криптосистеми з секретним ключем.
4. Моделі відкритого повідомлення.
5. Моделі криптосистеми.
6. Проблематика криптографії.
7. Завдання криптографічного захисту інформації
8. Сучасні застосування криптографії.
9. Поняття алгебраїчної структури.
10. Ізоморфізм алгебраїчних структур.
11. Групи і підгрупи.
12. Циклічні групи.
13. Порядок групи і порядок елемента групи.
14. Групи підстановок.
15. Кільця і поля.

16. Скінченні поля на базі кілець класів лишків за даним модулем.
17. Характеристика поля.
18. Число елементів скінченного поля.
19. Мультиплікативна група кільця.
20. Примітивні елементи скінченного поля.
21. Структура скінченного поля.
22. Скінченновимірні векторні простори.

Змістовий модуль 2. Теоретико-числові методи криптографії
Математичні моделі криптоалгоритмів

23. Подільність цілих чисел. НСД, НСК. Взаємно прості числа.
24. Алгоритм Евкліда.
25. Лінійні діофантові рівняння з двома невідомими.
26. Прості числа і основна теорема арифметики.
27. Конгруентність цілих чисел.
28. Модульна арифметика.
29. Обчислення мультиплікативного оберненого за модулем.
30. Функція Ейлера. Теорема Ейлера. Мала теорема Ферма.
31. Лінійні конгруенції.
32. Системи лінійних конгруенцій. Китайська теорема про остачі.
33. Конгруенції 2-го степеня за простим модулем. Алгоритм Шенкса-Тонеллі.
34. Алгебраїчні конгруенції другого степеня за модулем складеного числа, що є добутком двох простих чисел.
35. Моделі шифрів класичної криптографії.
36. Математичні моделі блокових криптосистем DES, AES.
37. Математичні моделі асиметричних криптоалгоритмів.
38. Криптосистема RSA. Функції шифрування/розшифрування.
39. Атаки на RSA.
40. Проблема факторизації великих чисел.
41. Вимоги до параметрів RSA.
42. Цифровий підпис RSA.
43. Цифровий підпис DSA.

Змістовий модуль 3. Многочлени над скінченними полями
Лінійні рекурентні послідовності над полем *GF*(2)

44. Кільце многочленів над алгебраїчною структурою.
45. Операції над многочленами.
46. Алгоритми ділення многочленів.
47. Алгоритм Евкліда для многочленів.
48. Розкладання в кільці многочленів. Незвідні многочлени.
49. Многочлени над скінченними полями.
50. Алгоритм Берлекемпа розкладання многочлена на незвідні множники над скінченним полем.
51. Лінійні рекурентні послідовності над скінченним полем.
52. Регістри зсуву з лінійним зворотним зв’язком.
53. Лінійна рекурентна послідовність, що генерується регістром зсуву з лінійним зворотним зв’язком.
54. Запис станів двійкового регістру через супроводжуючу матрицю.
55. Анулюючі та мінімальні многочлени послідовностей над полем GF(2).
56. Алгоритм Берлекемпа-Мессі пошуку найкоротшого РЗЛЗЗ для даної двійкової послідовн ості.

Змістовий модуль 4. Алгоритми дискретного логарифмування

Методи алгебраїчної геометрії в криптографії

57. Первісні корені та їх властивості.
58. Індекси (дискретні логарифми).
59. Задача дискретного логарифмування в скінченному полі.
60. Алгоритм дискретного логарифмування Сільвера-Полліга-Хеллмана.
61. Алгоритм дискретного логарифмування Шенкса (алгоритм малого та великого кроку);
62. ρ-алгоритм Полларда дискретного логарифмування.
63. Криптосистеми типу Ель-Гамаля.
64. Цифровий підпис Ель-Гамаля.
65. Цифровий підпис DSA.
66. Еліптичні криві та їх властивості.
67. Групова операція на множині точок еліптичної кривої.
68. Еліптичні криві над скінченним полем. Визначення порядку групи точок еліптичної кривої над скінченним полем.
69. Знаходження точки еліптичної кривої над полем $GF(2^n)$.
70. Методи обчислення скалярного добутку на еліптичній кривій.
71. Задача дискретного логарифмування в групі точок еліптичної кривої.

6.6 Шкала відповідності оцінок

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни (п. 7), де зазначено види контролю і кількість балів за видами. Систему рейтингових балів подано нижче у таблиці.

Шкала оцінювання

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	**Відмінно** — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	**Дуже добре** – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	**Добре** – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	**Задовільно** – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	**Достатньо** – мінімально можливий допустимий рівень знань (умінь)
FX	35-59	**Незадовільно з можливістю повторного складання** – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	**Незадовільно з обов'язковим повторним вивченням курсу** – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична карта дисципліни

Разом: 120 год., лекції – 16 год., практичні заняття – 16 год., модульний контроль – 8 год., самостійна робота – 80 год.

