Факультет прикладної математики та інформатики
Кафедра прикладної математики

ПРОГРАМА КУРСУ
“ Основи криптології ”

Напрям : прикладна математика
Факультет : прикладної математики та інформатики
Форма навчання : денна

факультету прикладної математики та інформатики

Форма навчання	Курс	Семестр	Загальний обсяг (год.)	Всього аудит. (год.)	у тому числі (год.):			Самостійна робота (год.)	Контрольні (модульні) роботи (шт.)	Розрахунково-графічні роботи (шт)	Курсові проекти (роботи), (шт.)	Залік (сем.)	Екзамен (сем.)
					Лекції	Лабораторні	Практичні						
Денна	4	8	56	58	28	28		56	2			+	

Анотація. Завдання захисту інформації в комп’ютерних і телекомунікаційних мережах набули особливого значення. Без їхнього вирішення не можна провадити жодного типу інформаційної діяльності. Аналіз різних видів загроз дає змогу визначити головні завдання захисту, які ґрунтуються на використанні криптологічних алгоритмів і протоколів.

Даний курс умовно розбитий на три основні розділи. Перший присвячений історичному екскурсу від стародавнього світу до нині. Тут вивчаються такі класичні методи як поліграмні шифри та поліалфавітні шифри; шифрування блоками та шифри перестановки; шифр одноразового блокноту та стандарт шифрування даних DES.

Другий розділ присвячений ознайомленню з базовими поняттями теорії складності обчислень. У курс цього розділу ввійшло вивчення поняття конгруенції та її основні властивості, алгоритм Евкліда, розклад на прості співмножники, кільце лишків, теореми Ейлера та Ферма, афінні шифри вищих порядків

Третій розділ знайомить з основами теорії чисел. Особлива увага надається вивченню первісних коренів, квадратичних лишків, дискретному логарифму та обчисленню функції Ейлера. Тут також розглядаються методи тестування простоти та факторизації; розпізнавання квадратичності та добування квадратних коренів.

На завершення курсу розглядаються алгоритми з відкритим ключем та криптологічні протоколи.