МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Львівський національний університет імені Івана Франка

Кафедра дискретного аналізу та інтелектуальних систем

ПРОГРАМА КУРСУ

«ОСНОВИ КРИПТОГРАФІЇ»

(шифр і назва навчальної дисципліни)

Напрями підготовки: _____інформатика__

(шифр і назва напряму підготовки)

Факультет прикладної математики та інформатики

Форма навчання: денна

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	Лаб.	Практ.						
Денна	3	6	136	68	34	34		68	2	4		1	

1. АНОТАЦІЯ

Курс криптографії є важливим розділом у сучасному інформаційному просторі. З часом все більше виникає задач захисту електронної інформації. Більшість фінансових операцій проводиться через електронні засоби зв'язку. Це робить неможливим використання традиційних засобів засвідчення платіжних документів на зразок великої гербової печатки та підпису головного бухгалтеру. Завдання вирішується за допомогою протоколу цифрового підпису, який базується на криптографічних алгоритмах. З розвитком всесвітньої мережі Інтернет виникають задачі захисту конфіденційної інформації, які дозволяє вирішити курс криптографії.

Цей курс пропонується всім, хто зацікавлений в ознайомленні з предметом. Він має вступний характер, значна увага приділяється конкретним криптосистемам – від найдавніших до сучасних.

Метою курсу є ознайомлення з основними поняттями елементарної криптографії, математичними підходами до криптографії, алгоритмами та їх складністю, складністю арифметичних задач, криптосистемами з відкритим ключем, криптографічними інструментами та протоколами.

Головним завданням курсу є вивчення криптографічних систем від часів античності до сучасних, розуміти основні принципи роботи сучасних криптосистем з відкритим ключем.

2. ЗМІСТ ПРОГРАМИ

1. ЕЛЕМЕНТАРНА КРИПТОГРАФІЯ. Початкові поняття та приклади. Шифри простої заміни. Частотний аналіз.

2. ЕЛЕМЕНТАРНА КРИПТОГРАФІЯ. Поліграмні шифри. Поліалфавітні шифри. Шифрування блоками, шифри перестановки

3. ЕЛЕМЕНТАРНА КРИПТОГРАФІЯ. Шифри одноразового блокноту та DES.

4. МАТЕМАТИЧНИЙ ПІДХІД ДО КРИПТОГРАФІЇ. Головні положення, дешифрування ітераціями, арифметика, алгоритм Евкліда. Розклад на прості співмножники. Конгруенції. Кільце лишків. Кільце матриць.

5. МАТЕМАТИЧНИЙ ПІДХІД ДО КРИПТОГРАФІЇ. Афінні шифри. Шифр простої заміни. Афінні шифри вищих порядків.

6. КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ. Концепція; RSA. Система Рабіна, обчислення функції Ейлера. Імовірнісне криптування. Система Ельгамала.

7. ПРОТОКОЛИ. Обмін ключем. Цифровий підпис. Підпис у системі RSA. Загальна схема. Система цифрового підпису ЕльГамала. Коди достовірності. Система Шнорра. DSA.

8. ПРОТОКОЛИ. Підкидання монети по телефону. Гра в карти заочно. Розподіл таємниць.

9. ПРОТОКОЛИ. Доведення без розголошення. Ідентифікація.

ОСНОВНА ЛІТЕРАТУРА

1. *Берегуляк І.Я.* Класичні методи криптування. Львівський університет, 1997.
2. *Вербіцький О.В.* Вступ до криптології. Львів, 1998.
3. *Жельников В.* Криптография от папируса до компьютера. ABF, Москва, 1996.
4. *Месси Дж. Л.* Введение в современную криптологию. Труды института инженеров электроники и радиофизики, 76(5):24-42, 1988.
5. *Фаль А.М.* DES – этап в развитии криптологии. Безопасность информации, 2:18-21,1995.
6. *Шнайер Б.* Прикладная криптография. Триумф, 2002.

ДОДАТКОВА ЛІТЕРАТУРА

1. *Дориченко С.А., Ященко В.В.* 25 этюдов о шифрах. Математические основы криптологии. М., ТЕИС, 1994.
2. *Biham E., Shamir A.* Differential Cryptoanalysis of the Data Encryption Standard. Springer Verlag, Berlin, 1993.
3. *Blum M., Micali S.* How to generate cryptographically strong sequences of pseudo-random bits. SIAM Journal on Computing, 13(4):850-863, 1984.
4. *Goldreich O.* Foundations of Cryptography (Fragments of a Book). Electronic Colloquium on Computational Complexity, 1995.