КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи

_____ Харитонов О.М

«____»_____20 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Постквантова криптографія

для студентів

галузь знань	**01 «Освіта/Педагогіка»**
спеціальність	**«014 Середня освіта (за предметними спеціальностями)»**
предметна спеціальність	**014.04 «Середня освіта (Математика)»**
освітній рівень	перший (бакалавр)
освітня програма	**«Математика»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**20 /20**
Семестр	**8**
Кількість кредитів ECTS	**3**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладачі: Олійник А.С., д. ф.-м. н., доцент, професор кафедри алгебри і комп'ютерної математики

Пролонговано: на 20 /20 н.р. ( ) « » 20 р.
на 20 /20 н.р. ( ) « » 20 р.

КИЇВ – 20

Розробник Олійник А.С., д. ф.-м. н., доцент, професор кафедри алгебри і комп'ютерної математики

ЗАТВЕДЖЕНО
Зав. кафедри алгебри і комп'ютерної математики

_____ Петравчук А.П.
(підпис)

Протокол № від 20 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "____" _____ 20 року № ___

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

1. Мета дисципліни – ознайомлення з основними методами побудови криптографічних алгоритмів, стійких до квантових атак, оволодіння математичних апаратом, який лежить в основі розробки та використання відповідних криптографічних інструментів, використання в процесі навчання математики.

2. Попередні вимоги до опанування навчальної дисципліни:
1. *Знати* основні поняття, факти і теореми лінійної алгебри, алгебри і теорії чисел, дискретної математики, теорії ймовірностей, теорії складності, основні навички з програмування.
2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Постквантова криптографія».
3. *Володіти елементарними навичками* роботи з векторними просторами, скінченними групами, кільцями і полями, вміти будувати оцінки складності алгоритмів, проводити обчислення за допомогою спеціалізованого програмного забезпечення.

3. Анотація навчальної дисципліни.
Навчальна дисципліна «Постквантова криптографія» є складовою освітньої програми підготовки фахівців за освітнім рівнем «бакалавр» галузі знань 01 Освіта зі спеціальності 014 Середня освіта освітньої програми «Математика». Дана дисципліна є вибірковою. В курсі «Постквантова криптографія» розглядаються цілочисельні решітки, їх алгебраїчні та геометричні характеристики, редуковані базиси, алгоритм LLL та його застосування, криптосистеми на основі решіток, їх стійкість до квантових атак, білінійне спарювання, алгоритм Міллера, криптосистеми на основі спарювання та їх застосування.

Викладається у **8** семестрі **4** курсу в обсязі **90 год**. ***(3 кредитів ECTS[1])*** зокрема: *лекції – всього 28 год., консультації 2 год., самостійна робота – 60 год.* У курсі передбачено 2 *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна **іспитом** у восьмому семестрі.

4. Завдання (навчальні цілі): формування здатності розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі середньої освіти, що передбачає застосування теорій та методів педагогіки та математики і характеризується комплексністю та невизначеністю педагогічних умов організації навчально-виховного процесу в основній (базовій) середній школі; набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у педагогіці та математиці, відповідно до освітнього рівня «Бакалавр». Зокрема, професійне оволодіння компетентностями:

1) Здатність до абстрактного мислення, аналізу та синтезу (ЗК-1);
2) Здатність застосовувати знання у практичних ситуаціях (ЗК-2)
3) Знання й розуміння предметної області та професійної діяльності (ЗК-3)
4) Здатність спілкуватися державною мовою як усно, так і письмово (ЗК-4);
5) Здатність спілкуватися іноземною мовою (ЗК-5);
6) Навички використання інформаційних і комунікаційних технологій (ЗК-6);
7) Здатність учитися і оволодівати сучасними знаннями (ЗК-7)
8) Здатність до пошуку, обробки та аналізу інформації з різних джерел (ЗК-8);
9) Здатність приймати обґрунтовані рішення (ЗК-9);
10) Здатність працювати в команді (ЗК-10);
11) Здатність працювати автономно (ЗК-11);

1 кредитів ECTS – кредит кратний 30 годинам.

