Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра математичного аналізу та теорії ймовірностей

Елементарна теорія чисел та криптографія

Робоча програма кредитного модуля навчальної дисципліни «Елементарна теорія чисел та криптографія» (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	**Перший (бакалаврський)**
Галузь знань	11 Математика та статистика
Спеціальність	111 Математика
Освітня програма	Страхова та фінансова математика
Статус дисципліни	Вибіркова
Форма навчання	Очна(денна)/дистанційна
Рік підготовки, семестр	3 курс, осінній семестр
Обсяг дисципліни	120 годин (36 години – Лекції, 36 годин – Практичні, 48 годин – СРС)
Семестровий контроль/ контрольні заходи	Залік /МКР, РГР
Розклад занять	http://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	**Лектор**: Кубайчук Оксана Олексіївна, кандидат фізико-математичних наук, доцент кафедри математичного аналізу та теорії ймовірностей, o.kubaychuk@gmail.com, 0664507032. **Практичні**: асистент, Юськович Віктор Костянтинович, viktyusk@gmail.com ; асистент, Колеснік Олександр Валерійович, https://t.me/lxndr_klsnk
Розміщення курсу	https://campus.kpi.ua

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Опис дисципліни	Відповідно до навчального плану освітній компонент «*Елементарна теорія чисел та криптографія*» належить до циклу професійної підготовки та має велике значення у підготовці фахівця за освітньою програмою «*Страхова та фінансова математика*». Компонент містить основні положення криптографії, знайомить з найбільш розповсюдженими типами шифрів та методами криптоаналізу, криптографічними протоколами (електронні гроші, електронний підпис, електронне голосування тощо). Пояснюється математична теорія, яка лежить в основі криптографії (а саме основні поняття сучасної теорії чисел). Знайомить з основними криптографічними протоколами (електронний підпис, електронні гроші, електронні вибори тощо).
Цілі дисципліни	Ціллю навчальної дисципліни є ознайомлення з теоретичними основами криптографії, придбання навичок в практичному використанні, постановці і розв'язанні задач шифрування інформації, розуміння суті інформаційних процесів в криптографічних системах, застосування комп'ютерів для вирішення завдань.
Предмет навчальної дисципліни	Предметом «*Елементарна теорія чисел та криптографія*» є вивчення теоретичних основ основних сучасних методів шифрування та дешифрації, а на їх основі декількох практичних застосувань, як то електронні гроші, електронне голосування, сліпий підпис
Компетентності	Метою навчальної дисципліни є формування у студентів здатностей: ЗК2 Здатність застосовувати знання у практичних ситуаціях. ЗК6 Навички використання інформаційних і комунікаційних технологій. ЗК12 Здатність працювати автономно. ЗК16 Здатність проявляти творчий підхід та ініціативу. ФК1 Здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання. ФК5 Здатність до кількісного мислення. ФК7 Здатність застосовувати чисельні методи для дослідження математичних моделей. ФК8 Здатність до аналізу математичних структур, у тому числі до оцінювання обґрунтованості й ефективності використовуваних математичних підходів. ФК9 Здатність застосовувати спеціалізовані мови програмування та ФК14 Здатність демонструвати математичну грамотність, послідовно пояснити іншим математичні теорії або їх складові частини, взаємозв'язок та відмінність між ними, навести приклади застосувань у природничих науках.
Програмні результати навчання	РН4 Розуміти фундаментальну математику на рівні, необхідному для досягнення інших вимог освітньої програми. РН5 Мати навички використання спеціалізованих програмних засобів комп'ютерної та прикладної математики і використовувати інтернет-ресурси. РН7 Пояснювати математичні концепції мовою, зрозумілою для нефахівців у галузі математики. РН11 Розв'язувати конкретні математичні задачі, які сформульовано у формалізованому вигляді; здійснювати базові перетворення математичних моделей. РН12 Відшуковувати потрібну науково-технічну інформацію у науковій літературі, базах даних та інших джерелах інформації. РН15 Знати теоретичні основи і застосовувати алгебраїчні методи для вивчення математичних структур.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Пререквізити: Навчальна дисципліна «*Елементарна теорія чисел та криптографія*» базується на знаннях, отриманих при вивченні дисциплін «Лінійна алгебра» (ПО3), «Скінченновимірний лінійний аналіз» (ПО4), «Математична логіка та дискретна математика» (ПО6), «Історія науки і техніки» (ЗО2), «Культура науково-технічного мовлення фахівця» (ЗО1), які вивчаються на бакалаврському рівні вищої освіти за спеціальністю 111 Математика.

