Kryptografie Fur Entwickler

Getting the books **kryptografie fur entwickler** now is not type of inspiring means. You could not lonely going like book stock or library or borrowing from your friends to door them. This is an very simple means to specifically get lead by on-line. This online proclamation kryptografie fur entwickler can be one of the options to accompany you in imitation of having supplementary time.

It will not waste your time. give a positive response me, the e-book will totally reveal you additional matter to read. Just invest tiny mature to admittance this on-line statement **kryptografie fur entwickler** as competently as review them wherever you are now.

Visual Basic 2008 Jürgen Kotz 2008

Informations- und Kommunikationstechnologien im Krankenhaus Britta Herbig 2006

Linux-Administrations-Handbuch Evi Nemeth 2007

Kryptographie und IT-Sicherheit Joachim Swoboda 2008-04-11 Kryptographische Verfahren sind unverzichtbar bei der Realisierung von elektronischen Geschäftsprozessen. Sie sichern die Abrechnung in Mobilfunknetzen und bilden eine Basis für Sicherheit im Internet und in Endgeräten sowie für die elektronische Vergabe von Lizenzen. In diesem Buch werden Sicherheitsdienste und Sicherheitsmechanismen begrifflich eingeführt und einfache kryptographische Mechanismen anhand historischer Verfahren veranschaulicht. Moderne kryptographische Algorithmen basieren auf diskreter Algebra; diese kann mit einfachen Beispielen intuitiv nachvollzogen werden. Mit elliptischen Kurven und Quanten-Kryptographie werden auch neuere Bereiche angesprochen. Neben den grundlegenden kryptographischen Mechanismen und Protokollen gibt das Buch Einblick in Anwendungen wie neuere Sicherheitsverfahren im Internet und in Mobilfunknetzen, Betriebssysteme von Chipkarten, Trusted Computing und Public-Key-Infrastrukturen.

Blockchain fur Dummies Tiana Laurence 2017-11-13 Blockchain verspricht, Finanztransaktionen im Besonderen und die Informationssicherheit im Allgemeinen zu revolutionieren. Nachträgliche Datenmanipulationen sind unmöglich. Je früher Sie wissen, wie die Blockchain arbeitet, desto eher können Sie und Ihr Unternehmen von der neuen Technologie profitieren. Dieses Buch beantwortet Ihre Fragen, was die Blockchain ist, wie sie funktioniert und welches Potenzial sie hat.

c't Windows optimieren (2018) c't-Redaktion 2018-08-02 Windows 10 bringt eine Vielzahl an nützlichen Funktionen mit, für die man früher zusätzliche Software brauchte. Das Sonderheft "c't Windows optimieren" bündelt eine Fülle an Tipps, wie man Windows 10 optimal einrichten, absichern, effizient verwalten, aufräumen und reparieren kann. So erfahren Sie, wie Sie die Windows-10-Optik ihren Bedürfnissen anpassen und das Startmenü effizienter gestalten. Sie bekommen Tipps zum kostenlosen Umstieg von Windows 7 oder 8.1 auf Windows 10, der Sie mit einem Berg an Neuerungen konfrontiert. Viele davon sind praktisch oder schick, doch es gibt Fallstricke, die Sie mit diesem Heft aus dem Weg räumen. Wenn Windows klemmt, will man nicht mühsam nach den Ursachen forschen,

sondern eine schnelle Lösung ist gefragt. Genau dafür enthält das aktuelle Betriebssystem etliche Mechanismen, die mit wenigen Klicks die häufigsten Probleme zuverlässig beseitigen. Windows bringt inzwischen auch eigene Sicherheitsfunktionen mit, die bei Virenschutz, Verschlüsselung & Co fast alle Wünsche erfüllen. Eine Windows-Installation belegt im Laufe der Zeit immer mehr Platz auf der Festplatte beziehungsweise auf der SSD – wenn man ihr dies nicht abgewöhnt. Mit den Tipps der c't-Redaktion beheben Sie den Platzmangel selbst bei kleinen Speichern dauerhaft.

Blockchain für Dummies Tiana Laurence 2019-08-16 Die Blockchain-Technologie verspricht, den Finanzmarkt, die Versicherungsbranche, das Supply-Chain-Management und andere Branchen zu revolutionieren. Aber Sie müssen kein Tech-Nerd sein, um die Blockchain zu verstehen. Dieses Buch erklärt die Grundlagen und wichtige Anwendungen wie Kryptowährungen und Smart Contracts. Reale Beispiele machen deutlich, wie Blockchains funktionieren und wo ihr Mehrwert liegt. Erstellen Sie eine eigene Blockchain, schauen Sie sich die wichtigsten Blockchain-Anbieter an, erkennen Sie das Disruptionspotenzial für eingesessene Industrien und vieles mehr.

Electronic commerce Otto W. Gardon 2000

Super Secreto – Die Dritte Epoche der Kryptographie Theo Tenzer 2022-03-21 Die weltweite Krise der Privatsphäre im 21. Jahrhundert umfasst zugleich die Diskussionen um ein Recht auf Verschlüsselung sowie um Einschränkungen der sog. Ende-zu-Ende-Verschlüsselung. Um vertraulich und abhörsicher zu kommunizieren, bedarf es einfacher und praktischer Verschlüsselung für alle. Doch wie kann diese wirklich allen zur Verfügung stehen? Die Magie, lesbare Zeichen durch andere, anscheinend zufällige und damit unlesbare Zeichen zu ersetzen, hatte seit Jahrhunderten fast schon etwas Religiöses: Nur Eingeweihte in die Erfindung einer Geheimsprache konnten die Botschaften knacken. Verschlüsselung blieb Super Secreto – Top Secret – Streng Geheim! Im Zeitalter der Smartphone- und Taschen-Computer steht sie nun allen zur Verfügung: immer raffiniertere Mathematik berechnet in unseren Messengern den sog. Cipher-Text mit entsprechenden Schlüsseln. Und beides – Schlüssel wie der verschlüsselte Text – musste früher zum Empfänger übertragen werden. In der heutigen Epoche der Kryptographie ist die Übertragung der Schlüssel nicht mehr notwendig: Der riskante Transportweg für die Schlüssel kann sogar entfallen! Von der Faszination, wie Kryptographie abstinent wurde in der Übermittlung von Schlüsseln – welche Auswirkung es auf den Wunsch der Interessierten nach Zweitschlüsseln hat – und wie mehrfache sowie exponentielle Verschlüsselung resistent machen gegen die Entschlüsselungsversuche von Super-Quanten-Computern, ... erzählt Theo Tenzer in diesem spannenden politischen, technischen und gesellschaftsrelevanten Innovations- und Wissenschaftsportrait zur Dritten Epoche der Kryptographie.

