КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Олексій ХАРИТОНОВ
«31» серпня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математична 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	**обов'язкова**

Форма навчання	**денна**
Навчальний рік	**2021/2022**
Семестр	**6**
Кількість кредитів ECTS	**6**
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 – 2021

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

ЗАТВЕРДЖЕНО
Зав. кафедри алгебри і комп'ютерної математики

_____ Петравчук А.П.
(підпис)

Протокол № 1 від 31.08 2021 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "31" 08 2021 року № 1

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

1. Мета дисципліни – ознайомлення з основними поняттями, алгоритмами і методами сучасної криптографії та її математичними основами, а також практичними застосуваннями криптографії, програмними засобами роботи з криптографічними інструментами, методами застосування прикладних розділів математики при викладанні математики.

2. Попередні вимоги до опанування навчальної дисципліни:
1. *Знати* основні поняття, факти і теореми алгебри, конкретної математики, дискретної математики, теорії ймовірностей, теорії інформації та кодування, мати основні навички з програмування.
2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Математична криптографія».
3. *Володіти елементарними навичками* роботи з підстановками, лишками за модулем натуральних чисел, скінченними полями, дискретними ймовірносними просторами, матрицями та многочленами.

3. Анотація навчальної дисципліни.
Навчальна дисципліна «Математична криптографія» є складовою освітньої програми підготовки фахівців за освітнім рівнем «бакалавр» галузі знань 01 «Освіта/Педагогіка», спеціальності 014 «Середня освіта (за предметними спеціальностями)», предметної спеціальності 014.04 «Середня освіта (Математика)». Дана дисципліна є обов'язковою. В курсі «Математична криптографія» висвітлюються базові відомості, поняття та факти сучасної криптографії. Зокрема, розглядаються: поняття симетричної та асиметричної криптосистеми, блочні шифри, потокові шифри, криптографічні хеш функції, ймовірносні алгоритми, задачі факторизації та дискретного логарифма, криптосистеми RSA та ЕльГамаля, схеми цифрового підпису, протоколи узгодження ключів.

Викладається у **6** семестрі **3** курсув обсязі **180 год**. *(6* ***кредитів ECTS***[1]*)*зокрема: *лекції – 28 год., лабораторні - 28 год., практичні - 28 год., консультації - 4 год., самостійна робота – 92 год.* У курсі передбачено 2*змістових модулі* та 2 *модульніконтрольні роботи*. Завершується дисципліна **екзаменом** у другому семестрі 3-го курсу.

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 учитися і оволодівати сучасними знаннями (ЗК-7)
6) Здатність до пошуку, обробки та аналізу інформації з різних джерел (ЗК-8);
7) Здатність працювати автономно (ЗК-11);

[1] кредитів ECTS – кредит кратний 30 годинам.

8) Здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання (СК-1);
9) 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);
10) Здатність до кількісного мислення (СК-3);
11) Здатність розробляти і досліджувати математичні моделі явищ, процесів та систем (СК-4)
12) Здатність до комунікації з фаховими спільнотами державною (українською) мовою (СК-6);
13) Здатність до формування у учнів ключових і предметних компетентностей та здійснення міжпредметних зв'язків (СК-7);
14) Здатність здійснювати об'єктивний контроль і оцінювання рівня навчальних досягнень учнів (СК-9);
15) Здатність застосовувати системні знання з математики та методики навчання математиці, історії їх виникнення та розвитку (СК-14);
16) Здатність аналізувати сприйняття та засвоєння учнями математичних фактів та методів із метою визначення ефективності використання прийомів та засобів навчання (СК-15);
17) Здатність розв'язувати задачі шкільного курсу математики різного рівня складності та формувати відповідні уміння в учнів (СК-16);
18) Здатність формувати в учнів критичне мислення, переконання в необхідності обґрунтування гіпотез, розуміння математичного доведення та математичного моделювання (СК-17);
19) 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; 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 криптосистеми, алгоритмів шифрування та дешифрування, симетричної криптосистеми, історичні шифри, методи конвертації бінарних даних, шифри AES та Калина	лекція, самостійне опрацювання	Екзамен, модульна контрольна робота 1, опитування під час лабораторних та практичних занять	5%
1.2	Знати: поняття потокового шифру, потокові режими блочних шифрів, поняття криптографічної хеш функції, , парадокс днів народження, метод Меркла-Дамгарда, криптографічні хеш функції SHA-2 і Купина, методи доповнення повідомлень, алгоритми генерування секретних ключів	лекція, самостійне опрацювання	Екзамен, модульна контрольна робота 1, опитування під час лабораторних та практичних занять	10%
1.3	Знати: поняття ймовірносного алгоритму, ймовірносні алгоритми шифрування,	лекція,	Екзамен, модульна контрольна робота 2,	

