Національний технічний університет України «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»	Навчально-науковий фізико-технічний інститут Кафедра математичних методів захисту інформації

СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ (ПО-3)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Обов'язкова (нормативна) (цикл професійної та практичної підготовки)*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*Загальна кількість: (4.5 кред) 135 год* *Лекційних занять: 36 год* *Практичних занять: 18 год* *Лабораторних робіт: 18 год* *Самостійної роботи студентів: 63 год*
Семестровий контроль/ контрольні заходи	*екзамен, МКР, РР,* *поточний контроль*
Розклад занять	*http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектори: доцент Яковлєв Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua), доцент Завадська Людмила Олексіївна, к.ф.-м.н., с.н.с. (zavadskalo-ipt@lll.kpi.ua)* *Практичні: Завадська Людмила Олексіївна, к.ф.-м.н., с.н.с. (zavadskalo-ipt@lll.kpi.ua)* *Лабораторні роботи: Пекарчук Ніна Андріївна (nina.pekarchuk@gmail.com)*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

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

Робота сучасних криптографічних систем (особливо асиметричних) базується на обчислювльних алгоритмах, які працюють з дуже великими числами або у певних алгебраїчних структурах. Дисципліна «Спеціальні розділи обчислювальної математики» ознайомлює студентів

з цією тематикою взагалі та низкою конкретних схем, методів, алгоритмів та прийомів ефективної програмної реалізації компонентів сучасних криптографічних систем та їх криптоаналізу.

Метою навчальної дисципліни «Спеціальні розділи обчислювальної математики» є формування та закріплення у студентів здатностей застосовувати найуживаніші у криптології теоретико-числові, алгебраїчні та обчислювальні методи й алгоритми, а також практичних навичок їх програмної реалізації.

Предмет навчальної дисципліни: обчислювальні алгоритми, які лежать в основі побудови, функціонування та аналізу як симетричних, так і асиметричних сучасних криптосистем, включно з криптосистемами на еліптичних кривих, та їх ефективна комп'ютерна реалізація.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями.

ЗК 2 – Здатність застосовувати знання у практичних ситуаціях.

ЗК 3– Здатність генерувати нові ідеї (креативність).

ЗК 5 – Здатність проведення досліджень на відповідному рівні.

ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК 8 – Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 10 – Навички у використанні інформаційних і комунікаційних технологій.

Фахові компетентності

ФК 1 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі.

ФК 3 – Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

ФК 7 – Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.

ФК 9 – Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.

ФК 13 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

ФК 14 – Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.

ФК 18 – Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем.

Програмні результати навчання

РН 1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.

РН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати

отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів.

РН 4 – Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів.

РН 7 – Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач.

РН 9 – Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач.

РН 11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.

РН 13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.

РН 14 – Виявляти здатність до самонавчання та продовження професійного розвитку.

РН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

РН 19 – Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні

РН 21 – Вміти формулювати та розв'язувати алгебраїчні та комбінаторні задачі, будувати та реалізовувати комбінаторні алгоритми та алгоритми прикладної алгебри, аналізу вати теоретичну та практичну складність таких алгоритмів.

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

Для успішного засвоєння даної дисципліни необхідне володіння знаннями та уміннями, які набувають студенти при вивченні таких дисциплін та кредитних модулів: «Дискретна математика», «Алгебра та геометрія», «Програмування», «Прикладна алгебра», «Алгоритми та структури даних», «Математична логіка та теорія алгоритмів», «Теорія складності».

В свою чергу, результати навчання з дисципліни «Спеціальні розділи обчислювальної математики» використовуються у наступних дисциплінах: «Симетрична криптографія», «Асиметричні криптографічні системи та протоколи», «Теорія інформації та кодування».

3. Зміст навчальної дисципліни

Розділ 1. Арифметика великих чисел.

Тема 1.1. Алгоритми швидкого множення.

Тема 1.2. Алгоритми швидкої модулярної редукції.

Розділ 2. Операції у полях характеристики 2.

Тема 2.1. Поліноміальні та нормальні базиси, особливості операцій у них.

Тема 2.2. Оптимальні нормальні базиси. Множенння у ОНБ. Алгоритм Іто-Цудзиї.

