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**: Клесов Олег Іванович, доктор фізико-математичних наук, професор кафедри математичного аналізу та теорії ймовірностей, voselk@gmail.com **Практичні**: Клесов Олег Іванович, доктор фізико-математичних наук, професор кафедри математичного аналізу та теорії ймовірностей, voselk@gmail.com
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. Прості шифри; подільність натуральних чисел, арифметика за модулем	32	12	10	10

Розділ 2. Адитивні та експоненційні шифри; функція Ойлера	28	8	8	10
Розділ 3. Криптосистеми з відкритим ключем (RSA)	36	12	10	12
Розділ 4. Розподіл простих чисел, застосуваня у криптографії	**7**	4	4	1
Розрахункова робота	9	-	-	9
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.
2. Buchmann J. A., *Introduction to cryptography*, second edition, 2004, Springer Verlag, New York.
3. Koshy T., *Elementary Number Theory with Applications*, 2007, 2nd edition, Elsevier, Amsterdam.
4. Rosen K. H., *Elementary Number Theory*, 2011, 6th edition, Addison Wesley, Boston MA.
5. W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets. A computational Approach, 2009, Springer-Verlag, New York.
6. Young A. L., *Mathematical Ciphers: from Caesar to RSA*, 2006, American Mathematical Society, Providence, RA.

Допоміжна література.

7. Василенко О. Н., *Теоретико-числовые алгоритмы в криптографии*, 2006, ``МЦНМО'', Москва.
8. Деза Е. И., Котова Л. В., *Сборник задач по теории чисел*, 2011, УРСС, Москва.
9. Осипян В. О., Осипян К. В., *Криптография в упражнениях и задачах*, 2004, Гелиос АРВ, Москва.
10. Coutinho S., *The Mathematics of Ciphers. Number Theory and RSA Criptography*, 1999, A. K. Peters, Natick, Massachusetts.

Інформаційні ресурси.

Дистанційні курси: О.І. Клесов «Елементарна теорія чисел та елементи криптографії» https://ela.kpi.ua/handle/123456789/30046

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	Звязок між теорією чисел та криптографією. ***Рекомендована література:*** **[1]**
2	Шифр Цезаря. Шифрація. Дешифрація. Арифметика за модулем ***Рекомендована література:*** **[1], [6]**
3	Мультиплікативні шифри. Обернені числа за модулем ***Рекомендована література:*** **[1], [3], [4]**
4	Мультиплікативні шифри. Криптотаналіз ***Рекомендована література:*** **[1], [6]**
5	Алгоритм Евкліда. Розширений алгоритм Евкліда ***Рекомендована література:*** **[1], [3], [4]**
6	Шифр Хілла ***Рекомендована література:*** **[1]**
7	Аддитивні шифри. Функція Ойлера. Теорема Ойлера. Мала теорема Ферма ***Рекомендована література:*** **[1], [3], [4]**
8	Аддитивні шифри. Криптоаналіз. Принцип Керкхофса ***Рекомендована література:*** **[1], [2], [6]**
9	Експоненціальні шифри. Шифрування. Показник кореня за модулем ***Рекомендована література:*** **[1], [3], [4]**
10	Експоненціальні шифри. Криптоаналіз. Односторонні функції. Алгоритм Крайчика ***Рекомендована література:*** **[1], [5]**
11	Криптосистеми з відкритими ключами. Головоломки Меркла. Метод Діффі-Хелмана ***Рекомендована література:*** **[1], [2], [5]**
12	Метод RSA. Доведення. Атаки на RSA ***Рекомендована література:*** **[1], [2], [5]**
13	Рюкзачна система. Метод Ель-Гамаля. ***Рекомендована література:*** **[1], [3], [5]**
14	Цифровий підпис. Сліпий цифровий підпис ***Рекомендована література:*** **[1], [3], [5]**
15	Електронні вибори на базі RSA ***Рекомендована література:*** **[1], [3], [5]**
16	Електронні гроші на базі RSA ***Рекомендована література:*** **[1], [3], [5]**
17	Перевірка натуральних чисел на простоту ***Рекомендована література:*** **[1], [3], [4]**
18	Теорема про розподіл простих чисел ***Рекомендована література:*** **[1], [3], [4]**

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1	Вступ до криптографії. Зв'язок з теорією чисел
2	Шифр Цезаря. Арифметика за модулем
3	Мультиплікативні шифри. Числа, обернені за модулем
4	Застосування чисел, обернених за модулем. Криптоаналіз мультиплікативних шифрів
5	Алгоритм Евкліда. Розширений алгоритм Евкліда. Алгоритм знаходження чисел, обернених за модулем
6	Шифр Хілла. Системи лінійних рівнянь за модулем
7	Аддитивні шифри. Функція Ойлера
8	Аддитивні шифри. Криптоаналіз
9	МКР
10	Експоненціальні шифри. Показник кореня за модулем
11	Експоненціальні шифри. Односторонні функції
12	Криптосистеми з відкритими ключами. Головоломки Меркла. Метод Діффі-Хелмана
13	Метод RSA. Доведення. Атаки на RSA
14	Рюкзачна система. Метод Ель-Гамаля
15	Цифровий підпис. Сліпий цифровий підпис
16	Електронні вибори на базі RSA. Електронні гроші на базі RSA
17	Перевірка натуральних чисел на простоту
18	Теорема про розподіл простих чисел

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;
- підготовка та виконання модульної контрольної роботи;
- підготовка та виконання РГР .

