ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
та навчальної роботи
_____О.І. Гура
(підпис)
«____» _____ 20____ р.

СУЧАСНА КРИПТОГРАФІЯ

ПРОГРАМА
навчальної дисципліни
підготовки магістрів
спеціальності 8.05010302 - "Інженерія програмного забезпечення"

(шифр за ОПП 4.3)

Кафедра математичного моделювання

2014 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО: кафедра математичного моделювання, математичний факультет

РОЗРОБНИКИ ПРОГРАМИ: Чопоров С.В., доцент кафедри математичного моделювання, к.т.н.

ОБГОВОРЕНО ТА РЕКОМЕНДОВАНО ДО ЗАТВЕРДЖЕННЯ КАФЕДРОЮ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ
«28» серпня 2014 року, протокол № 1

Завідувач кафедри д.т.н., професор _____ С.І. Гоменюк
(підпис)

Вступ

Програма вивчення навчальної дисципліни «Сучасна криптографія» складена відповідно до освітньо-професійної програми підготовки магістрів спеціальності 8.05010302 - "Інженерія програмного забезпечення".

Предметом вивчення навчальної дисципліни є методи і засоби сучасної криптографії.

Міждисциплінарні зв'язки: навчальна дисципліна «Сучасна криптографія» пов'язана з теоретичними знаннями та практичними уміннями з дисциплін «Алгоритми та структури даних», «Архітектура комп'ютера», «Комп'ютерна дискретна математика», «Методи та засоби комп'ютерних інформаційних технологій», «Основи програмування та інформаційна культура студентів», «Об'єктно-орієнтоване програмування», «Організація і функціонування ЕОМ», «Основи програмної інженерії».

Програма навчальної дисципліни складається з таких змістових модулів:

1. Класифікація алгоритмів шифрування
2. Основні криптографічні алгоритми

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «Сучасна криптографія» є оволодіння основними методами і засобами використання криптографічних методів для захисту інформації.

1.2. Основними завданнями вивчення дисципліни «Сучасна криптографія» є формування практичних навичок, необхідних для використання методів і засобів сучасної криптографії у професійній діяльності.

1.3. Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- криптографічні алгоритми;
- категорії алгоритмів шифрування;
- структуру алгоритмів симетричного шифрування;
- режими роботи алгоритмів шифрування;
- можливі атаки на алгоритми шифрування;
- можливі атаки на шифратори.

вміти:

- використовувати бібліотеки криптографічних алгоритмів;
- програмувати методи криптографії;
- визначити структуру алгоритмів симетричного шифрування;
- використовувати режими алгоритмів шифрування;
- розрізняти атаки на алгоритми шифрування та шифратори.

На вивчення навчальної дисципліни відводиться 180 годин 5,0 кредитів ЄКТС.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Класифікація алгоритмів шифрування

Тема 1. Загальна структура криптографічних алгоритмів

Криптографічні алгоритми. Категорії алгоритмів шифрування. Алгоритми на основі мережі Фейстеля. Алгоритми на основі підстановок і перестановок. Алгоритми зі структурою «квадрат». Алгоритми з нестандартною структурою.

Тема 2. Режими роботи криптографічних алгоритмів

Електронна кодова книга. Зчеплення блоків шифру. Зворотній зв'язок за шифром тексту. Зворотний зв'язок за виходом. Інші режими роботи.

Тема 3. Атаки на алгоритми шифрування

Мета атак. Класифікація атак. Кількісна характеристика криптостійкості алгоритмів шифрування. Криптоаналіз модифікованих алгоритмів. Метод «грубої сили». Атаки класу «зустріч посередині». Диференціальний криптоаналіз. Лінійний криптоаналіз. Метод бумеранга. Зсувова атака. Метод інтерполяції. Неможливі диференціали.