Cyber-Sicherheit Norbert Pohlmann 2019-07-30 Dieses Lehrbuch gibt Ihnen einen Überblick über die Themen der IT-Sicherheit Die Digitalisierung hat Geschäftsmodelle und Verwaltungsprozesse radikal verändert. Dadurch eröffnet der digitale Wandel auf der einen Seite viele neue Möglichkeiten. Auf der anderen Seite haben Hacker jüngst mit Cyber-Angriffen für Aufsehen gesorgt. So gesehen birgt die fortschreitende Digitalisierung auch Gefahren. Für eine erfolgreiche Zukunft unserer Gesellschaft ist es daher entscheidend, eine sichere und vertrauenswürdige IT zu gestalten. Norbert Pohlmann gibt Ihnen mit diesem Lehrbuch eine umfassende Einführung in den Themenkomplex der IT-Sicherheit. Lernen Sie mehr über Mechanismen, Prinzipien, Konzepte und

Eigenschaften von Cyber-Sicherheitssystemen. Der Autor vermittelt aber nicht nur theoretisches Fachwissen, sondern versetzt Sie auch in die Lage, die IT-Sicherheit aus der anwendungsorientierten Perspektive zu betrachten. Lesen Sie, auf welche Sicherheitseigenschaften es bei Cyber-Systemen ankommt. So sind Sie mit Hilfe dieses Lehrbuchs in der Lage, die Wirksamkeit von IT-Lösungen mit Blick auf deren Sicherheit zu beurteilen. Grundlegende Aspekte der Cyber-Sicherheit Im einführenden Abschnitt dieses Lehrbuchs vermittelt Ihnen Pohlmann zunächst die Grundlagen der IT-Sicherheit und schärft Ihren Blick für folgende Aspekte: Strategien Motivationen Bedürfnisse Probleme Herausforderungen Wirksamkeitskonzepte Tauchen Sie tiefer in die Materie ein In den darauffolgenden Kapiteln befasst sich Pohlmann mit diesen Teilbereichen der IT-Sicherheit Kryptographie Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen Digitale Signatur, elektronische Zertifikate sowie PKIs und PKAs Identifikation und Authentifikation Enterprise Identity und Access Management Trusted Computing Cyber-Sicherheit Frühwarn- und Lagebildsysteme Firewall-Systeme E-Mail-Sicherheit Blockchain-Technologie Künstliche Intelligenz und Cyber-Security Social Web Cyber-Sicherheit Zudem erfahren Sie mehr über IPSec-Verschlüsselung, Transport Layer Security (TLS), Secure Socket Layer (SSL) sowie Sicherheitsmaßnahmen gegen DDoS-Angriffe. Anschauliche Grafiken und Tabellen bilden Prozesse und Zusammenhänge verständlich ab. Didaktisch gut aufbereitet, können Sie die Inhalte mit zahlreichen Übungsaufgaben vertiefen. Das Lehrbucht richtet sich speziell an Leser, für die die IT-Sicherheit eine besondere Rolle spielt, etwa: Studierende der Informatik Auszubildende im Bereich Fachinformatik Mitarbeiter und Führungspersonen der IT-Branche

Super Secreto - Verschlüsselung für alle Theo Tenzer 2022-04-01 Die vorliegende Tutorial- und Taschenbuch-Ausgabe des Bandes "Super Secreto - Die Dritte Epoche der Kryptographie" gibt eine Einführung in die »streng-geheime« Kommunikation und integriert gesellschaftlich-politische Sichtweisen mit technischen Innovationen sowie Hinweisen zu praktischen Programmen und Werkzeugen zur Verschlüsselung: Mit der sog. »Ende-zu-Ende«-Verschlüsselung für alle kann die Privatsphäre der Bürger:innen gesichert bleiben: nicht nur mit »GPG«, aufgrund der wachsenden Rechenkraft von Quanten-Computern idealerweise auch mit Algorithmen wie »McEliece« oder »NTRU« - oder gar einer Multi-Verschlüsselung, bei der sog. »Cipher-Text« noch weitere Male verschlüsselt wird. Quell-offene Messenger wie »Delta-Chat« oder »Smoke-Chat Messenger« sind damit bestens ausgerüstet und Software-Programme wie die aus praktischen Tutorials bekannte und sehr ausgearbeitete Encryption-Suite »Spot-On« oder »VeraCrypt« wie auch mehr als zwei Dutzend weitere erläuterte Crypto-Werkzeuge zeigen good-practice Modelle kryptographischer Innovationen. Nur sog. »TEE«-Ausführungsumgebungen ggf. ohne Internet wandeln zukünftig Texte vertrauensvoll. In diesem Buch werden epochale Veränderungen durch Quanten-Computer und Überwachungsmaßnahmen beleuchtet und auch die Grundlagen der Derivativen Kryptographie vertieft, bei der Schlüssel nicht mehr übertragen werden, sondern rechnerisch abgeleitet sind: Das Schlüssel-Transport-Problem wurde in angewandter Kryptographie nun für Messenger gelöst. "Verschlüsselung für alle" gibt dazu einen Überblick.