12) Здатність до адаптації та дії в новій ситуації (ЗК-16)
13) Здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання (СК-1);
14) Здатність подавати математичні міркування та висновки з них у формі, придатній для цільової аудиторії, а також аналізувати та обговорювати математичні міркування інших осіб, залучених до розв'язання тієї самої задачі (СК -2);
15) Здатність до кількісного мислення (СК-3);
16) Здатність розробляти і досліджувати математичні моделі явищ, процесів та систем (СК-4)
17) Здатність застосовувати спеціалізовані мови програмування та пакети прикладних програм (СК-5);
18) Здатність до комунікації з фаховими спільнотами державною (українською) мовою (СК-6);
19) Здатність до формування у учнів ключових і предметних компетентностей та здійснення міжпредметних зв'язків (СК-7);
20) Здатність здійснювати об'єктивний контроль і оцінювання рівня навчальних досягнень учнів (СК-9);
21) Здатність формувати в учнів критичне мислення, переконання в необхідності обґрунтування гіпотез, розуміння математичного доведення та математичного моделювання (СК-17);
22) Здатність забезпечувати розвиток прийомів розумової діяльності та просторової уяви учнів, усвідомлюючи й реалізуючи специфічні можливості процесу навчання математики для розвитку логічного та алгоритмічного мислення (СК-19);

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація)		**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: основні поняття і властивості цілочисельних решіток, алгоритмічні задачі на решітках, LLL алгоритм та його застосування	лекція, самостійне опрацювання	іспит, модульна контрольна робота 1, опитування під час лекцій	5%
1.2	Знати: криптосистеми GGH та NTRU, методи їх криптоаналізу, принцип побудови гомоморфних криптосистем	лекція, самостійне опрацювання	іспит, модульна контрольна робота 1, опитування під час лекцій	10%
1.3	Знати: поняття білінійного спарювання, групи дівізорів еліптичної кривої, алгоритм Міллера	лекція, самостійне опрацювання	іспит, модульна контрольна робота 2, опитування під час лекцій	10%
1.4	Знати: поняття функціональної криптосистеми, приклади криптосистем на основі ідентифікаторів та на основі скалярного добутку	лекція, самостійне опрацювання	іспит, модульна контрольна робота 2, опитування під час лекцій	5%

2.1	Уміти: обчислювати алгебраїчні та геометричні інваріанти цілочисельних решіток, застосовувати LLL алгоритм	практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота 1, іспит	12.5%
2.2	Уміти: застосовувати криптосистеми GGH та NTRU, проводити їх криптоаналіз	практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота 1, іспит	20%
2.3	Уміти: виконувати обчислення з дівізорами, застосовувати алгоритм Міллера для обчислення значень білінійних спарювань	практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота 2, іспит	20%
2.4	Уміти: застосовувати криптосистеми на основі ідентифікаторів та на основі скалярного добутку	практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, контрольна робота 2, іспит	12.5%
3.1	Здатність обґрунтовувати власний погляд на задачу та формулювати робочі гіпотези, спілкуватися з колегами з питань застосування математичних методів та теорій	лекція, практичне заняття, самостійна робота	активна робота на лекції, усні відповіді	2.5%
3.2	Вироблення навиків командної роботи	лекція, практичне заняття, самостійна робота	активна робота на лекції, усні відповіді	2.5%

6. Співвідношення результатів навчання дисципліни з програмними результатами

Результати навчання дисципліни **Програмні результати навчання**	**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**
Має навички використання спеціалізованих програмних засобів комп'ютерної та прикладної математики і використовувати інтернет-ресурси (РН-3)					+	+	+	+		

Використовує усно і письмово професійну українську мову (РН-4)	+	+	+	+	+	+	+	+	+	+
Знає та розуміє принципи, форми, сучасні методи, методичні прийоми навчання математики в закладах середньої освіти (рівень базової середньої освіти) (РН-6)									+	+
Знає та розуміє особливості навчання різнорідних груп учнів, застосовує диференціацію навчання, організовує освітній процес з урахуванням особливих потреб учнів (РН-7)									+	+
Оперує базовими категоріями та поняттями математики (РН-8)	+	+	+	+	+	+	+	+	+	
Здатний демонструвати та застосовувати знання з математики, необхідні для формування математичних компетентностей учнів (РН-16)	+	+	+	+	+	+	+	+	+	+
Знає, розуміє і здатний використати рекомендації з методики навчання математики для виконання освітньої програми з математики в базовій середній школі (РН-17)	+	+	+	+	+	+	+	+	+	+
Уміє розв’язувати задачі різних рівнів складності шкільного курсу математики (РН-21)					+	+	+	+	+	
Здатний формувати в учнів розуміння основ математичного моделювання, готовність до застосування моделювання для розв’язування задач (РН-22)	+	+	+	+	+	+	+	+	+	
Здатний до ефективної комунікації в процесі навчання учнів математиці, до пошуку та обробки нової інформації, до використання сучасних інформаційних технологій (РН-25)	+	+	+	+	+	+	+	+	+	
Здатний оцінювати та розвивати власні математичні й методичні компетентності, усвідомлювати відповідальність за їх рівень (РН-26)	+	+	+	+	+	+	+	+	+	
Формує ціннісний аспект математичного знання, координує його емоційне сприйняття учнями, розробляє і пропонує різні форми та прийоми виховання позитивного ставлення до математики, мотивації учнів до засвоєння її основ та методів (РН-27)									+	+

