DESCRIPTION

Complete coverage of the current major public key cryptosystems their underlying mathematics and the most common techniques used in attacking them Public Key Cryptography: Applications and Attacks introduces and explains the fundamentals of public key cryptography and explores its application in all major public key cryptosystems in current use, including ElGamal, RSA, Elliptic Curve, and digital signature schemes. It provides the underlying mathematics needed to build and study these schemes as needed, and examines attacks on said schemes via the mathematical problems on which they are based – such as the discrete logarithm problem and the difficulty of factoring integers.

The book contains approximately ten examples with detailed solutions, while each chapter includes forty to fifty problems with full solutions for odd-numbered problems provided in the Appendix. Public Key Cryptography:

• Explains fundamentals of public key cryptography
• Offers numerous examples and exercises
• Provides excellent study tools for those preparing to take the Certified Information Systems Security Professional (CISSP) exam
• Provides solutions to the end-of-chapter problems
Public Key Cryptography provides a solid background for anyone who is employed by or seeking employment with a government organization, cloud service provider, or any large enterprise that uses public key systems to secure data.

ABOUT THE AUTHOR

Professor Lynn Batten holds the Deakin Chair in Mathematics and is the Director of the Information Security Research Group at Deakin University. Her research interests include combinatorial geometry, computer network security and computational chemistry. As Associate Dean for Academic and Industrial Research at the University of Manitoba, her former institution, she established a number of agreements between the University and various industry and government sectors.

SERIES

IEEE Press Series on Information and Communication Networks Security

For additional product details, please visit https://www.wiley.com/en-us