Розділ 3. Розв'язання квадратних рівнянь у деяких алгебраїчних структурах.

Тема 3.1. Квадратичність. Здобування квадратних коренів у кільцях лишків.

Тема 3.2. Розв'язання квадратних рівнянь у полях характеристики 2.

Розділ 4. Еліптичні криві.

Тема 4.1. Еліптичні криві над простими скінченними полями.

Тема 4.2. Еліптичні криві над полями характеристики 2.

Розділ 5. Регістри зсуву з лінійним зворотним зв'язком.

Тема 5.1. Регістри зсуву з лінійним зворотним зв'язком, способи їх завдання, періоди вихідних послідовностей, *m*-послідовності та їх властивості.

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. *Анісімов А.В.* Алгоритмічна теорія великих чисел. К.: Академперіодика, 2001. – 218с.
2. *Завадська Л.О.* Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006 – 54с.
3. *Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я.* Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.
4. *Задірака В.К., Олексюк О.С.* Комп'ютерна криптологія. – К.: 2002. – 504 с.
5. *Задірака В., Олексюк О.* Комп'ютерна арифметика багаторозрядних чисел. Київ, 2003. – 264с.

Допоміжна рекомендована література

1. *Koblitz N.* A course in number theory and cryptography. New-York: Springer Verlag, 1993. – 179 pp.
2. *Rudolf Lidl, Harald Niederreiter.* Finite Fields. – Cambridge University Press, 2009. – 755 pp.
3. *T. Itoh and S. Tsujii.* A Fast Algorithm for Computing Multiplicative Inverses in GF(2^m) Using Normal Bases. *Information and Computation*, 78:171-177, 1988.
4. *J. L. Massey*, Shift-register synthesis and BCH decoding, IEEE Trans. Information Theory, IT-15 (1969), 122—127.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студента з метою засвоєння студентами матеріалу та розвитку у них практичних навичок. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички.

В рамках дисципліни заплановано наступні види навчальних занять:

- лекції;
- практичні заняття;
- лабораторні заняття (комп'ютерний практикум);
- самостійна робота.

