КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____О.М.Харитонов
«__» серпня 20__року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія чисел та криптографія

для студентів

галузь знань	**11 «Математика та статистика»**
спеціальність	**112 «Статистика»**
освітній рівень	**перший (бакалавр)**
освітня програма	**«Статистика»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2020/2021**
Семестр	4
Кількість кредитів ECTS	5
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: Кочубінська Євгенія Анатоліївна, к.ф.-м.н., доцент, доцент кафедри алгебри і комп'ютерної математики

Пролонговано: на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)
на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)

КИЇВ – 2020

Розробник Кочубінська Є.А., к. ф.-м. н., доцент, доцент кафедри алгебри і комп'ютерної математики

ЗАТВЕДЖЕНО
Зав. кафедри алгебри і компютерної математики
_____ Петравчук А.П.
(підпис)

Протокол №1 від 11.08 2020 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "31" 08 2020 року № 1

Голова науково-методичної комісії _____професор, д.ф.-м.н. Олійник А.С.
(підпис)

1. Мета дисципліни – оволодіння сучасними методами, теоретичними положеннями та основними застосуваннями теорії чисел до різних задачах криптографії.

2. Попередні вимоги до опанування або вибору навчальної дисципліни
1. *Знати* основні поняття, факти і теореми лінійної алгебри, алгебри, алгебри і теорії чисел, дискретної математики.
2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Теорія чисел та криптографія».
3. *Володіти елементарними навичками* роботи з множинами, функціями, знати лінійну алгебру, основні поняття із теорії чисел, знати основні поняття із теорії групи кілець.

3. Анотація навчальної дисципліни. В курсі «Теорія чисел та криптографія» висвітлюються базові відомості, поняття, факти теорії теорії чисел, криптографічних методів захисту інформації, застосування теорії чисел в криптографії.

Викладається у 2 семестрі 2 курсу в обсязі **150 год**. *(5* ***кредитів ECTS***[1]*)* зокрема: *лекції – всього 26 год., лабораторні роботи 48 год., консультації 2 год., самостійна робота – 74 год.* У курсі передбачено 2 *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна **заліком** у другому семестрі 2-го курсу.

4. Завдання (навчальні цілі):

формування здатності розв'язувати складні задачі та практичні проблеми у математиці або у процесі навчання, що передбачає застосування теорій та методів математики, статистики й комп'ютерних технологій і характеризується комплексністю та невизначеністю умов; набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у математиці, відповідно до освітнього рівня «Бакалавр». Зокрема, професійне оволодіння компетентностями:
1) Здатність до абстрактного мислення, аналізу та синтезу;
2) Здатність застосовувати знання у практичних ситуаціях;
3) Знання й розуміння предметної області та професійної діяльності;
4) Здатність спілкуватися українською мовою як усно, так і письмово;.
5) Навички використання інформаційних і комунікаційних технологій;
6) Здатність вчитися і оволодівати сучасними знаннями;
7) Здатність до пошуку, обробки та аналізу інформації з різних джерел;
8) Здатність приймати обґрунтовані рішення;
9) Здатність працювати автономно;
10) Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків;
11) Здатність оцінювати та забезпечувати якість виконуваних робіт;
12) Здатність діяти на основі етичних міркувань (мотивів).
13) Здатність здійснювати логічні математичні міркування із чітким зазначенням припущень та висновків ;
14) Здатність до математичного формулювання задач та вибору методів їх розв'язання ;
15) Здатність робити якісні висновки з кількісних даних.

5. Результати навчання за дисципліною:

[1] кредитів ECTS – кредит кратний 30 годинам.

