Анотація курсу
”Математичні основи криптології”

Розглядаються класичні та сучасні підходи до побудови та аналізу криптографічних протоколів та криптосистем. Значна увага звертається на важливість теоретичного аналізу коректності та надійності криптографічних алгоритмів. Вводяться поняття криптографії та криптоаналізу, надійності та ефективності криптосистем. Описані класичні криптографічні методи (шифри перестановки та заміни, поліграмні та поліалфавітні шифри, шифр Віженера, шифр одноразового блокноту, афінні шифри). Наведено формальне визначення криптосистеми, властивості шифрувальних відображень, шифри, що утворюють групу. Розглянуто деякі математичні аспекти (класичний та розширений алгоритми Евкліда, групи та кільця по модулю, арифметика лишків, конгруенції), які використовуються в процесі побудови та аналізу криптографічних алгоритмів. Подано ідею криптосистем з відкритим ключем (опис, коректність та надійність алгоритму RSA). Розглянуто проблему сертифікації та обміну ключів (алгоритм обміну ключами Діффі-Гелмана) та ідею цифрового підпису (коректність та надійність системи цифрового підпису Ель-Гамала).

Доцент каф. програмування Ю.М.Сибіль

09.2011 р.