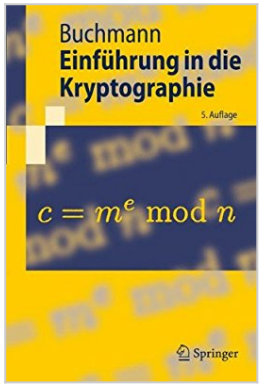

Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition)

Johannes Buchmann

Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition)
Johannes Buchmann

Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition)

Johannes Buchmann

Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition) Johannes Buchmann

304 Seiten

Pressestimmen

Aus den Rezensionen zur 2. Auflage:„Diese von einem Mathematiker geschriebene „Einführung in die Kryptographie" fällt sofort durch ihren präzisen und logisch einwandfreien Stil auf. Die verwendeten Begriffe (Verschlüsselungsverfahren, perfekte Sicherheit, Hashfunktion,...) werden mathematisch sauber und kurz definiert, und es wird sehr wohl unterschieden, was „bewiesen" ist [...] und was „allgemeiner Glaube der Experten" ist.Trotz dieser mathematischen Genauigkeit ist dieses Buch insbesondere für Anfänger und speziell auch für Nicht-Mathematiker sehr verständlich gehalten. Das nötige mathematische Werkzeug (Restklassenringe, Matrizen und lineare Abbildungen, Wahrscheinlichkeit, Erzeugung von Primzahlen, Faktorisierungsverfahren, Ausblick auf elliptische Kurven) wird vor der jeweiligen Anwendung vorgestellt. Dann wird der Themenkreis prägnant, sehr verständlich und mit Beispielen illustriert, besprochen, wobei der Geübte die dahinterliegende mathematische Idee schnell erkennen kann. Dabei werden im Wesentlichen alle Basistechniken der modernen Kryptographie erfasst. Soweit möglich bzw. üblich, wird das englische Fachvokabular der Kryptographie in die deutsche Sprache übersetzt. Ich hoffe, dass die Freude des Rezensenten beim Lesen dieses Buches auch von vielen anderen Lesern ebenfalls empfunden werden kann." (Int. Math. Nachrichten 2002, Vol 56, Issue 189).„[...] „Klein, aber fein" ist das Charakteristikum des Buches: Jeder Abschnitt ist mit (für Mathematiker) sehr anschaulichen Beispielen und kleinen Übungsaufgaben versehen. Entwickler finden hier eine reiche Quelle der Hintergründe, die sie für eine Implementation wissen müssen."

(Amazon.de-Redaktion)Kurzbeschreibung

Der Band behandelt die aktuellen Techniken der modernen Kryptographie wie Verschlüsselung und digitale Signaturen. Alle mathematischen Grundlagen werden anhand zahlreicher Beispiele und Übungen behandelt, so dass Lesern ein fundiertes Verständnis der modernen Kryptographie vermittelt wird. In die 5. Auflage hat der Autor die Beweise für die Sicherheit des Lamport-Diffie-Einmalsignaturverfahrens und des Merkle-Signaturverfahrens sowie einen Abschnitt über algebraische Angriffe auf Blockchiffren neu aufgenommen.

Buchrückseite

Das Internet durchdringt alle Lebensbereiche: Gesundheitsversorgung, Bildung, Unterhaltung, Produktion, Logistik, Verkauf, den Finanzsektor, die öffentliche Verwaltung aber auch kritische Infrastrukturen wie Verkehr, Energieversorgung und Kommunikationsnetze. Kryptographie ist eine zentrale Technik für die Absicherung des Internets. Ohne Kryptographie gibt es im Internet keine Sicherheit. Kryptographie entwickelt sich ständig weiter und ist ein hochaktuelles Forschungsgebiet. Dieses Kryptographiebuch ist geschrieben für Studierende der Mathematik, Informatik, Physik, Elektrotechnik oder andere Leser mit mathematischer Grundbildung und wurde in vielen Vorlesungen erfolgreich eingesetzt. Es behandelt die aktuellen Techniken der modernen Kryptographie, zum Beispiel Verschlüsselung und digitale Signaturen. Das Buch vermittelt auf elementare Weise alle mathematischen Grundlagen, die zu einem präzisen Verständnis der Kryptographie nötig sind, mit vielen Beispielen und Übungen. Die Leserinnen und Leser dieses Buches erhalten ein fundiertes Verständnis der modernen Kryptographie und werden in die Lage versetzt Forschungsliteratur zur Kryptographie zu verstehen. In der fünften Auflage hat der Autor die Beweise für die Sicherheit des Lamport-Diffie-Einmalsignaturverfahren und des Merkle-Signaturverfahren erweitert und einen Abschnitt über algebraische Angriffe auf Blockchiffren neu aufgenommen. Es handelt sich dabei um eine Angriffstechnik, die neue Anforderungen an die Konstruktion von kryptographischen Verfahren stellt.Aus den Rezensionen zur 2. Auflage:„Diese von einem Mathematiker geschriebene „Einführung in die Kryptographie" fällt sofort durch ihren präzisen und logisch einwandfreien Stil auf. Die verwendeten Begriffe (Verschlüsselungsverfahren, perfekte Sicherheit, Hashfunktion,...) werden mathematisch sauber und kurz definiert, und es wird sehr wohl unterschieden, was „bewiesen" ist [...] und was „allgemeiner Glaube der Experten" ist.Trotz dieser mathematischen Genauigkeit ist dieses Buch

insbesondere für Anfänger und speziell auch für Nicht-Mathematiker sehr verständlich gehalten. Das nötige mathematische Werkzeug (Restklassenringe, Matrizen und lineare Abbildungen, Wahrscheinlichkeit, Erzeugung von Primzahlen, Faktorisierungsverfahren, Ausblick auf elliptische Kurven) wird vor der jeweiligen Anwendung vorgestellt. Dann wird der Themenkreis prägnant, sehr verständlich und mit Beispielen illustriert, besprochen, wobei der Geübte die dahinterliegende mathematische Idee schnell erkennen kann. Dabei werden im Wesentlichen alle Basistechniken der modernen Kryptographie erfasst. Soweit möglich bzw. üblich, wird das englische Fachvokabular der Kryptographie in die deutsche Sprache übersetzt. Ich hoffe, dass die Freude des Rezensenten beim Lesen dieses Buches auch von vielen anderen Lesern ebenfalls empfunden werden kann."
(Int. Math. Nachrichten 2002, Vol 56, Issue 189).„[...] „Klein, aber fein" ist das Charakteristikum des Buches: Jeder Abschnitt ist mit (für Mathematiker) sehr anschaulichen Beispielen und kleinen Übungsaufgaben versehen. Entwickler finden hier eine reiche Quelle der Hintergründe, die sie für eine Implementation wissen müssen."
(Amazon.de-Redaktion)

Lesen Sie Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann für online ebookEinführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann Kostenlose PDF d0wnl0ad, Hörbücher, Bücher zu lesen, gute Bücher zu lesen, billige Bücher, gute Bücher, Online-Bücher, Bücher online, Buchbesprechungen epub, Bücher lesen online, Bücher online zu lesen, Online-Bibliothek, greatbooks zu lesen, PDF Beste Bücher zu lesen, Top-Bücher zu lesen Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann Bücher online zu lesen.Online Einführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann ebook PDF herunterladenEinführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann DocEinführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann MobipocketEinführung in die Kryptographie (Springer-Lehrbuch) (German Edition) von Johannes Buchmann EPub