

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики
Кафедра обчислювальної математики

ПРОГРАМА КУРСУ

«Основи криптології»

Напрямок: прикладна математика

Факультет: прикладна математика та інформатика

Форма навчання: денна

Витяг з навчального плану

Курс	Семестр	Кількість кредитів	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						
4	8	3	108	42	28	14	–	66	1	–	–	–	+

1. Анотація

У спеціальному курсі розглядаємо: історію криптографії; фатальні наслідки нехтування надійним захистом інформації; симетричне шифрування – проста заміна та перестановки; основні досягнення двадцятого століття; революція в криптографії – асиметричні системи; роль математичних методів у побудові та реалізації надійних систем шифрування; протоколи; цифровий підпис; важкооборотні функції та їх роль у криптографії; поняття про еліптичні криві.

2. Зміст програми

2.1. Симетричні методи шифрування.

Тема 1. Основні поняття криптології. Постановка задачі шифрування. Термінологічні застереження. Історичний екскурс. Математичні основи. Нові перспективні напрями.

Тема 2. Класичні методи шифрування та криптоаналізу. Шифри заміни та шифри перестановки, їх криптоаналіз. Окремо про багатоалфавітні шифри. Кількаразове шифрування.

Тема 3. Цифрові методи шифрування. Шифр одноразового блокноту, складність його практичної реалізації. Алгоритми шифрування даних DES і ГОСТ. Режими використання блокових шифрів.

2.2. Методи шифрування з відкритим ключем.

Тема 4. Математична постановка задачі шифрування. Основні відомості теорії груп, кілець, полів. Приклади алгебричних структур, які найчастіше використовують при аналізі криптографічних схем. Афінні шифри як приклад застосування вищезазначених структур.

Тема 5. Алгоритм шифрування даних RSA . Базові поняття теорії чисел. Основна ідея симетричних методів шифрування. Коректність та проблеми, що виникають під час практичної реалізації.

Тема 6. Ймовірнісне шифрування. Про принципово інший рівень надійності таких криптосистем. Відповідний математичний апарат. Система Ель Гамала та подібні.

2.3. Проблеми, що розв'язують методами криптології.

Тема 7. Важкооборотні функції. Означення важкооборотної функції та її ядра. Сфери застосування важкооборотних функцій.

Тема 8. Цифровий підпис. Загальна схема цифрового підпису. Цифровий підпис на основі алгоритмів RSA і Ель Гамала. Функції вкорочення та коди достовірності. Стандарт цифрового підпису DSS.

Тема 9. Задача генерації псевдовипадкових послідовностей. Означення генератора псевдовипадкових послідовностей. Псевдовипадкові генератори із важкооборотних перестановок. BBS генератор.

Основна література

1. **Вербіцький О.В.** Вступ до криптології. Вид-во науково-технічної літератури. Львів. 1998. – 248 с.
2. **Нечаев В.И.** Элементы криптографии. М.: Высшая школа. 1999. – 109 с.
3. Введение в криптографию. Под общей редакцией **В.В. Яценко**. М.: МЦНМО – ЧеРо. 1999. – 271 с.
4. **Mirosław Kutylowski, Willy-B. Strothmann.** Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych. Oficyna Wydawnicza Read Me. Warszawa. 1999. – 267 st.
5. **Андрей Чмора.** Современная прикладная криптография. М.: Гелиос АРВ. 2001. – 244 с.
6. **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.** Основы криптографии. М.: Гелиос АРВ. 2002. –480 с.

Додаткова література

1. **Иванов М.А.** Криптографические методы защиты информации в компьютерных системах и сетях. М.: Кудиц-образ. 2001.- 368 с.
2. **Коутинхо С.** Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет. 2001. – 328 с.
3. **Ємець В., Мельник А., Попович Р.** Сучасна криптографія. Основні поняття. Львів: БАК. 2003.– 144 с.

Програму склав доцент Остудін Б.А.