Для лекційних занять використовуються пояснювально-ілюстративний та частково-пошуковий або евристичний методи, коли підчас лекції викладач пропонує студентам визначити спосіб або підходи до розв'язання тієї чи іншої проблеми (задачі), і внаслідок керованої викладачем дискусії знаходиться вірний розв'язок проблеми. На практичних заняттях використовуються метод проблемного викладу та репродуктивний метод: викладач попередньо задає студентам завдання, для виконання яких вони мають розібратися в певному теоретичному матеріалі і творчо застосувати ці знання до розв'язання поставлених задач. Після обговорення і осмислення матеріалу на практичних заняттях студенти шляхом відтворення і повторення певних дій на типових прикладах закріплюють свої знання та навички. Для проведення лабораторних робіт використовується частково-пошуковий та дослідницький методи навчання. При цьому викладач ставить перед студентами задачі створення комп'ютерних програм для специфічних, доволі складних алгоритмів, що вимагає від студентів пошуку (з допомогою викладача) та опанування нових для них програмістських прийомів.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Поняття великого числа, класичні алгоритми арифметики великих чисел. Алгоритми множення великих чисел, оцінка їх ефективності. Алгоритм Карацуби. Схема Горнера для піднесення до степеня.
2	Алгоритми модулярної редукції. Алгоритм Барретта.
3	Алгоритм Монтгомері, множення з модулярною редукцією.
4	Базиси скіченного поля. Поліноміальні та нормальні базиси. Операції у поліноміальному базисі.
5	Нормальні базиси у скінченному полі характеристики 2. Піднесення до квадрата, обчислення сліду у нормальному базисі.
6	Виконання операції множення у нормальному базисі. Мультиплікативна матриця. Гаусівські нормальні базиси, тип гаусівського нормального базису
7	Оптимальні нормальні базиси. Обчислення мультиплікативної матриці для оптимальних нормальних базисів I та II типу.
8	Обчислення оберненого за множенням елемента у нормальному базисі. Алгоритм Ітo-Цудзії.
9	Квадратичні лишки. Символи Лежандра та Якобі, їх властивості.
10	Здобування квадратних коренів за простим модулем.
11	Здобування квадратних коренів за модулем, що є добутком двох нерівних простих чисел.
12	Розв’язання квадратних рівнянь у скінченних полях характеристики 2.
13	Означення еліптичної кривої над полями різних характеристик, уведення операції додавання точок еліптичної кривої, геометрична інтерпретація.
14	Вивід формул для координат суми точок еліптичної кривої над полем характеристики не 2 і не 3. Побудова еліптичної кривої на простим полем, приклади. Знаходження порядків точок кривої.
15	Побудова еліптичної кривої над полем характеристики 2. Приклади.
16	Властивості суперсингулярних та несуперсингулярних еліптичних кривих над полем характеристики 2. Операціїї додавання у групі точок цих кривих.
17	Поняття лінійної рекурентної послідовності над скінченним полем та регістра зсуву з лінійним зворотним зв’язком.
18	Характеристичний поліном лінійного регістра зсуву, періоди лінійних рекурентних послідовностей, послідовнсті максимального періоду. Алгоритм Берлекемпа-Мессі.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Класичні алгоритми арифметики великих чисел. Алгоритм Карацуби, схема Горнера. Алгоритм Баррета, редукція Монтгомері.
2	Виконання операцій у полях характеристики 2 у поліноміальному та нормальному базисах.
3	Визначення типу гаусівського нормального базису. Виконання множення у нормальному базисі. Обчислення мультиплікативної матриці для ОНБ.
4	Здобування квадратних коренів за простим модулем та модулем, що є добутком двох нерівних простих чисел.
5	Розв’язання квадратних рівнянь у скінченних полях характеристики 2 у поліноміальному та нормальному базисах.
6	Побудова еліптичної кривої на простим полем характеристики не 2 і не 3. Обчислення координат суми точок. Знаходження порядків точок кривої.
7	Побудова еліптичної кривої над полем характеристики 2.
8	Побудова регістрів зсуву з лінійним зворотним зв’язком за характеристичним поліномом, імпульсної функції, супроводжуючої матриці. Визначення циклової

	структури регістра за властивосями характеристичного поліномому. Алгоритм Берлекемпа-Мессі.
9	Модульна контрольна робота.

Лабораторні роботи (комп'ютерний практикум)

№ заняття	Назва теми
1-2	Комп'ютерний практикум 1**.** Багаторозрядна арифметика.
3-4	Комп'ютерний практикум 2. Багаторозрядна модулярна арифметика.
5-6	Комп'ютерний практикум 3. Реалізація операцій у скінченних полях характеристики 2 (поліноміальний базис).
7-8	Комп'ютерний практикум 4. Реалізація операцій у скінченних полях характеристики 2 (нормальний базис).
9	Підведення підсумків

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями треба повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до модульної контрольної роботи.

При виконанні лабораторної роботи (комп'ютерного практикуму) студент має розібратися у відповідному теоретичному матеріалі за допомогою наданої літератури включно з методичними вказівками до даного практикуму, написати відповідну комп'ютерну програму та зробити за її допомогою вказані у методичних вказівках обчислення. Викладач, що проводить практикум, консультує студентів з питань його виконання, перевіряє правильність роботи програми та приймає усний звіт студента з питань створення комп'ютерної програми та відповідного теоретичного матеріалу. Крім того, викладачем проводиться перевірка програми на плагіат.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу. Для підготовки до виконання розрахункової роботи слід скористатися методичними вказівками до її виконання. Завдання на розрахункову роботу надає викладач, який також встановлює граничні строки для її здачі.

Розподіл часу самостійної роботи студента

№ з/п	**Вид самостійної роботи**	**Кількість годин СРС**
1.	Підготовка до лабораторних робіт	20
2.	Підготовка до практичних занять	7
3.	Підготовка до МКР	2
4.	Виконання розрахункової роботи	4
5.	Підготовка до екзамену	30

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольної та розрахункової робіт. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно. Відповідно до Наказу по КПІ 1-273 від 14.09.2020 р. заборонено оцінювати присутність або відсутність здобувача на аудиторному занятті. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, що розвивають практичні уміння та навички.