Постреквізити: Освітній компонент «*Елементарна теорія чисел та криптографія*» передує вивченню дисципліни «Теорія ймовірностей» (ПО2), «Основи математичної статистики» (ПО17), «Основи теорії випадкових процесів» (ПО20), «Методи математичної економіки» (ПО22), «Статистичні методи у ризиковому страхуванні» (ПО23), «Основні математичні моделі процесів ризику» (ПО24), «Лінійний регресійний аналіз» (ПО26).

3. Зміст навчальної дисципліни

Назва розділів і тем	Кількість годин			
	Всього	У тому числі		
		Лекції	**Практичні**	**СРС**
Розділ 1. Алгоритми та їх складність	4	2		2
Розділ 2. Елементи абстрактної алгебри та теорії чисел	50	18	16	16
Розділ 3. Криптографія	48	16	16	16
Розрахункова робота	10	-	-	10
Контрольна робота	2		2	
Залік	6	-	2	4
Всього годин	120	36	36	48

4. Навчальні матеріали та ресурси

Базова література.

1. Клесов О.І., *Елементарна теорія чисел та елементи криптографії*, 2017, ТВіМС, Київ, 394 стор. https://ela.kpi.ua/handle/123456789/30046.
2. Т.Г. Кормен, Ч.Е. Лейзерсон, Р.Л. Рівест, К. Стайн. *Вступ до алгоритмів*, К: К.І.С., 2023, 1288 с.
3. Т.В. Авдєєва, В.М. Горбачук, *Алгебра. Основи алгебраїчних структур*, К.: НТУУ «КПІ», 2015. – 79 с.
4. О.Г. Ганюшкін, О.О. Безущак. *Завдання до практичних занять з алгебри і теорії чисел*, К.: ВПЦ «Київський університет», 2007. – 103 с
5. Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко. *Практикум з прикладної алгебри*, К.:, 2015. – 59 с.
6. Buchmann J. A., *Introduction to cryptography*, second edition, 2004, Springer Verlag, New

York.
7. Koshy T., *Elementary Number Theory with Applications*, 2007, 2nd edition, Elsevier, Amsterdam.
8. Rosen K. H., *Elementary Number Theory*, 2011, 6th edition, Addison Wesley, Boston MA.
9. W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets. A computational Approach, 2009, Springer-Verlag, New York.
10. Young A. L., *Mathematical Ciphers: from Caesar to RSA*, 2006, American Mathematical Society, Providence, RA.

Допоміжна література.

11. Coutinho S., *The Mathematics of Ciphers. Number Theory and RSA Criptography*, 1999, A. K. Peters, Natick, Massachusetts.
12. Вербицький О. В., *Вступ до криптології*. – Львів.: ВНТЛ., 1998. – 248 с.
13. Калашнікова Н. В. *Елементи алгебри та їх застосування в криптографії*. – Д.: РВВ ДНУ, 2015. – 40 с.
14. Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко. *Збірник задач з теорії кілець*, К.: ВПЦ «Київський університет», 2013. – 86 с.
15. Bruce Schneier, *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*, John Wiley & Sons, 1996, P. 1027.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)
Очна/дистанційна форма