На самостійне опрацювання виноситься декілька підрозділів з усіх розділів на розсуд викладача. Їх можна взяти з підручників [1-6], але дозволяється використовувати інші джерела для поглибленого вивчення того, чи іншого питання. Планом також передбачені індивідуальні завдання для студентів, які виконуються самостійно або робочими групами.

Контрольні роботи Запланована модульна контрольна робота.

Політика та контроль

7. Політика навчальної дисципліни «*Елементарна теорія чисел та криптографія*»

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 заліку).

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
Умови одержання атестації	Поточний рейтинг		більше 50% можливих на даний момент балів	більше 50% можливих на даний момент балів
	Поточний контрольний захід	РГР,СР.	+	+
		МКР, РГР, 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.

Семестр	Навчальний час		Розподіл навчальних годин				Контрольні заходи		
	кредити	акад. год.	Лекц.	Практич.	Лаб. роб.	СРС + іспит	МКР	РГР	Семестрова атестація
5	4	120	36	36	-	48	1	1	залік

Рейтинг студента з дисципліни складається з балів, що він отримує за
1.відповіді на практичних заняттях та домашні завдання;
2.одна контрольна робота;
3.одна РГР (розрахунково-графічна робота);
Розмір шкали рейтингу *R* = 100 балів.

Система рейтингових (вагових) балів та критерії оцінювання

1. Робота на практичних заняттях

Ваговий бал – 15. Максимальна кількість балів на всіх практичних заняттях дорівнює 20 балів.

0.0 – відмова від відповіді, незнання необхідного теоретичного матеріалу;

0.25 – знання окремих фрагментів теоретичного матеріалу,;

0,5 – поверхневе знання теоретичного матеріалу, розв'язування задачі;

0.75 – добре знання теоретичного матеріалу, вміння його застосовувати;

1 – досконале знання теоретичного матеріалу, самостійне розв'язування задачі.

2. Домашні роботи

Ваговий бал – 15. Максимальна кількість балів за всі домашні роботи дорівнює 15 балів.
Критерій оцінювання ДЗ:
відсутність домашніх робіт – 0 балів.
За несвоєчасне (пізніше ніж на тиждень) подання домашньої роботи зараховується не більше 50%.

3. Модульний контроль

Ваговий бал – 40. Максимальна кількість балів дорівнює 40 балів.
Критерій оцінювання МКР:
відсутність на контрольній роботі – 0 балів,
МКР не переписується, оцінка МКР (в балах) дорівнює величині відсотка (від максимальної кількості балів 10) її виконання.

4. Розрахунково-графічна робота (РГР) – самостійне дослідження студента.

Ваговий бал – 30.
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.

За несвоєчасне (пізніше ніж на тиждень) подання РГР (без захисту роботи) зараховується не більше 60% .

4. Штрафні та заохочувальні бали

- несвоєчасне (пізніше ніж на тиждень) подання розрахункової роботи -1 бал
- заохочувальні бали за виконання творчих завдань
- успішна участь у олімпіаді з вищої математики

Максимальна кількість штрафних (заохочувальних) балів не перевищує 10% (10 балів)

Студент допускається до заліку, якщо його рейтинг семестру не менший 60 балів..

Якщо рейтинг семестру менший 60 балів, студент може написати допускову контрольну роботу. При успішному (не менше 60% правильно виконаних завдань) її написанні рейтинг семестру дорівнюватиме 60 балам.

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

$R = R_I + R_E$	**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
Менше 60	F	не допущений

- **У випадку дистанційної форми навчання у РСО відбуваються наступні зміни:**

- Контрольні заходи проводяться дистанційно із застосуванням електронної пошти, Telegram, Zoom та освітньої платформи Moodle, зокрема у вигляді тестових контрольних робіт.
- Максимальну суму вагових балів контрольних заходів протягом семестру встановлюється на рівні 100 балів.
- Допусковий бал до заліку встановлюється на рівні 60 балів.
- Сума балів набрана студентом протягом семестру згідно затвердженого РСО, повідомляється на останньому практичному занятті.
- Підтвердження виконання студентом вимог поточного контролю та умов допуску до заліку повинно бути відображено в Електронному кампусі.
- У разі не отримання студентом допускового балу, йому надається можливість підвищити R_1 шляхом проведення додаткових контрольних заходів до допускового з відповідним відображенням результатів в Електронному кампусі.
- Рівень набуття передбачених навчальною програмою компетентностей визначається на підставі проведених заходів поточного контролю, а також виконання студентом умов допуску до заліку відповідно до затвердженого РСО.

1. Додаткова інформація з дисципліни (освітнього компоненту)

У випадку дистанційної форми навчання організація освітнього процесу здійснюється з застосуванням електронної пошти, Telegram, відео-конференцій в Zoom та освітньої платформи Moodle (або Google Classroom G Suite for Education).
У разі проведення карантинних заходів РСО може бути змінено згідно наказу КПІ та рішення кафедри.

Робочу програму навчальної дисципліни (силабус):

Складено: професором кафедри МАтаТЙ, доктором фіз.-мат. наук, професором Клесовим О.І.;
Ухвалено кафедрою МАтаТЙ (протокол № 11 від 04.06.2021 р.)

Погоджено Методичною комісією ФМФ (протокол № 13 від 22.06.2021р.)