Пропущені контрольні заходи

Результат модульної контрольної роботи для студента, який не з'явився на контрольний захід, є нульовим. Якщо пропуск стався без поважної причини, студент має можливість написати контрольну, але максимальний бал за неї буде дорівнювати 60% від загальної кількості балів. У разі, якщо пропуск стався з поважних причин (наприклад, хвороби), про що бажано вчасно повідомити викладачу, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання модульної контрольної роботи не допускається.

За невчасно зданий комп'ютерний практикум накладається штраф, розмір якого залежить від величини затримки і оголошується викладачем на першому занятті. При виявленні плгіату у програмі студент має програму переробити.

Пропущений іспит не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен складати іспит на додатковій сесії.

Оголошення результатів контрольних заходів

Результати виконання контрольних заходів оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються оціночними листами, в яких студенти можуть побачити свою оцінку за певними критеріями, а також позначення основних помилок та коментарі до них.

Захист виконаного та оформленого індивідуального розрахункового завдання проводиться у формі співбесіди з викладачем. Під час захисту студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач. Результати виконаної та повністю оформленої розрахункової роботи у встановлений викладачем термін кожен студент захищає індивідуально. Результати захисту оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок.

Результати модульної контрольної роботи вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) або у листах електронної пошти чи у Classroom (при дистанційному навчанні) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

На усному екзамені студенту оголошується оцінка після закінчення відповіді на кожне теоретичне питання або задачу із зазначенням усіх помилок, коментарями, зауваженнями тощо, після чого оголошується загальна оцінка за екзамен, що є сумою оцінок за теоретичні питання та задачі.

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.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

№ з/п	Контрольний захід	Макс бал	Ваговий бал	Кіль-кість	Всього
1.	Модульна контрольна робота	10	1	1	10
2.	Розрахункова робота	15	1	1	15
3.	Лабораторна робота (комп'ютерний практикум)	7	1	4	28
4	Завдання до практичних робіт	1	1	7	7
7.	Екзамен	40	1	1	40
	Всього				100

Рейтинг студента з кредитного модуля *RD* розраховується зі 100 балів, з них 60 балів складає стартова шкала R_C .

Семестровим контролем є іспит, який проводиться в усній формі. Розмір екзаменаційної шкали R_E = 40 балів.

Стартовий рейтинг (протягом семестру) r_C складається з балів, які студент отримує за:

1) одну модульну контрольну роботу,
2) виконання 1 розрахункової роботи та її захисту,
3) виконання та захисту комп'ютерного практикуму (4 роботи),
4) виконання завдань до практичних робіт (7 робіт),
5) заохочувальних та штрафних балів.

Критерії оцінювання контрольних заходів

Модульна контрольна робота

- Повне виконання, непринципові помилки 8 -10 балів;
- Часткове виконання, істотні помилки 5 - 7 балів;
- Присутні ідеї без реалізації 3 - 4 бали;
- Роботу не зараховано 0 - 2 бали.

Максимальна кількість балів $R_{(МКР)}$ за модульну контрольну роботу – 10 балів.

Розрахункова робота

- Повне виконання, непринципові помилки, роботу захищено вчасно 13-15 балів;
- Неповне виконання (не менше 75%) , роботу захищено 10-12балів;
- Неповне виконання (менше 75%, але більше 50%), роботу захищено 8-11 балів;
- Виконання менше, ніж на 50%, але більше ніж на 25% , роботу захищено 4-7 балів;
- Виконання менше, ніж на 25% або роботу не захищено 0 балів.

Максимальна кількість балів $R_{(РР)}$ за розрахункову роботу – 15 балів.

Комп'ютерний практикум (за кожну роботу)

- Повне виконання, роботу захищено вчасно 7 балів
- Неповне виконання (не менше 75%) , роботу захищено 5-6 балів;
- Неповне виконання (менше 75%, але більше 50%), роботу захищено 4 бали;
- Повне виконання, роботу не захищено 3 бали;
- Виконання менше, ніж на 50%, але більше ніж на 25% 2 бали;

Виконання менше, ніж на 25% 0 балів.