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1	Алгоритми та їх складність. ***Рекомендована література:*** **[1], [2], [15]**
2	Групи. Теорема Лагранжа ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13]**
3	Циклічні групи. Відображення груп ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13]**
4	Кільця. Кільце лишків за модулем ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13], [14]**
5	Кільця поліномів та їх властивості ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13], [14]**
6	Поля. Поля Галуа ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13]**
7	Алгоритм евкліда. Основна теорема арифметики. Конгруенції та їх властивості. Китайська теорема про лишки ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13]**
8	Подільність, факторизація. Застосування факторизації. Розподіл простих чисел. Псевдопрості числа. Тестування простоти ***Рекомендована література:*** **[1], [2], [3], [4], [5], [12], [13]**
9	Квадратичні лишки та нелишки. Добування квадратного кореня у кільці лишків ***Рекомендована література:*** **[1], [3], [4], [5], [12], [13]**
10	Найпростіші методи дискретного логарифмування та факторизації. Важкооборотні функції

	Рекомендована література: **[1], [6], [7], [8], [9], [10], [12],[15]**
11	Задачі криптографії. Моделі шифрів. Стійкість криптосистем. Історичні шифри (Цезаря, Віженера, Вернама, Бофора). Шифри гамування. ***Рекомендована література:*** **[1], [6], [7], [8], [9], [10], [12]**
12	Основи побудови симетричних потокових криптосистем. RC4, A5/1. ***Рекомендована література:*** **[1], [6], [7], [8], [9], [10], [12], [15]**
13	Основи побудови блокових криптосистем. Стандарти шифрування DES, AES, «Калина» ***Рекомендована література:*** **[1], [6], [7], [8], [9], [10], [12], [15]**
14	Основи побудови асиметричних криптосистем. Алгоритм Діффі-Хеллмана ***Рекомендована література:*** **[1], [6], [7], [8], [9], [10], [12], [15]**
15	Побудова, аналіз стійкості та застосування криптографічних геш-функцій ***Рекомендована література:*** **[1], [6], [7], [8], [9], [10], [12], [15]**
16	Схеми відкритого шифрування RSA і Ель-Гамаля. Цифровий підпис ***Рекомендована література:*** **[1], [2], [7], [8], [9], [10], [12], [15]**
17	Національний стандарт ДСТУ- 4145. Цифровий підпис, що грунтується на еліптичних кривих ***Рекомендована література:*** **[1], [15]**
18	Електронні гроші. Електронні вибори ***Рекомендована література:*** **[1], [7], [9]**

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1	Обчислення складності алгоритмів
2	Групи. Теорема Лагранжа. Розв’язання задач
3	Циклічні групи. Відображення груп. Розв’язання задач
4	Кільця. Кільце лишків за модулем. Розв’язання задач
5	Кільця поліномів та їх властивості. Розв’язання задач
6	Поля. Поля Галуа. Розв’язання задач
7	Алгоритм евкліда. Основна теорема арифметики. Конгруенції та їх властивості. Китайська теорема про лишки. Розв’язання задач
8	Подільність, факторизація. Застосування факторизації. Розподіл простих чисел. Псевдопрості числа. Тестування простоти. Розв’язання задач
9	Квадратичні лишки та нелишки. Добування квадратного кореня у кільці лишків. Розв’язання задач
10	Найпростіші методи дискретного логарифмування та факторизації. Важкооборотні функції. Розв’язання задач
11	Історичні шифри, шифри гамування. Розв’язання задач
12	Розв’язання задач на дослідження основних властивостей лінійних регістрів зсуву
13	Розв’язання завдань на дослідження властивостей елементів сучасних блокових алгоритмів
14	Задачі дискретного логарифмування та факторизації як основа стійкості асиметричних криптосистем.
15	Стандарт функції гешування «Купина» ДСТУ 7564:2014
16	Розв’язання задач зашифрування, розшифрування та формування цифрового підпису

	повідомлень з використанням криптосистем RSA та Ель-Гамаля
17	МКР
18	Залік

6. Самостійна робота здобувача освіти

Вивчення дисципліни «*Елементарна теорія чисел та криптографія*» включає наступні види самостійної роботи:

- підготовка до лекційних та практичних занять, виконання домашніх завдань;
- виконання розрахунково-графічної роботи;
- підготовка та виконання модульної контрольної роботи;
- підготовка презентацій доповідей;
- підготовка до заліку.

Контрольна робота

Запланована модульна контрольна робота, яка поділяється на дві частини:

1. МКР.