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 – 10 балів/5 бали;

2. Модульна контрольна робота 1: РН1.1, РН1.2, РН2.1, РН2.2 – 25 балів/14 балів;
3. Модульна контрольна робота 2: РН1.3, РН1.4, РН2.3, РН2.4 –25 балів/14 балів;
- підсумкове оцінювання: іспит.
- *максимальна кількість балів, які можуть бути отримані:* 40 балів;
- *результати навчання, які будуть оцінюватись:* РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2, РН2.3, РН2.4;
- *форма проведення і види завдань:* письмова робота.

7.2. Організація оцінювання:
Самостійна робота передбачає активну роботу по розв'язанню задач і формулюванню основних теоретичних положень під час лабораторних та практичних занять, при цьому кожен студент отримує індивідуальне завдання, яке він повинен виконати за обмежений проміжок часу (складність завдання є пропорційною відведеному на його виконання часу). Активна робота на лекціях передбачає виконання тестових завдань за лекційним матеріалом. 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 – **24** бали, тобто, якщо оцінка студента на іспиту є нижчою від мінімального порогового рівня (**24** бали), то бали за іспит не додаються до семестрової оцінки (вважаються рівними нулю), а підсумкова оцінка з дисципліни є незадовільною.

Терміни проведення форм оцінювання:
1. Модульна контрольна робота №1: на 7-му тижні 2 семестру 4-го курсу.
2. Модульна контрольна робота №2: на 11-му тижні 2 семестру 4-го курсу.
3. Оцінювання завдань самостійної роботи за РН2.1 *на* 3-му тижні, за РН2.2 на 6 тижні, за РН2.3 на 12 тижні, за РН2.4 на 16 тижні.

Форма іспиту – письмово-усна. Екзаменаційний 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 іспит можна отримати від 0 до 40 балів.

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.

7.3 Шкала відповідності оцінок:

Відмінно/ Excelent	90 – 100
Добре/ Good	75 – 89
Задовільно/ Satisfactory	60 – 74
Не задовільно/ Fail	0 – 59
Зараховано/ Passed	60 – 100
Не зараховано/ Fail	0 – 34

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ

№ п/п	Назва теми	Кількість годин			
		Лекції	Самост. робота	Модульна контрольна робота	Інші форми контролю
Змістовий модуль 1 „Криптосистеми на основі решіток”					
1	Цілочисельні решітки	8	16		
2	Криптосистеми, стійкі до квантових атак	8	14	2	
Змістовий модуль 2 „Криптосистеми на основі спарювання”					
3	Білінійне спарювання	6	16		
4	Функціональне шифрування	6	14	2	
Всього годин		28	60	4	

Загальний обсяг 90 годин, у тому числі:
лекції – 28 годин,
консультації – 2 години,
самостійна робота – 60 годин.

9. Рекомендовані джерела

Основні:

1. D. Boneh, V. Shoup A graduate course in applied cryptography, 2020.
2. I. F. Blake, G. Seroussi, N. P. Smart (Eds.) Advances in elliptic curve cryptography, Cambridge University Press, 2005.
3. J. Katz, Y. Lindell Introduction to modern cryptography CRC Press, 2015.
4. J.H. Silverman, J. Pipher, J. Hoffstein An introduction to mathematical cryptography, Springer, 2008.

Додаткові:

5. S. D. Galbraith Mathematics of public key cryptography, Cambridge University Press, 2012.
6. A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi Classical and quantum computation, AMS, 2002.
7. P. Q. Nguyen, B. Vall´ee (Eds.) The LLL algorithm. Survey and applications, Springer, 2010.
8. N.P. Smart Cryptography made simple, Springer, 2016