Moderne Kryptographie Ralf Küsters 2011-08-04 Dieses Buch behandelt die Kernfragen und grundlegenden Verfahren der Kryptographie. Diese werden aus Sicht der modernen Kryptographie studiert, die durch eine präzise mathematische und informatische Herangehensweise geprägt ist. Die Inhalte dieser Einführung sind dabei aus der Praxis motiviert und es werden wichtige, in der Praxis eingesetzte kryptographische Verfahren, vorgestellt und diskutiert.

Java-Web-Security Dominik Schadow 2014-02-24 Java hat den Ruf, eine relativ sichere Programmiersprache zu sein. Verschiedene Spracheigenschaften und Java-interne Sicherheitsmechanismen unterstützen den Entwickler beim Erstellen sicherer Anwendungen. Sie helfen aber nicht, wenn bei der Programmierung ungewollt Schwachstellen eingebaut werden, über die Übeltäter erfolgreiche Angriffe durchführen können. Das betrifft insbesondere Webapplikationen für Intranets oder das Internet. Dieses Buch zeigt, wie Sie als Java-Entwickler vielen dieser teilweise längst bekannten Unzulänglichkeiten und Programmierfehlern entgegentreten können. Dabei erfahren Sie Hintergründe zu Java-basierten Sicherheitsmechanismen und bekommen einen Überblick über hilfreiche Tools. Sie lernen unter anderem folgende Angriffsformen kennen und erfahren, wie Sie Ihre Java-Webapplikationen von diesen Schwachstellen freihalten: - Injections, u.a. SQL Injection - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF) Nicht immer ist es nötig, dass Sie die eigene Entwicklungsmethodik oder gar Ihren Software-Entwicklungsprozess komplett umkrempeln. An vielen Stellen genügen geringe Änderungen am Code und kleine Anpassungen der eigenen Entwicklungsweise. Die auf diese Weise entstehenden Webapplikationen profitieren von einer höheren Sicherheit und machen das Ausnutzen von sicherheitskritischen Programmierfehlern für Angreifer deutlich schwieriger. Vorausgesetzt werden Kenntnisse der Java-Programmierung, vor allem im Umfeld von Webanwendungen.

Pseudozufallszahlen in der Kryptographie Christian Schiestl 2001-05-16 Inhaltsangabe:Einleitung: Viele Bereiche der Informatik sind in steigendem Ausmaß auf Zufallszahlen angewiesen. Man denke nur an Monte-Carlo-Simulationen, Optimierungen mittels genetischer Algorithmen oder aber an Computerspiele, die ohne intelligente Monster wohl nur halb so interessant wären. Durch die zunehmende weltweite Vernetzung von Rechnern haben Sicherheitsaspekte in den letzten Jahren an Bedeutung gewonnen. Schutzmechanismen gegen unbefugten Zugriff auf vertrauliche Daten sowie zur Authentifizierung und Identifikation von Kommunikationspartnern spielen eine immer größer werdende Rolle. Kryptographische Verfahren wie symmetrische Verschlüsselungs-, Public-Key- und Signaturverfahren bieten Möglichkeiten, diese Sicherheitsrisiken zu verringern. Gerade diese kryptographischen Basismechanismen kommen heutzutage kaum noch ohne Zufallszahlen aus. Beinahe jedes Kryptosystem benötigt irgendwann geheime, nicht vorhersagbare Zufallszahlen. Ohne Zufallsgeneratoren gäbe es keine Kryptographie! Man denke nur an folgende, exemplarische Einsatzgebiete: Schlüsselerzeugung: Symmetrische und asymmetrische Kryptosysteme benötigen für die sichere Datenverschlüsselung zufällige Schlüssel. Parametererzeugung: Ein weiteres wichtiges Einsatzgebiet für Zufallszahlen ist die Erzeugung von Parametern für asymmetrische Verschlüsselungsverfahren (z.B. die Generierung großer Primzahlen im RSA-Verfahren). Symmetrische Blockchiffren im CBC-Mode erfordern in Form von Initialisierungsvektoren ebenfalls zufällige Parameter. Identifikationsprotokolle: Bei Challenge-Response-Verfahren wird auf einer Seite eine zufällige Challenge erzeugt, die die Gegenseite mit ihrem geheimen Schlüssel in signierter Form retourniert. Im Zuge einseitiger Challenge-Response-Verfahren empfängt und verarbeitet beispielsweise jedes GSM-Handy bei jeder Netzanmeldung eine Zufallszahl. Digitale Signatur-Verfahren: Bestimmte digitale Signatur-Verfahren (wie z. B. DSA, ElGamal) benötigen bei jedem Signiervorgang einen neuen Zufallswert. Bei Zero-Knowledge-Signatur-Verfahren setzt der Signierende eine Zufallszahl ein, um sein Geheimnis zu verbergen. Protokolle zur Schlüsselverteilung: Zu Beginn einer Sitzung müssen zufällige Sitzungsschlüssel erzeugt und verteilt werden. Bei Diffie-Hellman ähnlichen Protokollen benötigen dazu beide Parteien jeweils einen zufälligen Startwert. Verschlüsselung: Zufallsfolgen können unmittelbar zur Verschlüsselung

eingesetzt werden. Man denke dabei an das [...]