Політика та контроль

7. Політика навчальної дисципліни «Розвиток класичних ідей в сучасній математиці»

Рекомендовані методи навчання: вивчення основної та допоміжної літератури за тематикою лекцій, розв'язування задач на практичних заняттях. Важливим аспектом якісного засвоєння матеріалу, відпрацювання методів та алгоритмів розв'язання/побудови основних завдань дисципліни є самостійна робота (опрацювання навчальних матеріалів лекційних занять, підготовка до практичних занять, виконання завдань домашньої роботи, підготовку до МКР та іспиту).

- **Пропущені контрольні заходи**

Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

- **Календарний рубіжний контроль.**

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем. Метою проведення атестації є підвищення якості навчання студентів та моніторинг виконання графіка освітнього процесу студентами.

Критерій			Перша атестація	Друга атестація
Термін атестації				
Умови одержання атестації	Поточний рейтинг		більше 50% можливих на даний момент балів	більше 50% можливих на даний момент балів
	Поточний контрольний захід	МКР, СР.	+	+

Академічна доброчесність
Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

Норми етичної поведінки
Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО) (очна\дистанційна форма)

Розподіл навчального часу за видами занять і завдань з дисципліни згідно з робочим навчальним планом.

Рейтинг студента з дисципліни складається з балів, що він отримує за

1) відповіді на практичних заняттях та домашні завдання;
2) одна контрольна робота (МКР може бути поділена на декілька контрольних робіт);
3) одна РГР (розрахунково-графічна робота);

Розмір шкали рейтингу *R* = 100 балів.

Система рейтингових (вагових) балів та критерії оцінювання

За несвоєчасне (пізніше ніж на тиждень) подання модульної та розрахункової роботи зараховується не більше 50%.

1. Модульний контроль
Модульна контрольна робота може ділитись на частини. Максимальний бал – 50.
Критерій оцінювання МКР:
відсутність на контрольній роботі – 0 балів,
МКР не переписується, оцінка МКР (в балах) дорівнює величині відсотка (від максимальної кількості балів 50) її виконання.

2. Розрахунково-графічна робота (РГР) – самостійне дослідження студента.
Ваговий бал – 50.
Критерій оцінювання РГР:
Невиконання РГР – 0 балів. Вимоги до оформлення РГР і захисту по завершенню семестру, а також тематику самостійного дослідження буде надано викладачем практичних занять.

3. В разі незгоди з отриманим балом, але за умови виконання всіх робіт, студент може здавати залік. В цьому випадку усі попередньо набрані бали анулюються. На залік студент отримує два теоретичних питання і одну задачу. Теоретичні питання оцінюються максимально у 30 балів, а задача у 40.

4. Штрафні та заохочувальні бали
- несвоєчасне (пізніше ніж на тиждень) подання розрахункової роботи -1 бал
- заохочувальні бали за виконання творчих завдань
Максимальна кількість штрафних (заохочувальних) балів не перевищує 10% (10 балів)

Студент допускається до заліку, якщо його рейтинг семестру не менший 30 балів, при цьому він має хоча б одну позитивну атестацію, зараховані модульні контрольні роботи та РГР (виконану не менше ніж на 60%).

Якщо рейтинг семестру менший 30 балів, студент може написати допускову контрольну роботу.

Таблиця переведення рейтингової оцінки з навчальної дисципліни R: *(згідно з Табл. 1)*

R	**Оцінка ECTS**	**Традиційна оцінка**
95...100	A	відмінно
85...94	B	дуже добре
75...84	C	добре
65...74	D	задовільно
60...64	E	достатньо
R<=60	Fx	незадовільно
R<=30 або не виконані інші умови допуску до заліку	F	не допущений

Робочу програму навчальної дисципліни (силабус):
Складено: професором кафедри МАтаТЙ, д.ф.-м.н., проф. Клесовим О.І.;
доцентом кафедри МАтаТЙ, к.ф.-м.н., Кубайчук О.О.

Ухвалено: кафедрою МАтаТЙ (протокол № 12 від 19.06.2023)
Погоджено: Методичною радою ФМФ (протокол № 10 від 27.06.2023р.)