СИЛАБУС
Навчальної дисципліни

Вступ до криптографії
вид дисципліни **за вибором**

рівень вищої освіти **бакалавр;** галузь знань **11 – Математика та статистика;** спеціальність **111 - «Математика»;** освітня програма **«Математика»;** факультет **математики і інформатики**

РОЗРОБНИК: **Каролинський Евген Олександрович**, кандидат фізико-математичних наук,
доцент кафедри фундаментальної математики, доцент.

1. Опис навчальної дисципліни

Мета курсу полягає у навчанні майбутніх спеціалістів основам криптографії з відкритим ключем, а також необхідним відомостям з теорії чисел.
Основні завдання курсу є навчання студентів основам алгоритмічних аспектів арифметики і їх застосуванню в сучасній криптографії.
Кількість кредитів – 3
Загальна кількість годин – 90

2. Тематичний план навчальної дисципліни

Розділ 1. Відомості з теорії чисел.

1. Складність арифметичних дій.
2. Алгоритм Евкліда і його складність.
3. Прості числа. Факторіальність кільця цілих чисел.
4. Порівняння і кільця лишків.
5. Огляд теорії полів.
6. Скінченні поля.
7. Квадратичні лишки. Квадратичний закон взаємності.
8. Обчислення квадратного кореня в скінченному полі.

Розділ 2. Елементи криптографії.

1. “Класична” криптографія.
2. Криптографічна система RSA.
3. Перевірка чисел на простоту. Тести Ферма, Соловея-Штрассена, Міллера-Рабіна.
4. Розкладання чисел на множники: ρ-метод Полларда, метод факторних баз.
5. Дискретний логарифм. Криптографічні системи Діффі-Хеллмана.

3. Методи навчання

Лекційно-практичні**.** Лекції та практичні заняття проводяться аудиторно. У разі оголошення карантину та ув умовах воєнного стану заняття проводяться аудиторно або дистанційно (за допомогою платформ ZOOM, MOODLE) відповідно до наказу ректора Харківського національного університету імені В.Н.Каразіна.

4. Методи контролю

1) поточний семестровий: Контрольна робота (1) 2) підсумковий семестровий (залік).

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка за національною шкалою	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90–100	відмінно	зараховано
70–89	добре	
50–69	задовільно	
1–49	незадовільно	не зараховано

5. Рекомендована література

Основна література

1. James S. Kraft (Author) An Introduction to Number Theory with Cryptography, Chapman and Hall/CRC; 1st edition (Sept. 6 2013)
2. Н. Кобліц. Курс теорії чисел та криптографії. М.: ТВП, 2001.

Допоміжна література

1. S. D. Galbraith. Mathematics of Public Key Cryptography. Cambridge Univ. Press, 2012.

6. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC