ЛИТЕРАТУРА

Базовый учебник

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. - М.: Гелиос АРВ, 2001.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-Образ, 2001.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. - СПб.: БХВ-Петербург, 2009.
4. Токарева Н.Н. Симметричная криптография. Краткий курс. - Новосиб. гос. ун-т. Новосибирск, 2012.

Дополнительная литература

5. Агибалов Г.П. Избранные теоремы начального курса криптографии. - Томск: Томский госуниверситет, 2005.
6. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. - М.: МИФИ, 1997.
7. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н. Поточные шифры. - М.: Кудиц-Образ, 2003.
8. Бабаш А.В., Шанкин Г.П. Криптография. - М.: СОЛОН-ПРЕСС, 2007.
9. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа.- М.: Гелиос АРВ, 2006.
10. Белкин П.Ю., Михальский О.О., Першаков А.С. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 1999.
11. Брассар Ж. Современная криптология. - М.: ПОЛИМЕД, 1999.
12. Ван дер Варден Б.Л. Алгебра. - Изд. 2. - М.: Наука, 1979.
13. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: Учеб. пособие. - Владивосток: Изд–во ДВГТУ, 2007.
14. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. -М.: МЦНМО, 2006.
15. Вельщенбах М. Криптография на C и C++ в действии. - М.: Триумф, 2008.
16. Виноградов И.М. Основы теории чисел. - М.: Наука, Физматлит, 1983.
17. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети - анализ технологий и синтез решений. - М.: ДМК Пресс, 2004.
18. Гашков С.Б., Чубариков В.Н. Арифметика. Алгоритмы. Сложность вычислений. - М.: Дрофа, 2004.

19. Герасименко В.А., Малюк А.А. Основы защиты информации. - М.: МОПО РФ, МИФИ, 1997.
20. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. - СПб.: Лань, 2011.
21. ГОСТ 28147-89. - Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Блочный шифроалгоритм. - М.: Госстандарт СССР, 1989.
22. ГОСТ Р 34. 10-94. - Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. - М.: Госстандарт РФ, 1994.
23. ГОСТ Р 34. 11-94. Информационная технология. Криптографическая защита информации. Функция хеширования, 1994.
24. ГОСТ Р 34. 10-2001. - Информационная технология. Криптографическая защита информации. процессы формирования и проверки электронной цифровой подписи. - М.: Госстандарт РФ, 2001.
25. ГОСТ Р 34. 11-2012. - Национальный стандарт российской федерации. информационная технология. криптографическая защита информации. Функция хэширования. - М.: Госстандарт РФ, 2012. Введен 01. 01. 2013.
26. Грин Д., Кнут Д. Математические методы анализа алгоритмов. - М.: Мир, 1987.
27. Девянин П.Н., Михальский О.О. и др. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000.
28. Земор Ж. Курс криптографии. - М., Ижевск: НИЦ ″Регулярная и хаотическая динамика″; Институт компьютерных исследований, 2006.
29. Зенин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. Серия СКБ. Книга 1. - М.: Кудиц-Образ, 2002.
30. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. Серия СКБ. Книга 2. - М.: Кудиц-Образ, 2003.
31. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. - Казань, 2012.
32. Кнут Д.Э. Искусство программирования. Т. II. 3-е изд.: Пер. с англ. - М.-СПб-Киев: Вильямс, 2000.
33. Коблиц Н. Курс теории чисел и криптографии. - М.: ТВП, 2001.
34. Куракин В.Л. Алгоритм Берлекэмпа-Месси над конечными кольцами, модулями и бимодулями // Дискрет. матем. 1998. Т. 10, № 4. С. 3-34.
35. Лидл Р., Нидеррайтер Г. Конечные поля. - Т. 1, 2. М.: Мир, 1988.

36. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. - М.: Московский центр непрерывного математического образования, 2004.
37. Маховенко Е.Б. Теоретико-числовые методы в криптографии. - М.: ″Гелиос АРВ″, 2006.
38. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография. От примитивов к синтезу алгоритмов. - СПб.: БХВ-Петербург, 2004.
39. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. - СПб.: БХВ-Петербург, 2002.
40. Музыкантский А.И.. Фурин В.В. Лекции по криптографии. - Москва: Изд-во МЦНМО, 2011.
41. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). - М.:Высш. шк., 1999.
42. Применко Э.А. Алгебраические основы криптографии. -(Основы защиты информации). - М.: URSS: [ЛИБРОКОМ, 2013].
43. Проскурин В.Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. - М.: Радио и связь, 2000.
44. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001.
45. Ростовцев А.Г., Маховенко Е.Б.. Теоретическая криптография, Профессионал, СПб, 2005.
46. Саломаа А. Криптография с открытым ключом. - М.: Мир, 1996.
47. Столингс В. Криптография и защита сетей. Принципы и практика. -М.: Вильямс, 2001.
48. Фомичев В.М. Методы дискретной математики в криптологии. - М.: Диалог-МИФИ, 2010.
49. Черемушкин А.В. Лекции по арифметическим функциям в криптографии. - М.: МЦНМО, 2002.
50. Шеннон К.Э. Теория связи в секретных системах/В кн.: Работы по теории информации и кибернетике. - М.: ИЛ, 1963.
51. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф. 2002.
52. Шнайер Б., Фергюссон Н. Практическая криптография. - М., Вильямс, 2005.
53. Ященко В. В. Введение в криптографию. - М.: МЦНМО, 1998, 1999, 2000.