Сумарний рейтинг за виконання комп'ютерного практикуму складається з суми балів, одержаних за виконання кожної з чотирьох робіт. Максимальна кількість балів $R_{(комп.\ пр)}$ за комп'ютерний практикум – 28 балів.

Виконання завдань до практичних робіт

- Виконання повне і вчасне, непринципові помилки 1 бал;
- Виконання вчасне, неповне (але не менше 50%) або є істотні помилки 0,5 бала;

Виконання невчасне або менше 50% 0 балів.

Заохочувальні бали

- Активність на практичних заняттях 0,5 бала за заняття
- Виконання додаткового завдання з комп'ютерного практикума 4 бали

Максимальна кількість заохочувальних балів – 8 балів.
Заохочувальні бали не входять до 100 балів семестрового рейтингу.

Штрафні бали

- Невчасна здача комп'ютерного практикуму - 1 бал за кожні 2 тижні затримки

Максимальний розмір штрафу – 6 балів.

Розмір стартової шкали R_C = 10 + 15 + 4×7 +7×1 = 60 балів.

Поточний контроль здійснюється шляхом опитування на практичних заняттях, перевірки домашніх завдань до практичних занять, модульної контрольної роботи, а також при здачі комп'ютерних практикумів та захисті розрахункової роботи.

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Календарний контроль базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Семестровий контроль (екзамен) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску є:

- стартовий рейтинг (сума балів за роботу в семестрі) $r_C \geq 36$;
- написання МКР на позитивну оцінку (≥ 3)
- виконання та захист розрахункової роботи (≥ 4);
- зарахування всіх комп'ютерних практикумів.

Під час екзамену забороняється використання будь-яких додаткових довідкових матеріалів, користування телефонами та іншими гаджетами.

Критерії екзаменаційного оцінювання:

Рейтинг студента на екзамені складається з балів, що він отримує за:

1) відповідь на теоретичне питання №1,
2) відповідь на теоретичне питання №2,
3) розв'язок задачі,
4) відповідь на додаткові питання.

Відповідь на теоретичні питання №1 та №2.

Максимальна кількість балів за відповідь на одне теоретичне питання – 12.

Результат кожної відповіді оцінюється за такими критеріями:

- повна правильна відповідь	12 балів,
- повна правильна відповідь з незначними неточностями	10-11 балів,
- неповна (у невеликій мірі) правильна відповідь з незначними неточностями	8-9 балів,
- неповна відповідь з невеликою кількістю неточностей	5-7балів,
- часткова відповідь з помилками	3-4 бали,
- відповідь на окремі несуттєві пункти в питанні з помилками	1-2 бали,
- неправильна відповідь з суттєвими помилками або відповідь не дана	0 балів.

4.2. *Розв'язок задачі.*

Максимальна кількість балів за задачу – 10.

Результат розв'я зання задачі оцінюється за такими критеріями:

- виконання завдання (розв'язок) у повному обсязі, правильна відповідь 10 балів,
- розв'язок з незначною кількістю непринципових неточностей або описок 9 балів,
- хід розв'язку правильний , відповідь невірна з причини непринципових помилок 6-8 балів,
- часткове виконання, є помилки, неповне обґрунтування або неправильна відповідь 3-5 балів,
- хід розв'язку неправильний, відповідь невірна, але у виконанні присутнє раціональне зерно та деяке розуміння задачі 1-2 бали,
- завдання не виконане або виконане з грубими помилками, немає обґрунтування відповіді 0 балів.

4.3. *Відповідь на додаткові питання.*

Для перевірки рівня засвоєння матеріалу курсу в цілому студент отримує три додаткових питання. Максимальна кількість балів за додаткові питання – 6.

Результат відповіді на кожне питання оцінюється за такими критеріями:

- вірна відповідь 2 бали,
- відповідь вірна в основному, з деякими неточностями 1 бал,
- відповідь невірна або відповіді немає 0 балів.

Максимальна кількість балів, що студент може отримати на іспиті, дорівнює:

R_E =12+12+10+6 = 40 балів.

