

---

# Contents

November 1993 Release

*An Overview of the PKCS Standards.*

*A Layman's Guide to a Subset of ASN.1, BER, and DER.*

*PKCS #1: RSA Encryption Standard. Version 1.5.*

*PKCS #3: Diffie-Hellman Key-Agreement Standard. Version 1.4.*

*PKCS #5: Password-Based Encryption Standard. Version 1.5.*

*PKCS #6: Extended-Certificate Syntax Standard. Version 1.5.*

*PKCS #7: Cryptographic Message Syntax Standard. Version 1.5.*

*PKCS #8: Private-Key Information Syntax Standard. Version 1.2.*

*PKCS #9: Selected Attribute Types. Version 1.1.*

*PKCS #10: Certification Request Syntax Standard. Version 1.0.*

*Some Examples of the PKCS Standards.*