

# **BEGINNING CRYPTOGRAPHY WITH JAVA**

Acknowledgments.

Introduction.

Chapter 1: The JCA and the JCE.

Chapter 2: Symmetric Key Cryptography.

Chapter 3: Message Digests, MACs, and HMACs.

Chapter 4: Asymmetric Key Cryptography.

Chapter 5: Object Description in Cryptography Using ASN.1.

Chapter 6: Distinguished Names and Certificates.

Chapter 7: Certificate Revocation and Path Validation.

Chapter 8: Key and Certificate Management Using Keystores.

Chapter 9: CMS and S/MIME.

Chapter 10: SSL and TLS.

Appendix A: Solutions to Exercises.

Appendix B: Algorithms Provided by the Bouncy Castle Provider.

Appendix C: Using the Bouncy Castle API for Elliptic Curve.

Appendix D: Bibliography and Further Reading.

Index.