Федеральное агентство по образованию
ГОУ ВПО «Алтайский государственный университет»

УТВЕРЖДАЮ
декан математического факультета
Кузиков С.С.
“18” февраля 2008г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Криптография

Направление: 010200.68 Математика. Прикладная математика
Магистерская программа: Алгебра
Квалификация: Магистр математики
Математический факультет
Кафедра алгебры и математической логики

курс 6

семестр 11, 12

лекции	34	(час.)			
Практические (семинарские)					
Занятия	0	(час.)	Зачет в 12 семестре		
Лабораторные					
Занятия	34	(час.)			
Всего часов 68		Самостоятельная работа		102	(час.)
Итого часов трудозатрат на дисциплину (для студента) по ГОС				170	(час.)

2007 г.

Рабочая программа составлена на основании примерной программы, принятой на заседании Ученого совета математического факультета «__»_____2008.

Рабочая программа обсуждена на заседании кафедры алгебры и математической логики

«11» февраля 2008г.

Заведующий кафедрой _____ А.И. Будкин

Одобрено методической комиссией математического факультета
«18» февраля 2008г.

Председатель методической комиссии математического факультета _____ Н.В. Баянова

Введение (пояснительная записка).

Курс «Криптография» предназначен для магистрантов математического факультета, обучающихся по магистерской программе 511206 - Алгебра.

Общий объем лекций составляет 34 час (из них 17 час в 11 семестре), лабораторных занятий – 34 час (из них 17 час в 11 семестре), самостоятельная работа магистрантов занимает 102 час (из них 51 час в 11 семестре). Итоговый контроль работы магистрантов – зачет в 12 семестре. Текущий контроль состоит из выполненных магистрантами лабораторных работ и тестирований знаний магистрантов. Результирующая оценка формируется по результатам итогового тестирования и экзамена.

Раздел 1. Цели и задачи дисциплины, ее место в учебном процессе.

1.1. Цель преподавания дисциплины. освоение студентами основных принципов современной криптографии и умение практического применения знаний для защиты информации.

1.2. Задачи изучения дисциплины.

- дать представления о классических системах шифрование
- дать представление о современных симметричных блочных шифров и о методах их взлома
- дать представление о современных потоковых шифрах
- познакомить с современной ассиметричной криптографией

1.3. Перечень дисциплин с указанием разделов (тем), усвоение которых студентами необходимо для изучения данной дисциплины.

- Информатика (умение программировать).
- Теория чисел.

Раздел 2. Содержание дисциплины.

2.1. Наименование тем лекционных, практических и семинарских, лабораторных занятий, их содержание и объем в часах.

1 семестр

1. Основные понятия и определения.
2. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов.
3. Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера, криптосистема Хилла, система омофонов.
4. Шифры сложной замены: шифр Гронсфельда, система шифрования Вижинера, шифр «двойной квадрат» Уитсона, одноразовая система шифрования, шифрование методом Вернама, роторные машины.
5. Методы взлома классических шифров.
6. Современные симметричные криптосистемы. Принцип итерирования. Конструкция Фейтстеля.
7. Американский стандарт шифрования данных DES. Область применения алгоритма DES.
8. Основные режимы работы алгоритма DES: режим «Электронная кодовая книга», режим «Сцепление блоков шифра», режим «Обратная связь по шифру», режим «Обратная связь по выходу».
9. Алгоритм шифрования данных IDEA.
10. Отечественный стандарт шифрования данных: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.
11. Атаки на блочные шифры. Дифференциальный криптоанализ. Линейный криптоанализ.
12. Современный стандарт шифрования США.
13. Блочные и поточные шифры.

14. Шифрование методом гаммирования:
    методы генерации псевдослучайных последовательностей чисел.
15. Современные потоковые шифры.
16. Регистры сдвига с линейной обратной связью.
17. Генераторы истинно случайных последовательностей.

2 семестр

1. Концепция криптосистемы с открытым ключом. Однонаправленные функции.
2. Алгоритмы на основы задачи об укладке рюкзака.
3. Криптосистема шифрования данных RSA: процедуры шифрования и расшифрования в криптосистеме RSA, безопасность и быстродействие криптосистемы RSA.
4. Схема шифрования Полига-Хеллмана. Схема шифрования Эль Гамаля.
5. Комбинированный метод шифрования. Генерация простых чисел.
6. Построение больших простых чисел. Тесты проверки на простоту.
7. Криптосистемы с открытым ключом на основе конечных автоматов.
8. Введение в протоколы. Протоколы с посредником. Атаки на протоколы.
9. Обмен ключами. Атака «челолек посередине». Аутентификация.
10. Разделение секрета. Групповые подписи. Подписи по доверенности.
11. Подбрасывание монеты и игра в карты по телефону.
12. Эзотерические протоколы.
13. Идентификация и проверка подлинности. Основные понятия и концепции. Взаимная проверка подлинности пользователей.
14. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Схема идентификации Гиллоу-Куискоутера.
15. Проблема аутентификации данных и электронная цифровая подпись.
16. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции.
17. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

2.2.Курсовой проект (работа), его характеристика.

- Не планируется.

Раздел 3. Учебно-методические материалы по дисциплине.

3.1. Основная и дополнительная литература, другие информационные источники.

1. Алферов .А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. — Основы криптографии. М.: Гелиос АРВ, 2001
2. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В.. Криптография в банковском деле. — М.: Изд-во МИФИ, 1997.
3. Бернет С., Пейн С. Криптография. Официальное руководство RSA Security.
4. Березин Б.В., Дорошкевич П.В. Цифровая подпись на основе традиционной криптографии. Защита информации. — 1992. — Вып. 2. — С. 148—167.
5. Болл У., Коксетер Г. Математическое эссе и развлечения (криптография и криптографический анализ). — М.: Мир, 1986.
6. Брассар Ж. Современная криптография. — М.: Полимед, 1999
7. Варфоломеев А.А., Перепелицын М.Б. Методы криптографии и их применение в банковских технологиях. — М.: Изд-во МИФИ, 1995
8. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. — М.: Изд-во МИФИ, 2000.
9. Варфоломеев А.А., Домина О.С., Перепелицын М.Б. Управление ключами в системах криптографической защиты банковской информации — М.: Изд-во МИФИ, 1996.
10. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.
11. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001 – 328 с.
12. Конхейм А.Г. Основы криптографии. — М.: Радио и связь, 1987.
13. Кузьминов Т.В. Криптографические методы защиты информации. — М.: Наука, 1998.
14. Мэсси Дж.Л. Современная криптография: введение // ТИИЭР. — 1988. — Т.76. — №5.
15. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. — М.: Высшая школа, 1999.
16. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК, 2000.
17. Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996.
18. Соболева Т.А. Тайнопись в истории России. История криптографической службы России XVIII — начала XX в. — М.: Международные отношения, 1994.
19. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер.— М.: Гелиос АРВ, 2002 – 256 с.
20. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке C++. — М.: Изд-во ТРИУМФ, 2002 – 816 с.
21. Ященко В.В. Введение в криптографию. — М.: МЦНМО — ЧеРо, 1998.

3.2 Перечень наглядных и других пособий, методических указаний по проведению конкретных видов учебных занятий, а также методических материалов к используемым в учебном процессе техническим и компьютерным средствам.

1. Плакаты
2. Презентации
3. Учебные программы