Kryptographie in C und C++ Michael Welschenbach 2013-03-07 Das Buch bietet einen umfassenden Überblick über die Grundlagen moderner kryptographischer Verfahren und ihre programmtechnische Entwicklung mit Hilfe einer leistungsfähigen Erweiterung der Programmiersprachen C und C++. Es präsentiert fundierte und einsetzbare Funktionen und Methoden mit professioneller Stabilität und Performanz. Ihre Umsetzung wird an einer objektorientierten Implementierung des RSA-Kryptosystems demonstriert. Der zum neuen amerikanischen Advanced Encryption Standard (AES) erklärte Algorithmus "Rijndael" wird ausführlich mit vielen Hinweisen für die Implementierung erläutert. Die beiliegende CD-ROM bietet mit optimierten Implementierungen des Standards in C und C++, kryptographischen Funktionen in C und C++, einer umfangreichen Testsuite für die Arithmetik den Lesern einen gut sortierten Baukasten für eigene Anwendungen.

iX Developer – Java 2017 iX-Redaktion 2017-06-26 Was lange währt, wird letztlich gut: 2017 erscheinen endlich neue Versionen von Java SE und Java EE. Modularität, interaktive Shell, HTTP-2.0-Support, Cloud-Fokus und einiges andere mehr sollen ein zeitgemäßes Java sichern – auch mehr als 20 Jahre nach der initialen Einführung. Das 156 Seiten dicke Sonderheft zu Java 9 und Java EE 8 bringt Entwickler auf den neuesten Stand und vermittelt einen tief schürfenden Eindruck von der seit Jahren weltweit wichtigsten Programmierplattform. Das „Java 2017“-Sonderheft enthält in der digitalen Ausgabe einen Link, über den der auf Heft-DVD erhältliche Inhalt per Download zu beziehen ist. Es handelt sich um wichtige Werkzeuge für Java-Entwickler, Konferenzvideos, über 200 Seiten Buchauszüge zur Java-Entwicklung und sämtliche Beispielanwendungen und Listings zu den Artikeln des Heftes.

Bitcoin für Dummies Peter Kent 2022-09-14 Bitcoin bieten Ihnen neue Möglichkeiten, wie Sie Ihr Geld anlegen und grundlegende Transaktionen im Zahlungsverkehr durchführen können. Der erste Schritt in die Welt der Kryptowährungen kann jedoch verwirrend und einschüchternd sein. Dieses Buch ist Ihre Orientierungshilfe: Peter Kent und Tyler Bain erklären Ihnen die technischen Hintergründe und zeigen Ihnen, wie Sie Bitcoin kaufen, eine Wallet erstellen und mit Bitcoin bezahlen. Außerdem erfahren Sie, was Sie bei der Investition in Bitcoin beachten müssen und wie Sie sich vor Betrügern schützen.

Algorithmen für Dummies John Paul Mueller 2017-09-18 Wir leben in einer algorithmenbestimmten Welt. Deshalb lohnt es sich zu verstehen, wie Algorithmen arbeiten. Das Buch präsentiert die wichtigsten Anwendungsgebiete für Algorithmen: Optimierung, Sortiervorgänge, Graphentheorie, Textanalyse, Hashfunktionen. Zu jedem Algorithmus werden jeweils Hintergrundwissen und praktische Grundlagen vermittelt sowie Beispiele für aktuelle Anwendungen gegeben. Für interessierte Leser gibt es Umsetzungen in Python, sodass die Algorithmen auch verändert und die Auswirkungen der Veränderungen beobachtet werden können. Dieses Buch richtet sich an Menschen, die an Algorithmen interessiert sind, ohne eine Doktorarbeit zu dem Thema schreiben zu wollen. Wer es gelesen hat, versteht, wie wichtige Algorithmen arbeiten und wie man von dieser Arbeit beispielsweise bei der Entwicklung von Unternehmensstrategien profitieren kann.

Kryptographie und IT-Sicherheit Stephan Spitz 2011-03-23 Kryptographische Verfahren sind unverzichtbar bei der Realisierung von elektronischen Geschäftsprozessen. Sie sichern die Abrechnung in Mobilfunknetzen und bilden

eine Basis für Sicherheit im Internet und in Endgeräten sowie für die elektronische Vergabe von Lizenzen. In diesem Buch werden Sicherheitsdienste und Sicherheitsmechanismen begrifflich eingeführt und einfache kryptographische Mechanismen anhand historischer Verfahren veranschaulicht. Moderne kryptographische Algorithmen basieren auf diskreter Algebra; diese kann mit einfachen Beispielen intuitiv nachvollzogen werden. Mit elliptischen Kurven werden auch neuere Bereiche angesprochen. Neben den grundlegenden kryptographischen Mechanismen und Protokollen gibt das Buch Einblick in Anwendungen wie neuere Sicherheitsverfahren im Internet und in Mobilfunknetzen, Betriebssysteme von Chipkarten, Trusted Computing und Public-Key-Infrastrukturen.

Blockchain - und wie sie funktioniert Alan T. Norman 2019-11-05 Hier geht es nicht um Investitionen, sondern um die Funktionsweise der Blockchain-Technologie und ihre mögliche zukünftige Nutzung Anstatt über Investitionen zu sprechen, wird sich dieses Buch auf die Funktionsweise der Blockchain-Technologie und ihren möglichen zukünftigen Nutzen konzentrieren. Folgende Themen werden in diesem Buch behandelt: ●Welches Problem löst die Blockchain? ●Wie kann Technologie unsere Institutionen schneller und kostengünstiger machen? ●Könnte die Technologie unsere Institutionen (wie Regierungen, Banken usw.) vollständig ersetzen? ●Wie kann die Blockchain Vertrauen zwischen Fremden aufbauen? ●Wie erhöht Blockchain die Sicherheit für Transaktionen und Verträge? ●Kann die Blockchain auch außerhalb der Finanzwelt eingesetzt werden? ●Was ist ein Block? ●Was ist die Kette und warum brauchen wir sie? ●Was lautet die technische Erklärung dafür, was in der Blockchain geschieht? ●Was ist Mining und warum wird es benötigt? ●Gibt es im Hinblick auf die Erstellung einer Blockchain Alternativen zum Mining? ●Was ist die Geschichte von Bitcoin? ●Verursacht Bitcoin Probleme? ●Was ist Ethereum und was ein Smart Contract? ●Gibt es noch andere Blockchain-Technologien, über die ich Bescheid wissen sollte? ●Wie setzen Unternehmen Blockchain ein? ●Welche regulatorischen Hürden könnten der Einführung von Blockchain im Wege stehen? Das ist ein ganzes Bündel an Fragen. Wenn Sie bereit sind, sich damit auseinanderzusetzen, können wir beginnen. PUBLISHER: TEKTIME

