СПИСОК КЛЮЧЕВЫХ ТЕМ, ЗНАНИЕ КОТОРЫХ НЕОБХОДИМО ДЛЯ ПОСТУПЛЕНИЯ НА МАГИСТЕРСКУЮ ПРОГРАММУ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ».

1. Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства.
2. Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента. Криптографическая теорема (Обоснование криптосистемы RSA).
3. Сравнения второй степени. Символ Лежандра, Символ Якоби и их свойства.
4. Алгоритмы решения сравнений второй степени по простому модулю.
5. Поле. Простое поле. Строение конечного поля. Теорема о примитивном элементе. Минимальный многочлен и его свойства. Теорема об эквивалентности конечных полей одной мощности.
6. Примитивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = x^{p^n} - x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю.
7. Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности(ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства.
8. Теорема об определении структуры ЛРП по её характеристическому многочлену.
9. Прямое произведение групп. Теорема о представлении групп в виде прямого произведения своих подгрупп. Теорема о примарной абелевой группе.
10. Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп.
11. Нормализатор, централизатор , класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши. Теоремы Силова.
12. Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Полурегулярные , регулярные группы и их свойства.
13. Импримитивность, Критерий импримитивности транзитивной группы. Примитивные группы подстановок. Кратная транзитивность, критерий кратной транзитивности транзитивной группы.
14. Задача целой факторизации. Простейшие алгоритмы факторизации: методы Ферма, ро-метод Полларда, (р-1)-метод Полларада.
15. Задача дискретного логарифмирования в циклической группе. Проблема Диффи-Хеллмана. Простейшие алгоритмы дискретного логарифмирования: согласования индексов, большой шаг – малый шаг, ро-метод Полларда, метод Похлига-Хеллмана.
16. Определение хэш-функции, криптографические требования к хэш-функциям. Основные приложения криптографических хэш-функций, вывод криптографических требований к хэш-функциям из требований стойкости этих приложений.
17. Задача о днях рождения. Однородная и неоднородная схемы размещения шаров по ящикам. Оценки вероятности попадания двух и более шаров в один ящик для однородной схемы.
18. Угадывание прообраза. Поиск коллизий, моделируемый однородной и неоднородной (атака Ювала) схемами размещения шаров по ящикам. Оценка вероятности успеха этих атак.

19. Определение кода аутентификации (теоретико-информационный подход). Требования к кодам аутентификации. Атаки имитации и подмены. Вероятности успешной имитации и подмены, их свойства. Оптимальные коды аутентификации.
20. Дискреционная политика разграничения доступа. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах. Модель TAKE-GRANT.
21. Основы политики мандатного доступа. Решетка безопасности. Политика MLS.

СПИСОК ЛИТЕРАТУРЫ

1. Смарт Н. Криптография.-М.:Техносфера,2005.-525с.
2. Виноградов И.М. Теория чисел. М.:Наука,1990.-167с.
3. B. Preneel, Analysis and Design of Cryptographic Hash Functions, PhD Thesis, 1993.
4. А. В. Черемушкин, Криптографические протоколы. Основные свойства и уязвимости, Москва: Издательский центр "Академия", 2009.
5. Черепнёв М.А. Криптографические протоколы.-М.: Изд-во центра прикладных исследований при механико-математическом факультете.-2006.-70с.
6. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
7. А. П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин, Основы криптографии, Москва: Гелиос АРВ, 2005.
8. Ван Тилборг Х.К.А. Основы криптологии. – Москва: Мир, 2006.
9. С.Б. Гашков, Э.А. Применко, М.А. Черепнев. Криптографические методы защиты информации. М: Академия, 2010 – 304 с.
10. Э.А. Применко. Алгебраические основы криптографии. М: Либроком, 2013 – 288 с.
11. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002. - 816 с.
12. Грушо А.А. Применко Э.А. Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Издательский центр "Академия", 2009.
13. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: Издательский центр «Академия», 2005. – 144 с.
14. Криптография в банковском деле./ Анохин М.И.,Варновский Н.П.,Сидельников В.М.,Ященко В.В.;МИФИ.М.,1997.-274с.
15. Саломаа А. Криптография с открытым ключом.-М.:Мир,1996.-318с.
16. Брассар Ж. Современная криптология.-М.: ИПФ "Полимед",1999.-175с.
17. Лидл Р., Нидеррейтер Х. Конечные поля.т.1,2.-М.:Мир,1988.-818с.
18. Сидельников В.М., Черепнёв М.А., Ященко В.В. Системы открытого распределения ключей на основе некоммутативных полугрупп.// ДАН СССР-1993.-т.332-№5-с.566-567.
19. Кнут Д. Искусство программирования на ЭВМ. т.2.-С.-П.:Вильямс-2000.-682с.
20. N.Koblitz Algebraic Aspects of Cryptography.-Springer-Verlag,1998.-109p.
21. К.Прахар. Распределение простых чисел.-М.,Мир,1967.-511с.
22. Maurer U.M. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms.// Proc. Crypto'94.-1994.-p.271-281.
23. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии.-М.:МЦНМО,2006.-325с.