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання за необхідності	Відсоток у підсумковій оцінці з дисципліни
Код	**Результат навчання**			
1.1	Знати: поняття групи, циклічної групи, поля, скінченного поля, характеризацію скінченних полів, поняття симетричної та асиметричної схем шифрування.	лекція, самостійне опрацювання	опитування під час лекції, модульна контрольна №1	10%
1.2	Знати: означення та властивості функції Ейлера, будову мультиплікативної групи кільця лишків, формулювання задачі факторизації та алгоритми її розв'язання (метод Ферма, метод Полларда, метод випадкових квадратів), принцип роботи криптосистеми RSA.	лекція, самостійне опрацювання	опитування під час лекції, модульна контрольна №1	10%
1.3	Знати: властивості мультиплікативної групи скінченного поля, примітивного елемента скінченного поля, дискретного логарифма, формулювання задачі Діффі-Хелмана, принцип роботи криптоситеми Ель Гамаля, принцип роботи алгоритму Діффі-Хелмана.	лекція самостійне опрацювання	опитування під час лекцій, модульна контрольна №2	10%
1.4	Знати: означення квадратичного лишка, символа Лежандра, принцип роботи криптосистеми Гольвассер-Мікалі.	лекція, самостійне опрацювання	опитування під час лекцій, модульна контрольна №2	5%
2.1	Уміти: застосовувати алгоритми Полларда та Ферма для роз'вязування задачі факторизації.	самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	15%
2.2	Уміти: застосовувати алгоритм шифрування RSA та відповідну схему цифрового підпису.	самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	20%
2.3	Уміти: застосовувати алгоритм Шенкса знаходження дискретного лограрифму.	самостійне опрацювання	перевірка індивідуальних завдань, самостійна робота, модульна контрольна робота	15%
2.4	Уміти: обчислювати спільне таємне значення за допомогою алгоритму Діффі-Хелмана.	самостійне опрацювання	перевірка індивідуальних завдань, самостій-	10%

			на робота	
3.1	Здатність обґрунтовувати власний погляд на задачу та формулювати робочі гіпотези, спілкуватися з колегами з питань застосування математичних методів та теорій	Лекція, самостійна робота	активна робота на лекції, усні відповіді	2.5%
3.2	Вироблення навиків командної роботи	Лекція, самостійна робота	активна робота на лекції, усні відповіді	2.5%

6. Співвідношення результатів навчання дисципліни з програмними результатами

Результати навчання дисципліни / **Програмні результати навчання** (*з опису освітньої програми*)	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 1.4**	**РН 2.1**	**РН 2.2**	**РН 2.3**	**РН 2.4**	**РН 3.1**	**РН 3.2**
РН-1 - Здійснювати професійну письмову й усну комунікацію українською мовою та, принаймні, однією з іноземних мов	+	+	+	+	+	+	+	+	+	+
РН-14 - Володіти сучасними інформаційними технологіями для створення презентацій, роботи з базами даних, пошуку інформації та обміну нею	+		+		+		+			
РН-16 - Вміти використовувати в практичній діяльності спеціалізоване статистичне програмне забезпечення			+		+		+			

7. Схема формування оцінки.

7.1. Форми оцінювання студентів:

- оцінювання впродовж навчального періоду:

1. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2, РН2.3, РН2.4 – 8 балів/4 бали

2. Модульна контрольна робота 1: РН1.1, РН1.2, РН2.1, РН2.2 – 20 балів/12 балів;

3. Модульна контрольна робота 2: РН1.3, РН1.4 РН2.3 –20 балів/12 балів;

4. Розв'язання задач на практичних заняттях: РН2.1, РН2.2, РН2.3, РН2.4, РН3.1, РН3.2, – 12 балів/7 бали;

Разом має бути 60/35

- підсумкове оцінювання: залік.

- максимальна кількість балів, які можуть бути отримані: 40 балів;

- результати навчання, які будуть оцінюватись:

Вміння формулювати і доводити основні теореми із викладеної в курсі теорії кілець, вміння знаходити ніль-радикал кільця, тензорні добутки модулів, розвязувати задачі про основні властивості нетерових кілець, здійснювати основні операції в скінченних кільцях, знаходити кількість незвідних многочленів над скінченними полями, знаходити норму і слід елемента поля, застосовувати отримані знання для кодування інформаційних векторів за допомогою циклічних кодів, застосовувати еліптичні криві в криптографії

РН2.2, РН2.3, РН2.4;
- *форма проведення і види завдань:* письмова робота.

