



Теоретичні основи криптології

Галузі знань: 10 «Природничі науки», 11 «Математика та статистика»,
12 «Інформаційні технології», 15 «Автоматизація та приладобудування»,
16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації»,
19 «Архітектура та будівництво»

Рівень вищої освіти	перший (бакалаврський)		
Статус дисципліни	вибіркова		
Обсяг дисципліни	150 годин/ 5 кредитів ЄКТС		
Мова викладання	українська		
Що буде вивчатися (предмет вивчення)	Ознайомлення з базовими поняттями з елементарної теорії чисел і теорії алгебраїчних систем, основ теорії порівнянь і теорії квадратичних лишків, методів рішення порівнянь та систем порівнянь першого та другого ступенів, основ теорії груп, кілець, полів та теорії еліптичних кривих		
Чому це цікаво/треба вивчати (мета)	Засвоєння різноманітних теоретичних методів і засобів забезпечення криптологічних систем		
Як можна користуватися набутими знаннями і уміннями (компетентності)	В результаті засвоєння курсу студенти повинні знати та застосовувати базові положення (концепції) теорії алгебраїчних систем та елементарної теорії чисел; здійснювати вирішення задач з основних розділів елементарної теорії чисел і теорії алгебраїчних систем, побудови та перевірки чисел на простоту, знаходження найбільшого спільного дільника, знаходження прямого та оборотного чисел, алгоритми факторизації та дискретного логарифмування, основи теорії решіток та теорії порівнянь, визначення їх властивостей, арифметичні застосування теорії порівнянь першого та другого ступеня, їх рішення за допомогою методом прямої заміни та на основі китайської теореми про лишки, основи теорії груп, кілець, полів, їх приклади, основні теореми, особливості їх використання в криптологічних системах, примітивний (породжуючий) елемент поля, кільце вичетів за простим модулем та фактор-кільце многочленів як поле, поняття про еліптичні криві, засоби їх представлення над кінцевими полями з використанням різноманітних координат та їх використання в сучасних криптологічних системах		
Пререквізити	Вища математика		
Кореквізити	Прикладна криптологія		
Організація навчання	Види занять: лекції, практичні заняття. Форми здобуття освіти: денна. Форми контролю: модульний контроль, іспит		
Кафедра	Кафедра комп'ютерних систем, мереж і кібербезпеки № 503		
Факультет	Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій		
Викладач		ПІБ	Пєвнєв Володимир Яковлевич
		Посада	професор
		Вчене звання	доцент
		Науковий ступінь	д.т.н.
		e-mail	v.pevnev@csn.khai.edu
Посилання на електронні матеріали курсу			
Посилання на робочу програму (силабус)			