Модулі (назви, бали)	**Змістовий модуль 1. Вступ до курсу. Алгебраїчні методи криптографії.** (54 бали)		**Змістовий модуль 2. Теоретико числові методи криптографії Математичні моделі криптоалгоритмів** (54 бали)		**Змістовий модуль 3. Многочлени над скінченними полями Лінійні рекурентні послідовності над полем GF(2)** (54 бали)		**Змістовий модуль 4. Алгоритми дискретного логарифмування Методи алгебраїчної геометрії в криптографії** (54 бали)	
Теми	1	2	3	4	5	6	7	8
Лекції (теми, бали)	1. Вступ до курсу (1бал)	2. Основні алгебраїчні структури, що застосовуються у криптографії (1бал)	3. Поняття та алгоритми теорії чисел, що застосовуються у криптографії (1бал)	4. Математичні моделі шифрів (1бал)	5. Многочлени над скінченними полями (1бал)	6. Лінійні рекурентні послідовності над полем GF(2) (1бал)	7. Алгоритми дискретного логарифмування (1бал)	8. Еліптичні криві в криптографії (1бал)
Практичні заняття (теми, бали)	1. Шифри підстановки та перестановки (11балів)	2. Основні алгебраїчні структури в криптоперетвореннях (11балів)	3. Застосування теоретико-числових алгоритмів до криптоперетвореньп (11балів)	4. Криптосистема RSA (11балів)	5. Многочлени над скінченними полями (11балів)	6. Алгоритм Берлекемпа-Мессі (11балів)	7. Криптосистема EG (11балів)	8. Алгоритми на еліптичних кривих (11балів)
Самост. робота	Самостійна робота 1 (5 балів)		Самостійна робота 2 (5 балів)		Самостійна робота 3 (5 балів)		Самостійна робота 4 (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)	
Підсумковий контроль (вид, бали)	Залік							

8. Рекомендовані джерела

Основна література

1. Бабенко Т.В., Гулак Г.М., Сушко С. О., Фомичова Л.Я. Криптологія у прикладах, тестах і задачах: навч. посіб. – Дніпропетровськ: Національний гірничий університет, 2013. – 318 с.
2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. – Вінниця: ВНТУ, 2011. –198 с.
3. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало [та ін.] – Нац. ун-т "Львів. політехніка". – Львів : Вид-во Львів. політехніки, 2019. – 573 с.
4. Кузнецов Г. В., Фомичов В. В., Сушко С.О., Фомичова Л. Я. Математичні основи криптографії: навч. посіб. – Дніпропетровськ: Національний гірничний університет, 2004. –391 с.
5. Оглобліна О. І., Сушко Т.С., Шрамко Ю. В. Елементи теорії чисел: навч. посіб. – Суми: Сумський державний університет, 2015. – 186 с.
6. Сушко С. О., Кузнецов Г. В., Фомичова Л. Я., Корабльов А. В. Математичні основи криптоаналізу: навч. посіб. – Дніпропетровськ: Національний гірничний університет, 2010. – 466 с.
7. Фільштінський В. А., Бережний А. В. Математичні основи криптографії: конспект лекцій. – Суми: Сумський державний університет, 2011. – 138 с.
8. Фаль О.М. Криптографія: основні ідеї та застосування / О.М. Фаль. – К.: ІВЦ Видавництво «Політехніка», 2003. – 28 с.

Додаткова література

1. Блінцов В. С. Математичні основи криптології + CD: Навчальний посібник для студ. вищих навч. закл. / В. С. Блінцов, Ю. Л. Гальчевський. – Миколаїв : Національний ун-т кораблебудування ім. адмірала Макарова, 2006. – 232 с. 3.
2. Бобало Ю. Я. [та ін.] Інформаційна безпека: навч. посібник. – Львів: Видавництво Львівської політехніки, 2019. – 573 с.
3. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. – Київ: ДУІКТ, 2006. – 125 с.
4. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія: Підручник. – Київ, 2002. – 504 с.
5. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч. посібник / Г.Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с.
6. Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. – CRC Press, 2001. – 780 p.
7. Menezes A. Elliptic Curve Public Key Cryptosystems, – Kluwer Academic Publishers, 1993. – 141 p.
8. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition.– New York: Wiley, 2015. – 784 p.
9. Steinberg J., Beaver K., Winkler I., Coombs T. Cybersecurity All-in-One For Dummies. – New York: Wiley, 2022. – 700 p.

Додаткові ресурси (інформаційні ресурси)

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
2. The CrypTool Portal [Електронний ресурс]. — Режим доступу: https://www.cryptool.org/en
3. Wenbo Mao. Modern Cryptography: Theory and Practice. Hewlett-Packard Company. Published Prentice Hall PTR. 2003. 648 p. [Електронний ресурс] – Режим доступу: https://docs.google.com/file/d/0Bxy7_wFLYLfSYlpUdHhVQUU5Rnc/view?resourcekey=0-8Xf78RyrE1DuU8XA8xQHTA