7.2. Організація оцінювання:
Самостійна робота передбачає активну самостійну роботу по розвязанню задач і по формулюванню основних теоретичних положень під час практичних занять, при цьому кожен студент отримує індивідуальне завдання, яке він повинен виконати за невеликий проміжок часу (складність завданя пропорційно відведеному часу)
Критично-розрахунковий мінімум балів за навчання впродовж семестру становить **20** балів, рекомендований мінімум, розрахований з урахуванням специфіки дисципліни становить **35** балів. Студенти, які протягом семестру набрали сумарно меншу кількість балів ніж рекомендований мінімум **35** балів для підвищення балів отримують можливість написати додаткову контрольну роботу та доскласти домашні завдання. Мінімальна кількість балів, які додаються до семестрових – 20 балів, тобто, якщо оцінка студента на заліку є нижчою від мінімального порогового рівня (20 балів), то бали за залік не додаються до семестрової оцінки;
У випадку відсутності студента з поважних причин відпрацювання та перездачі форм контролю здійснюються у відповідності до „Положення про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка" (2018), http://www.univ.kiev.ua/pdfs/official/Organization-of-the-educational-process.pdf.

Форма заліку – письмово-усна. Білет складається із 5 завдань, перші два з яких є теоретичними, три інших – задачі. Кожне завдання оцінюються від 0 до 7 балів. Додатково від 0 до 5 балів студент отримує за усне опитування. Всього за залік можна отримати від 0 до 40 балів.

Терміни проведення форм оцінювання:

1. Модульна контрольна робота №1: на 3-му тижні 1 семестру.

2. Модульна контрольна робота №2: на 9-му тижні 1 семестру

3. Оцінювання завдань самостійної роботи за РН2.1 на 3-му тижні, за РН2.2 на 6 тижні, за РН2.3 на 12 тижні 1 семестру

7.3 Шкала відповідності оцінок

Зараховано/ Passed	60 – 100
Не зараховано/ Fail	0 – 34

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ЛАБОРТОРНИХ РОБІТ

Теми	Назва теми **І семестр**	Кількість годин				
		Лекції	Лабораторні роботи	Самост. робота	Модульна контрольна	Інші форми контролю
Змістовий модуль 1 „Елементарна теорія чисел. Факторизація та RSA "						
1	Деякі питання елементарної теорії чисел. Поняття криптографії з відкритим ключем.	6	10	18		
2	Задача факторизації та криптосистема RSA	6	12	18	2	

Змістовий модуль 2 „ Скінченні поля і їх застосування ”						
3	Будова скінченних полів. Дискретний логарифм та його застосування у криптографічних задачах.	8	14	20	2	
4	Квадратичні лишки. Криптоситема Гольвассер-Мікалі.	6	12	18		
Всього годин		26	48	74	4	

Загальний обсяг 150 годин, у тому числі:
лекції – 26 годин,
лабораторні роботи – 48 годин
консультації – 2 годин,
самостійна робота – 74 годин.

9. Рекомендовані джерела

Основні:

1. Э. Б. Винберг Курс алгебры, М.Факториал Пресс, 2002.
2. Н. Коблиц. Курс теории чисел и крипторграфии. М.: ТВП, 2001.
3. Hoffstein J., Pipher J., Silverman J. An introduction to mathematical cryptography. Springer, 2008.
4. Koblitz N. Algebraic aspects of cryptography. Algorithms and Computation in Mathematics, Berlin: Springer. 2004, 206 p.

Додаткові:

1. H.Matsumura, «Commutative Ring Theory» Cambridge University Press, 1986
2. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х тт. — М.: Мир, 1988.
3. R.Bose, Information Theory, Coding Theory and Cryptography, Third edition, McGraw Hill Education, 2008, 463p.
4. Вернер М. Основы кодирования, Техносфера. 2004, 286с.