Kryptografie für Entwickler Thomas St Denis 2017-04-10

c't Linux-Guide 2022 c't-Redaktion 2022-06-23 Mit dem neuen Sonderheft "c't Linux-Guide" behalten Sie Ihr Wunschsystem im Griff. Unser Linux-Netzplan schafft Orientierung für Einsteiger und bietet heimisch gewordenen Linuxern einen Blick über den Tellerrand. Wir zeigen, wie Sie Linux neben Windows installieren, auf Software aus verschiedenen Quellen zugreifen, Updates automatisieren und Ihre privaten Dateien verschlüsseln, ohne sich auszusperren. Wer unter die Haube schauen möchte, erfährt, was der Wechsel von X zu Wayland für die Zukunft von Linux bedeutet.

Sicherheit von Webanwendungen in der Praxis Matthias Rohr 2018-03-19 Webanwendungen bilden in Unternehmen zahlreiche sensible Geschäftsprozesse ab - ob mit Kunden, mit Mitarbeitern, Partnern und Zulieferern. Daher sind Webapplikationen ein Sicherheitsrisiko für Unternehmen und ihr Schutz von entscheidender Bedeutung. In dem Buch beleuchtet der Autor die wichtigsten Aspekte der Webanwendungssicherheit und stützt sich dabei auf seine langjährige Erfahrung als IT-Security-Berater für Webanwendungen und Entwicklungsprozesse. Der Band bietet neben einem allgemeinen Überblick zum Thema Sicherheit von Webanwendungen ausführliche und praxisorientierte Darstellungen zu wichtigen Einzelfragen: Was sind die häufigsten Schwachstellen und mit welchen Maßnahmen

lassen sich Webanwendungen am effektivsten gegen Angriffe absichern? Ein eigenes Kapitel befasst sich mit den Verfahren, die eingesetzt werden, um die Sicherheit von Anwendungen bereits im Entwicklungsprozess zu bewerten und zu überprüfen. Der Autor erläutert zudem, wie sich die Sicherheit in selbst entwickelten und zugekauften Webanwendungen durch organisatorische Prozesse nachhaltig verbessern lässt. Die zweite Auflage des 2014 erstmals erschienen Buchs wurde vor dem Hintergrund neuer Techniken zur Abwehr von Angriffen und neuer Prüfverfahren vollständig überarbeitet und aktualisiert. Auch aktuelle Beratungsprojekte des Autors haben Eingang in die Neuauflage gefunden – insbesondere dort, wo es um organisatorische Aspekte von Webanwendungssicherheit geht. Der Band richtet sich an Entwickler von Webanwendungen, IT-Security- und Qualitätsmanager genauso wie an Leser, die sich in das Thema Webanwendungssicherheit einarbeiten wollen.

Blockchain-Technologie in der Energiewirtschaft Bartek Mika 2019-11-26 Der Ausbau von erneuerbaren Energien nimmt im Zuge der Energiewende rasch zu. Die Struktur der Energieversorgungssysteme wird daher zunehmend dezentral organisiert und neue Akteure wie Prosumer, die ihren Strom selbst erzeugen und verbrauchen, können sich zukünftig auf dem Strommarkt etablieren. Hierdurch rücken Themenfelder wie die zunehmende Steuerungskomplexität, die Belastung der Netzinfrastruktur sowie hohe Anforderungen an die Datensicherheit in den Fokus. Die Blockchain-Technologie kann maßgeblich zur Lösung einiger der auftretenden Fragen und Probleme beitragen. Das vorliegende Buch beschäftigt sich mit der Frage, ob die Blockchain-Technologie als Treiber der Energiewende wirken kann und mit welchen neuen digitalen Geschäftsmodellen sie zur Transformation des Energiesystems beiträgt. Hierzu wird ein blockchainbasiertes Geschäftsmodell für den dezentralen Peer-to-Peer Stromhandel entwickelt und vorgestellt sowie die zu bewältigenden Herausforderungen am Markt diskutiert.

Visuelle Kryptographie Andreas Klein 2007-08-23 Mit Erfindung der Schrift entstand gleichzeitig der Bedarf, Geschriebenes vor unbefugten Lesern zu verbergen. Als Wissenschaft im modernen Sinne ist die Kryptographie jedoch noch sehr jung. 1994 erfanden Naor und Shamir folgendes Verfahren: Sie verteilten ein Bild so auf zwei Folien, dass auf jeder einzelnen Folie nur ein zufälliges Punktmuster zu sehen ist, aber beide Folien übereinander gelegt ein geheimes Bild ergeben. Das Buch gibt einen Einblick in die aktuelle Forschung, verzichtet aber bewusst auf Höhere Mathematik. Daher eine ideale Grundlage für Proseminare und Mathematik-AGs der Sekundarstufe. Plus: Aufgaben mit Musterlösungen.

Nicht hackbare Rechner und nicht brechbare Kryptographie Wolfgang A. Halang 2018-11-23 Viren, Würmer, Trojanische Pferde, das Arsenal der Hackerangriffe auf IT-Infrastrukturen scheint unerschöpflich. Nachdem Computerwurm Stuxnet 2010 das Steuerungssystem eines iranischen Atomkraftwerks befallen hatte und Computer durch die Malware Flame ferngesteuert und ausspioniert wurden, sorgte 2015 ein Virus namens Duqu 2.0 für Schlagzeilen, weil er die IT von Unternehmen in Europa, Asien und den USA infiziert hatte. Was aber wenn Computer grundsätzlich gegen solche Hackerangriffe immun wären? Wissenschaftlich fundiert und zugleich verständlich geschrieben, zeigen die beiden IT-Experten in ihrem Buch, wie Computer mithilfe von bekannten technischen Verfahren so konstruiert werden können, dass Hackerangriffe grundsätzlich an ihnen abprallen. Zum einen setzen die Autoren für die IT-Sicherheit auf eine Rechnerarchitektur, die in mindestens zwei Segmente unterteilt ist: in einen schreibgeschützten und für Programme nicht beeinflussbaren Bereich sowie einen nicht-schreibgeschützten Bereich für Daten gibt, die sich oft ändern.

