Освітній компонент	**Вибірковий освітній компонент 7** **«Алгебраїчні основи криптографії»**
Рівень ВО	Перший (бакалаврський) рівень
Назва спеціальності / освітньо-професійної програми	111 Математика / Математика
Форма навчання	Денна
Курс, семестр, протяжність	3 курс, 6 семестр, 5 кредитів ЄКТС
Семестровий контроль	Залік
Обсяг годин (усього: з них лекції / практичні)	150 год., з них: лекцій – 10 год., практичних – 20 год.
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Кафедра математичного аналізу та статистики
Автор ОК	Кандидат фізико-математичних наук, доцент кафедри математичного аналізу та статистики Волошина Тетяна Володимирівна
Короткий опис	
Вимоги до початку вивчення	Необхідний мінімум для початку вивчення дисципліни: основи теорії множин та елементи математичної логіки, що вивчаються в «Дискретній математиці» та в «Математичній логіці»; основи теорії груп та елементи теорії чисел, що вивчаються в «Алгебрі і теорії чисел»; елементарна математика в обсязі програми загально освітньої школи.
Що буде вивчатися	У курсі «Алгебраїчні основи криптографії» будуть вивчатися вибрані питання теорії груп та скінчених полів, теорії чисел, а також їх прикладні застосування у сучасній криптографії.
Чому це цікаво / треба вивчати	З обчислювальної точки зору задача знаходження дискретного логарифма вважається важкою в тому сенсі, що вимагає дуже великих об’ємів обчислень. На цій обчислювальній складності задачі дискретного логарифмування ґрунтується її застосування у криптографічних протоколах. Розглядаються протокол вироблення спільного секретного ключа, протокол цифрового підпису, протокол підкидання монети по телефону та інші. Цей матеріал знадобиться здобувачам для застосування у теорії захисту інформації та у криптографії.
Чому можна навчитися (результати навчання)	Вивчення вибіркового курсу «Алгебраїчні основи криптографії» сприяє тому, що здобувачі будуть розвивати у собі: • здатність застосовувати знання у практичних ситуаціях; • здатність генерувати ідеї, проявляти креативність; • здатність перевіряти гіпотези, умови виконання математичних тверджень, коректно переносити умови та твердження на нові класи об’єктів; • здатність вести конструктивну дискусію; • здатність формулювати та обґрунтовувати висновки у словесній та формальній формі, приймати обґрунтовані рішення; • здатність до автономної роботи; • здатність працювати у малих групах над розв’язанням

	професійних задач; • цілеспрямованість та наполегливість у досягненні мети.
Як можна користуватися набутими знаннями й уміннями (компетентності)	Результати навчання, здобуті при вивченні вибіркового курсу «Алгебраїчні основи криптографії», можна використати при вивченні теорії захисту інформації та криптографії. Набуті знання і вміння можна застосувати на практиці для вироблення протоколів, що базуються на обчислювальній складності певних теоретико-групових задач. Крім того спеціальні (фахові) компетентності, сформовані при вивченні вибіркового курсу ««Алгебраїчні основи криптографії», застосовуються для аналізу математичних структур, оцінки обґрунтованості й ефективності використовуваних математичних підходів.