Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004. -- 173с.

ISBN 5-89176-233-1

В монографии изложены основные подходы и методы современной криптографии для решения задач, возникающих при обработке, хранении и передаче информации. Основное внимание уделено новым направлениям криптографии, связанным с обеспечением конфиденциальности взаимодействий пользователей компьютеров и компьютерных сетей Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блоковые и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо не скрываемых криптосистем и криптографии на эллиптических кривых Изложение теоретического материала ведется достаточно строю, но с использованием довольно элементарного математического аппарата. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов.

Книга предназначается студентам и инженерам, работающим в области информационных технологий.

ОГЛАВЛЕНИЕ