Kombiniert unter anderem mit effektiven Verschlüsselungs- und Verschleierungsverfahren, einer sichereren Authentifizierung der Nutzer etwa durch biometrische Merkmale sowie sicheren virtuellen Adressen und Seitenverzeichnisstartadressen werden Computer unangreifbar für Software, die unerlaubt in den Rechner eindringt und Daten abschöpft. Die Autoren gehen in ihrer technisch-wissenschaftlich exakten Darstellung auf folgende Fragen ein: - Wie sicher sind Rechner und Netze heute? - Wie funktionieren Angriffe mit Stuxnet, Flame und Duqu und wie die Methoden zu ihrer Abwehr? - Welchen Schutz bieten Harvard- und Von-Neumann-Architekturen (VNA)? - Wie sehen neuartige Schutzmaßnahmen aus und wie können mobile Geräte geschützt werden? - Wie funktioniert sichere Datenverschlüsselung und -verschleierung? Das Buch richtet sich an IT-Experten und IT-Sicherheitsverantwortliche in Unternehmen und Organisationen und an alle, die sich für Fragen der Daten- und Netzsicherheit interessieren. Für das Verständnis sind nur elementare Vorkenntnisse erforderlich.

Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment Nils Braun-Dubler 2020-06-16 Blockchain is widely considered a new key technology. The Foundation for Technology Assessment (TA-SWISS) has proposed a comprehensive assessment of blockchain technologies. With this publication, TA-SWISS provides the much-needed social contextualisation of blockchain. The first, more technical part of the study takes an in-depth look at how blockchain functions and examines the economic potential of this technology. By analysing multiple real-world applications, the study sheds light on where the blockchain has advantages over traditional applications and where existing technologies continue to be the better solution. The second part of the study examines how blockchain became mainstream. It explores the origins of blockchain in the early history of information technology and computer networks. The study also reveals the impact blockchain has on industrial and public spaces. Finally, it discusses the social implications and challenges of blockchain against the background of a new socio-technical environment.

Allgemeinbildung Digitalisierung für Dummies Christina Czeschik 2022-03-14 "Die Digitalisierung geht nicht mehr weg." - Ein grundlegendes Verständnis der Prinzipien der Digitalisierung und ihrer wichtigsten Anwendungen ist deshalb die Voraussetzung, um im Beruf und als Privatperson informierte Entscheidungen treffen zu können - ob es nun um Kryptowährungen, New Work oder den Schutz der eigenen Daten in sozialen Medien geht. In diesem Buch wird das Thema Digitalisierung anschaulich und unterhaltsam aufbereitet. Der Fokus liegt auf der fundierten und leicht verdaulichen Vermittlung der Grundlagen, die es Ihnen ermöglicht, nach der Lektüre eigenständig auf dem Laufenden zu bleiben und neue Entwicklungen mit ihren Konsequenzen zu verstehen und einzuordnen.

Internet-Security aus Software-Sicht Walter Kriha 2008-01-08 Die Praxis zeigt, dass bei der Entwicklung großer, komplexer Softwaresysteme Sicherheitsaspekte oft gar nicht oder erst sehr spät berücksichtigt werden. IT-Security-Spezialisten werden in die Entwicklung neuer Systeme oft nicht eingebunden, und Softwareentwicklern fehlt häufig das Bewusstsein für Sicherheitsprobleme und die nötigen Detailkenntnisse, vorhandene Lösungen richtig einzusetzen. Hier setzt das Buch an und schlägt eine Brücke von der Softwaresicht zu mehr netzwerkorientierten Aspekten der Internet-Security. Ziel der Autoren ist es, bei Entwicklern und Projektleitern ein grundlegendes Sicherheitsbewusstsein zu schaffen und ihnen einen Leitfaden für den Bau sicherer verteilter Systeme an die Hand zu geben. Sicherheitsprobleme werden anhand konkreter Beispiele diskutiert und passende Lösungen aufgezeigt.

Introduction to Cryptography Johannes Buchmann 2013-12-01 This book explains the basic methods of modern cryptography. It is written for readers with only basic mathematical knowledge who are interested in modern cryptographic algorithms and their mathematical foundation. Several exercises are included following each chapter. From the reviews: "Gives a clear and systematic introduction into the subject whose popularity is ever increasing, and can be recommended to all who would like to learn about cryptography." --ZENTRALBLATT MATH

Erfolgreich Visual Basic 2010 programmieren Jürgen Kotz 2011 Werden Sie Visual Basic 2010-Profi!Das Buch spricht alle Themen an, die bei der täglichen Visual Basic-Programmierung eine Rolle spielen. Alle wichtigen Aspekte von Programmiergrundlagen, Windows Forms und WPF, Datenbankabfragen mit LINQ, ein intensiver Einstieg in die objektorientierte Programmierung mit Visual Basic 2010 sowie der Datenbankzugriff mit Access oder auch SQL Server. Mit der Testsoftware auf CD können Sie stets Ihr Wissen überprüfen. Aus dem Inhalt:Programmierung mit Windows FormsVerbindungen zu Datenbanken, wie dem Microsoft SQL Server 2008, mit ADO.NETXMLSerialization, Delegate.