Тема 4. Атаки на шифратори

Атака за часом виконання. Атаки за вживаною потужністю. Пасивні атаки. Види впливу на шифратори. Диференціальний аналіз на основі збоїв. Протидія активним атакам. Розширення ключа. «Класична» атака на зв'язних ключах. Алгоритми, що атакуються. Можливі проблеми процедури розширення ключа.

Змістовий модуль 2. Основні криптографічні алгоритми

Тема 1. Класичні симетричні методи криптографії

Основні поняття та визначення. Шифри перестановки: таблиці шифрування, застосування магічних квадратів. Шифри простої заміни: система шифрування Цезаря, афінна система підставок Цезаря, система Цезаря з ключовим словом, таблиці шифрування Трісємуса, біграмний шифр Плейфейра. Криптосистема Хілла. Шифри складної заміни: система шифрування Віжинера, шифр «подвійний квадрат», одноразова система шифрування, шифрування методом Вернама. Шифрування методом гамування.

Тема 2. Сучасні симетричні методи криптографії

Опис стандарту шифрування DES. Основні режими роботи алгоритму DES. Область застосування алгоритму DES. Комбінування блокових алгоритмів. Алгоритм шифрування IDEA. Вітчизняний стандарт шифрування. Блокові та потокові шифри. Методи криптографії з депонуванням ключа: процедура генерації ключів, програмування мікросхеми, обслуговування ключів, процедура дешифрування.

Тема 3. Асиметричні методи криптографії

Концепція криптосистеми з відкритим ключем. Однонаправлені функції. Метод шифрування даних RSA: процедури шифрування і дешифрування в криптосистемі RSA, безпека і швидкодія системи на основі RSA. Схема шифрування Поліга-Хеллмана. Схема шифрування Ель Гамаля. Комбінований метод шифрування.

Тема 4. Інші алгоритми шифрування

Алгоритм FEAL. Алгоритм FROG. Алгоритм Grand Cru. Родина алгоритмів Hierocrypt. Алгоритм HPC. Алгоритм ICE. Алгоритм ICEBERG. Алгоритм KASUMI. Алгоритм Khazad. Родина алгоритмів Khufu і Khafre. Варіанти алгоритму Lucifer. Алгоритм

MacGuffin. Алгоритм MAGENTA. Алгоритм MARS. Алгоритм Mercy. Алгоритми MISTY1 і MISTY2. Алгоритм NIMBUS. Огляд інших алгоритмів.

3. Рекомендована література

Основна:

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгиню – М.: Радио и связь, 2001. – 376 с.

2. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия, 2006. – 544 с.

3. Завгородний В.И. Комплексная защита информации в компьютерных системах / В.И. Завгородний. – М.: Логос, 2001. – 264 с.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – М.: Форум, 2008. – 416 с.

5. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.

Додаткова:

1. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

2. Вельшенбах М. Криптография на Си и С++ в действии. Учебное пособие / М. Вельшенбах. – М.: Триумф, 2004. – 464 с.

3. Щеглов А.Ю. Защита информации от несанкционированного доступа / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.

4. Мельников В.П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. – М.: Академия, 2008. – 336 с.

Інформаційні ресурси:

1. Защита информации от несанкционированного доступа [Електронний ресурс] – Режим доступу: http://ru.wikibooks.org/wiki/

2. Введение в криптографию [Електронний ресурс] – Режим доступу: http://algolist.manual.ru/defence/intro.php

3. Математическая криптография [Електронний ресурс] – Режим доступу: http://cryptography.ru/

4. Основы криптографии [Електронний ресурс] – Режим доступу: http://www.intuit.ru/studies/courses/691/547/info

5. Криптографические методы защиты в языках программирования [Електронний ресурс] – Режим доступу: http://compress.ru/article.aspx?id=10153

4. Форма підсумкового контролю успішності навчання

Залік

5. Засоби діагностики успішності навчання

Тестування, усне та письмове опитування, співбесіда, перевірка лабораторних робіт.