	основні методи криптоаналізу асиметричних шифрів, алгоритми тестування простоти, криптосистему RSA, задачу дискретного логарифма, криптосистему ЕльГамаля	самостійне опрацювання	опитування під час лабораторних та практичних занять	5%
1.4	Знати: поняття цифрового підпису, сертифіката публічного ключа, інфраструктури публічних ключів, цифрові підписи DSA та Шнорра, протокол узгодження ключів Діффі-Хелмана	лекція, самостійне опрацювання	Екзамен, модульна контрольна робота 2, опитування під час лабораторних та практичних занять	10%
2.1	Уміти: використовувати історичні шифри, проводити їх криптоаналіз, імплементувати криптосистеми AES та Калина	лабораторне, практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота №1, залік	12.5%
2.2	Уміти: використовувати потокові режими блочних шифрів, імплементувати криптографічні хеш-функції, проводити криптоаналіз криптографічних хеш-функцій, генерувати криптографічні ключі	лабораторне, практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота , екзамен	20%
2.3	Уміти: досліджувати ймовірності алгоритми, використовувати тести простоти, імплементувати криптосистему RSA, проводити криптоаналіз криптосистем з публічним ключем	лабораторне, практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота 2, екзамен	12.5%
2.4	Уміти: використовувати схеми цифрового підпису, імплементувати схему цифрового підпису DSA, використовувати протокол узгодження ключів Діффі-Хеллмана	лабораторне, практичне заняття, самостійне опрацювання	перевірка індивідуальних завдань, самостійна аудиторна робота, контрольна робота2, екзамен	20%
3.1	Здатність обґрунтовувати власний погляд на задачу та формулювати робочі гіпотези, спілкуватися з колегами з питань застосування математичних методів та теорій	лекція, лабораторне, практичне заняття, самостійна робота	активна робота на лекції, лабораторних та практичних заняттях, усні відповіді	2.5%
3.2	Вироблення навиків командної роботи	лекція, лабораторне, практичне заняття, самостійна робота	активна робота на лекції, лабораторних та практичних заняттях, 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**
РН-1. Знає основні етапи історичного розвитку математичних знань і парадигм, розуміти сучасні тенденції в математиці.	+	+	+	+	+	+	+	+	+	+
РН-2. Розуміє фундаментальну і прикладну математику на рівні, необхідному для досягнення інших вимог освітньої програми.	+	+	+	+	+	+	+	+	+	+
РН-4. Використовує усно і письмово професійну українську мову.	+	+	+	+	+	+	+	+	+	+
РН-6. Знає та розуміє принципи, форми, сучасні методи, методичні прийоми навчання математики в закладах середньої освіти (рівень базової середньої освіти).		+	+	+	+	+	+	+	+	+
РН-7. Знає та розуміє особливості навчання різнорідних груп учнів, застосовує диференціацію навчання, організовує освітній процес з урахуванням особливих потреб учнів.					+	+	+	+	+	+
РН-11. Добирає і застосовує сучасні освітні технології та методики для формування предметних компетентностей учнів і здійснює самоаналіз ефективності уроків.	+	+	+	+	+	+	+	+	+	
РН-16. Здатний демонструвати та застосовувати знання з математики, необхідні для формування математичних компетентностей учнів.	+	+	+	+	+	+	+	+	+	
РН-17. Знає, розуміє і здатний використати рекомендації з методики навчання математики для виконання освітньої програми з математики в базовій середній школі.					+	+	+	+	+	+
РН-21. Уміє розв’язувати задачі різних рівнів складності шкільного курсу математики.	+	+	+	+	+	+	+	+	+	+
РН-22. Здатний формувати в учнів розуміння основ математичного моделювання, готовність до застосування моделювання для розв’язування задач.		+	+	+	+	+	+	+	+	+
РН-25. Здатний до ефективної комунікації в процесі навчання учнів математиці, до пошуку та обробки нової інформації, до використання сучасних інформаційних технологій.	+	+	+	+	+	+	+	+	+	+
РН-26. Здатний оцінювати та розвивати власні математичні й методичні компетентності, усвідомлювати відповідальність за їх рівень.					+	+	+	+		

РН-27. 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.	+	+	+	+						

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 лабораторних та практичних заняттях: РН2.1, РН2.2, РН2.3, РН2.4, РН3.1, РН3.2, – 12 балів/7 балів;

- підсумкове оцінювання: екзамен.

- *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 іспиті 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 3-го курсу.

2. Модульна контрольна робота №2: на 11-му тижні 2 семестру 3-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. 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.

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/ Excellent	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	Лабораторні	Практичні заняття	Самост. робота	Модульна контрольна робота	Інші форми контролю
Змістовий модуль 1 „Симетрична криптографія”							
1	Симетричні шифри	8	6	6	22		
2	Потокові шифри і криптографічні хеш функції	6	8	8	24	2	
Змістовий модуль 2 „Асиметрична криптографія”							
3	Криптосистеми з публічним ключем	8	6	6	22		
4	Цифрові підписи за протоколи узгодження ключів	6	8	8	24	2	
Всього годин		28	28	28	92	4	

Загальний обсяг 180 годин, у тому числі:
лекції – 28 годин,
лабораторні - 28 годин,
практичні заняття – 28 годин,
консультації – 4 години,
самостійна робота – 92 години.

9. Рекомендовані джерела

Основні:

1. J.-P.Aumasson*Seriouscryptography*.Nostarchpress, 2018.
2. C. Paar, J. Pelzl*Understandingcryptography*.Springer, 2010.
3. N.Smart*Cryptographymadesimple*. Springer, 2016.
4. О.Вербіцький*Вступ до криптології.* ВНТЛ, 1998.

Додаткові:

5. J.H. Silverman, J. Pipher, J. Hoffstein*Anintroductiontomathematicalcryptography.*Springer, 2008.
6. J. Katz, Y. Lindell*Introductiontomoderncryptography.* CRC Press, 2015.
7. H.Bidgoli (Ed.) *HandbookofInformationSecurity,*Volume 1. JohnWiley&SonsInc., 2006.