IT-Sicherheit Roland Hellmann 2018-03-19 Noch vor wenigen Jahren war die IT-Sicherheit eher ein Randgebiet, doch inzwischen ist sie in der Informatik, in Unternehmen und auch im Alltagsleben allgegenwärtig. Immer mehr Menschen wird bewusst, dass sie nicht nur gläsern geworden sind, sondern dass sie selbst oder ihr Unternehmen, in dem sie arbeiten, von Bedrohungen ganz konkret gefährdet sind. Schadsoftware verschlüsselt unerwartet alle erreichbaren Daten und erpresst Lösegeld. Firmen werden massiv geschädigt oder gar insolvent, weil ihre Geschäftsgeheimnisse von der Konkurrenz gestohlen werden. Sogar Menschenleben stehen auf dem Spiel, wenn Energieversorger oder Krankenhäuser wegen eines Hackerangriffs funktionsunfähig werden. Ob es sich um die Entwicklung von Software handelt, um die Konfiguration von Netzwerken, Servern und Clients oder mittlerweile auch um Embedded Systems in Fahrzeugen oder der Unterhaltungselektronik - überall sind Kenntnisse der IT-Sicherheit gefragt. Gleichzeitig ist die IT-Sicherheit keine einfache Disziplin: Es kommen in großem Umfang kryptografische Verfahren zum Einsatz, die auf fortgeschrittenen mathematischen Grundlagen beruhen. Ferner spielen außer technischen Belangen und ihren komplexen Zusammenhängen auch rechtliche und Management-Aspekte eine Rolle. Genauso unterschiedlich werden die Vorkenntnisse sein, die Leser mitbringen und die Erwartungen, die sie hegen. Dieses Werk soll Studierenden der Informatik und verwandter Disziplinen helfen, ein grundlegendes Verständnis für die IT-Sicherheit und deren Bedeutung zu entwickeln. Es werden möglichst wenige mathematisch-technische Vorkenntnisse vorausgesetzt, so dass auch Studierende im Informatik-Grundstudium sowie technisch interessierte Studierende der Wirtschaftsinformatik, des Wirtschaftsingenieurwesens oder auch der Betriebswirtschaft davon profitieren sollten. Zu den einzelnen Kapiteln werden Übungsaufgaben gestellt, deren Lösungen im Anhang zu finden sind. Diese machen das Werk besonders geeignet für das Selbststudium. Inhalt: - Grundlagen und Motivation - Kryptologie und ihre Anwendung: Verschlüsselung, Digitale Signatur, Steganographie - Verfügbarkeit - Internetsicherheit und Schadsoftware - Firewalls - Sicherheit im Internet der Dinge

c't Security (2019) c't-Redaktion 2019-04-09 Das Sonderheft c't Security beinhaltet die besten und wichtigsten Security-Artikel aus c't in aktuell aufbereiteter Form. Als Ratgeber für Privatpersonen, Admins und Unternehmen bietet das Sonderheft Sicherheitsstrategien für PC, Smartphone und im Smart Home. Es enthält Informationen zu Gefahren und Risiken sowie zur Tauglichkeit

diverser Schutzmaßnahmen. Startet die Reise ins Internet mit einem Windows-PC, gilt es diesen vor digitalen Bedrohungen zu schützen. Mit welchen Bordmitteln das gelingt, erklären c't Redakteure und gehen dabei besonders auf den Umgang mit Verschlüsselungssoftware, Firewall und Virenscanner ein. Den Virenschutzprogrammen widmet sich eine komplette Rubrik im Heft. Vorgestellt werden Gratis-Tools zum Schutz im Netzwerk, aber auch ein interaktives Malware-Analyse-Tool. Acht Alternativen zum eingebauten Virenscanner von Windows 10 wurden im c't Labor getestet. Das Ergebnis gibt Auskunft, ob sie tatsächlich besser ausgestattet und außerdem noch komfortabler sind. Eine Laufwerksverschlüsselung mit BitLocker hilft, die Daten auf dem eigenen Rechner zu schützen. Und wer auf Reisen nicht auf sein Notebook verzichten kann, demjenigen helfen die praktischen Tipps dabei, das Windows-System mit eigenen Bordmitteln sicherer zu machen. Um die eigenen Daten zu schützen, ist es notwendig Barrieren zu errichten, die es den Dieben schwer machen. Sinnvoll ist ein Einsatz der Zwei-Faktor-Authentifizierung. Auch das Verschlüsseln von USB-Speicher-Medien. Das ist unkomplizierter, als man denkt, und bietet genug Sicherheit. Der Schutz der eigenen Daten umfasst allerdings mehr als nur Computer, Passwörter und Dateien, die gehackt und gestohlen werden können. Inzwischen ist die digitale Identität zum begehrten Angriffsziel geworden. c't Security zeigt, wie man sich vor Identitätsklau schützt und was Opfer von Identitätsmissbrauch dringend tun sollten. Auch ein Blick ins Darknet kann lohnen. Denn es bietet spannende Techniken und Lösungsansätze für Probleme wie Anonymität, Abhörsicherheit und betrugssichere Geschäfte. Tor als Zweitbrowser beispielsweise schützt im Internet vor Browser-Exploits und verhindert das Laden problematischer Inhalte. Dank Multisignatur-Treuhand können Mitglieder von Foren ihre Verkäufe absichern. Einst für zu verschleiernde Aktivitäten im Internet entwickelt, profitieren heute ganz normale Internetnutzer von ihrem Einsatz. Auch das Smartphone kann von Fremden missbraucht werden. Spionage-Apps beispielsweise dienen Stalkern und ermöglichen ihnen, andere Personen zu überwachen. Eine gesamte Rubrik widmet sich dem Thema und hilft diese Software zu erkennen und unschädlich zu machen. Selbst einige der modernen Smart-TVs plaudern und übermitteln Informationen ins Internet. Wie leicht man das unterbinden kann und wie sich die Sicherheit und Privacy am Smart-TV verbessern lässt, beschreibt das Sonderheft in der Rubrik "Clever oder tumb?". In aller Kürze und auf das Wesentlichste komprimiert, geben Security-Checklisten zu allen im Heft vorkommenden Themen einen Überblick.