Розмір шкали рейтингу $R = R_C + R_E = 100$

Студенти, які протягом семестру отримали менше ніж 36 балів, але виконали решту умов допуску, можуть з метою допуску до семестрової атестації (екзамену) пройти співбесіду, результат якої оцінюється максимум у 20 балів. Якщо результати співбесіди у сумі з балами, отриманими в семестрі, не менше за 36, студент отримує стартовий рейтинг r_C = 36 та допуск до екзамену.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено: доцентом кафедри ММЗІ, к.ф.-м.н., с.н.с. Завадською Л.О.

Ухвалено кафедрою математичних методів захисту інформації (протокол №6 від 22.06.2022 р.).

Погоджено Методичною комісією ННФТІ (протокол № 6 від 30.06.2022 р.).

ДОДАТОК 1

Спецрозділи обчислювальної математики

Перелік питань, які виносяться на іспит

1. Арифметика великих чисел. Алгоритм Карацуби. Відомі алгоритми множення чисел та оцінки їх складності.
2. Алгоритми швидкої модулярної редукції. Алгоритм Барретта.
3. Алгоритми швидкої модулярної редукції. Алгоритм Монтгомері.
4. Схема Горнера для піднесення до степеня. Застосування алгоритмів швидкої модулярної редукції у схемі Горнера.
5. Мультиплікативна група скінченного поля, порядки елементів скінченного поля, примітивні елементи.
6. Незвідні поліноми над скінченним полем, їх кількість. Властивості коренів незвідних поліномів. Примітивні поліноми.
7. Порядок полінома над скінченним полем. Знаходження порядків поліномів (незвідний поліном, степінь незвідного полінома, добуток ваємно-простих поліномів, поліном загального виду).
8. Спряжені елементи скінченного поля та їх властивості. Слід елемента, властивості сліду.
9. Базиси поля над підполем, поліноміальні та нормальні базиси. Операції у поліноміальному базисі.
10. Операціїї піднесння до квадрата та обчислення сліду у нормальному базисі скінченного поля характеристики 2.
11. Тип гаусівського нормального базису скінченного поля характеристики 2. Оптимальні нормальні базиси. Умови існування оптимального нормального базису поля $GF(2^m)$ при парному і непарному m.
12. Виконання операції множення у скінченних полях характеристики 2 у нормальному базисі. Обчислення мультиплікативної матриці Λ_0 для оптимальних нормальних базисів скінченного поля характеристики 2.
13. Алгоритм Ітo-Цуджиї.
14. Квадратичні лишки за простим модулем.Розв'язання рівняння виду $x^2 \equiv a \bmod p$, де p - просте виду $4k+3; 8m+5.; 8m+1.$
15. Квадратичні лишки за модулем, що є добутком двох різних простих чисел. Означення, теорема про необхідну та достатню умову квадратичності. Розв'язання рівняння виду $x^2 \equiv a \bmod n$, де n - добуток двох різних простих чисел.
16. Означення еліптичної кривої над полями різних характеристик, введення операції додавання точок еліптичної кривої над полем дійсних чисел (геометрична інтерпретація).
17. Виведення формул для координат суми та подвоєної точки еліптичної кривої над полем характеристики не 2 і не 3.
18. Побудова еліптичної кривої над скінченним полем характеристики не 2 і не 3. Приклад. Обчислення порядку кривої та порядків її точок.
19. Розв'язання рівняння виду $x^2 + ax + b = 0$ над полем $GF(2^m)$ у поліноміальному та нормальному базисах.
20. Побудова еліптичної кривої над полем характеристики 2. Приклад.
21. Операції в групах точок ЕК над полями характеристики 2.

22. Лінійні рекурентні послідовності над скінченними полями та регістри зсуву з лінійним зворотним зв’язком: означення, приклади. Форми завдання ЛРЗ.
23. Характеристичний поліном регістра зсуву з лінійним зворотним зв’язком. Залежність циклової структури множини послідовностей, що генеруються регістром, від властивостей характеристичного поліному.
24. Імпульсна функція. Лінійні рекурентні послідовності максимального періоду (m -послідовності) та їх властивості.
25. Поняття лінійної складності послідовності над скінченним полем, властивості лінійної складності. Алгоритм Берлекемпа-Мессі.