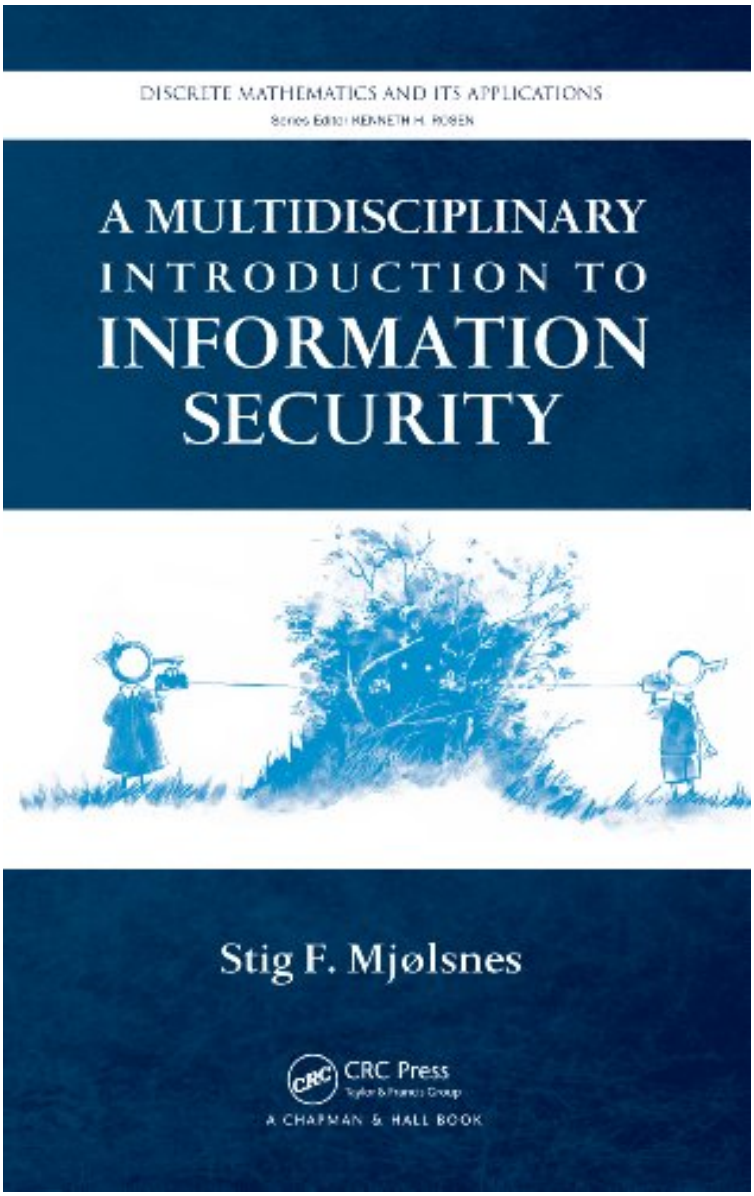
# A Multidisciplinary Introduction to Information Security (Discrete Mathematics and Its Applications)








#4535791 in eBooks 2011-11-09 2011-11-09File Name: B008NFBIGY | File size: 16.Mb

**From Chapman and Hall/CRC : A Multidisciplinary Introduction to Information Security (Discrete Mathematics and Its Applications)** before purchasing it in order to gage whether or not it would be worth my time,

and all praised A Multidisciplinary Introduction to Information Security (Discrete Mathematics and Its Applications):

With most services and products now being offered through digital communications, new challenges have emerged for information security specialists. A Multidisciplinary Introduction to Information Security presents a range of topics on the security, privacy, and safety of information and communication technology. It brings together methods in pure mathematics, computer and telecommunication sciences, and social sciences. The book begins with the cryptographic algorithms of the Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA). It explains the mathematical reasoning behind public key cryptography and the properties of a cryptographic hash function before presenting the principles and examples of quantum cryptography. The text also describes the use of cryptographic primitives in the communication process, explains how a public key infrastructure can mitigate the problem of crypto-key distribution, and discusses the security problems of wireless network access. After examining past and present protection mechanisms in the global mobile telecommunication system, the book proposes a software engineering practice that prevents attacks and misuse of software. It then presents an evaluation method for ensuring security requirements of products and systems, covers methods and tools of digital forensics and computational forensics, and describes risk assessment as part of the larger activity of risk management. The final chapter focuses on information security from an organizational and people point of view.As our ways of communicating and doing business continue to shift, information security professionals must find answers to evolving issues. Offering a starting point for more advanced work in the field, this volume addresses various security and privacy problems and solutions related to the latest information and communication technology.

About the AuthorStig F. Mjoslash;lsnes is a professor in the Department of Telematics at the Norwegian University of Science and Technology. His research focuses on the development and application of cryptographic protocols and security models.