Kryptographie von Cäsar bis RSA. Klassische und moderne Verfahren im Vergleich Tobias Steinicke 2016-01-27 Studienarbeit aus dem Jahr 2012 im Fachbereich Informatik - IT-Security, Note: 1,0, Fachhochschule der Wirtschaft Bielefeld, Sprache: Deutsch, Abstract: Schon vor Jahrtausenden verschlüsselten Menschen Nachrichten, um diese vor anderen geheim zu halten. Im Laufe der Jahre gab es immer wieder einen Wettkampf zwischen Kryptologen und Kryptoanalysten - Erstere, um eine vermeintlich sichere Methode zu entwickeln, Zweitere, um die Methoden wieder zu knacken. Die vorliegenden Arbeit gibt einen Einblick in die prägnantesten Vertreter von klassische und moderner Kryptographie und Kryptoanalyse.

Kryptografie Klaus Schmeh 2016-04-21 Dieses umfassende Einführungs- und Übersichtswerk zur Kryptografie beschreibt eine große Zahl von Verschlüsselungs-, Signatur und Hash-Verfahren in anschaulicher Form, ohne unnötig tief in die Mathematik einzusteigen. Hierbei kommen auch viele Methoden zur Sprache, die bisher kaum in anderen Kryptografiebüchern zu finden sind. Auf dieser breiten Basis geht das Buch auf viele spezielle Themen ein: Kryptografische Protokolle, Implementierungsfragen, Sicherheits-Evaluierungen,

Seitenkanalangriffe, Malware-Angriffe, Anwenderakzeptanz, Schlüsselmanagement, Smartcards, Biometrie, Trusted Computing und vieles mehr werden ausführlich behandelt. Auch spezielle Kryptografieanwendungen wie Digital Rights Management kommen nicht zu kurz. Besondere Schwerpunkte bilden zudem die Themen Public-Key-Infrastrukturen (PKI) und kryptografische Netzwerkprotokolle (WEP, SSL, IPsec, S/MIME, DNSSEC und zahlreiche andere). Die Fülle an anschaulich beschriebenen Themen macht das Buch zu einem Muss für jeden, der einen Einstieg in die Kryptografie oder eine hochwertige Übersicht sucht. Der Autor ist ein anerkannter Krypto-Experte mit langjähriger Berufserfahrung und ein erfolgreicher Journalist. Er versteht es, Fachwissen spannend und anschaulich zu vermitteln. Die Neuauflage ist aktualisiert und geht auf neueste Standards, Verfahren sowie Protokolle ein. "Eines der umfangreichsten, verständlichsten und am besten geschriebenen Kryptografie-Bücher der Gegenwart." David Kahn, US-Schriftsteller und Kryptografie-Historiker

Schneier on Security Bruce Schneier 2009-03-16 Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

iX Developer Programmiersprachen – Next Generation 2022 iX-Redaktion 2022-08-31 Steter Wandel in der Softwareentwicklung: Neue Patterns bringen frische Konzepte und öffnen die Tür für neue Sprachen. Im iX-Developer-Sonderheft „Programmiersprachen – Next Generation“ finden Entwicklerinnen und Entwickler eine kuratierte Auswahl sowohl neuer als auch aktualisierter Heft- und Online-Artikel, die einen umfassenden Überblick verschaffen und vielfältige Einblicke darin liefern, wie die modernen Programmiersprachen TypeScript, Kotlin, Rust und Go mit neuen Konzepten den Weg zu effizientem, sicherem und wartungsarmem Code weisen. TypeScript bringt Typsicherheit zu JavaScript, Kotlin vermischt funktionale Konzepte mit objektorientierter Programmierung auf der JVM. Gegenüber C bringt das Ownership-Konzept von Rust Speichersicherheit ohne den Overhead eines Garbage Collector, und Go zielt mit Blick auf Cloud-Computing und Anwendungen im Cluster auf nebenläufige Programmierung.

Sicherheit und Kryptographie im Internet Jörg Schwenk 2013-03-09 Besonderen Wert legt der Autor auf die Darstellung, wie bekannte kryptographische Verfahren an die jeweiligen Erfordernisse der Internet-Dienste angepasst wurden.

iX kompakt (2019) iX-Redaktion 2019-05-10 Das iX Kompakt beleuchtet aktuelle Security-Trends wie den Einsatz von KI zur Malware-Bekämpfung oder das grundschutzkonfome Arbeiten mit Containern. Es bildet die wichtigsten Aspekte eines ganzheitlichen IT-Sicherheitskonzeptes ab: Vom theoretischen "Stand der Technik" in der IT-Sicherheit über Praxistipps und nützliche Werkzeuge bis hin zu regulatorischen Vorgaben und "Härtetests" für Mensch und System in Form von Red Team Assessments. Das Heft ist eine Zusammenstellung der relevantesten Artikel aus iX – Magazin für professionelle IT. Alle Artikel wurden aktualisiert und ggf. ergänzt.

Digitale Kommunikation Christoph Meinel 2009-06-12 Internet und World Wide Web

basieren auf dem Vermögen, Informationen und Medien jeder Art in digitalisierter Form über Nachrichtenkanäle zu transportieren und zu verbreiten. Die Autoren erläutern Grundlagen und geschichtliche Hintergründe der digitalen Kommunikation und geben einen Überblick über Methoden und Verfahren der Kodierung von Text-, Audio-, Grafik- und Videoinformation, die im Internet zur Anwendung kommen. Zahlreiche Abbildungen sowie Sachindex, Personenindex und Glossar zu jedem Kapitel erhöhen den praktischen Nutzen dieses Handbuchs.