Sistemi Di Cifratura Storia Principi Algoritmi E Tecniche Di Crittografia

La realtà della parola è la realtà intellettuale. Non è la realtà demoniaca sospettata dalla demonologia.
Lo scopo di questo libro è quello di presentare i fondamenti della comunicazione segreta in modo conciso e semplice. La prima sezione ha lo scopo di correggere l'impressione che la crittografia sia una sorta di scienza occulta o che la crittoanalisi sia un gioco. Nei capitoli successivi vengono presentati i principi fondamentali della trasposizione e della sostituzione dei cifrari, con il resoconto dettagliato delle loro più importanti ramificazioni. La sezione sulla rottura dei cifrari porta direttamente ai problemi, che danno al lettore non solo un'applicazione pratica del suo studio, ma anche l'opportunità di valutare la sua abilità. Nota: gli esempi e gli esercizi sono dati per lo più in lingua inglese, essendo la più diffusa e utilizzata tra le lingue occidentali.
Fin dall'antichità si sono ideati metodi sempre più sicuri per occultare il reale significato di determinati segni e rendere un messaggio offuscato, in modo che non sia comprensibile a persone non autorizzate a leggerlo. Obiettivo di questo volume è presentare il linguaggio della crittografia moderna e dei vari aspetti collegati. Dopo un'introduzione storica che consente di acquisire dimestichezza con la terminologia e i problemi della disciplina, il testo tratta alcuni sistemi crittografici simmetrici (DES, AES) e asimmetrici. In particolare sono descritti gli algoritmi necessari per comprendere e implementare i crittosistemi e alcuni dei protocolli crittografici oggi più utilizzati. Vengono inoltre illustrati gli aspetti fondamentali della crittografia probabilistica. La completezza della trattazione che illustra tutti gli aspetti coinvolti (storia, matematica, algoritmi, applicazioni, complessità computazionale) rende questo volume adatto non solo agli studenti universitari di Informatica, Matematica e Ingegneria informatica, ma anche a chiunque sia interessato a conoscere il linguaggio della crittografia moderna. L'intero testo è integrato da numerosi esempi, diagrammi e figure, mentre materiali di complemento, tra cui diversi esempi "pratici" (svolti utilizzando il software Pari/Gp) sono disponibili online all'indirizzo www.hoeplieditore.it/66902.
Se volessimo trovare un esempio concreto di autentica vita vissuta all’insegna dell’art pour l’art, motto dei simbolisti e decadentisti del XIX secolo, Turing sarebbe indubbiamente un caso paradigmatico che avrebbe affascinato anche il più scettico dei poeti. Figlio di un’epoca in cui il futuro stava rapidamente trasformandosi in presente, Alan Turing è stato non solo parte integrante della grande rivoluzione scientifica che ha caratterizzato buona parte del XX secolo, ma è stato egli stesso quel “futuro” che avrebbe ridisegnato completamente i contorni del pensare e del vivere umano, elevando quel servo stupido che è la macchina ad un più alto gradino dell’essere, profetizzando un giorno in cui la macchina si sarebbe amalgamata con la vita umana emulandola in ogni suo aspetto. Dalla risoluzione dell’Entscheidungsproblem al gioco dell’imitazione, Turing ha riscritto le sorti del sapere e dell’agire umano preludendo a qualcosa che sarebbe andata insinuandosi sempre di più in ogni anfratto della nostra esistenza: l’informatica.
Un’affascinante e documentata storia dei servizi segreti dai faraoni alla Cia, passando per Napoleone, l’Unione sovietica e le due Germanie. L’autore, anche grazie a contatti personali con agenti segreti e rappresentanti diplomatici, ci permette di gettare uno sguardo nel funzionamento di uno strumento ambiguo e pericoloso, sempre in bilico tra esigenze di sicurezza, violazione dei diritti umani e manipolazione dell’opinione pubblica.
Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografiaMaggioli EditoreL'officina del meccanico quantistico. Dal gatto di Schröedinger al quantum computingMaggioli EditoreCrittografia analogica. L'uso nella pratica dall'antica Grecia all'avvento del digitale.Mario Canton
Durante la II guerra mondiale hanno avuto luogo numerosi risultati di rilievo nel campo della crittografia militare. Uno dei meno conosciuti è quello usato dal servizio di intelligence svedese, nei confronti del codice tedesco per le comunicazioni strategiche con i comandi dei paesi occupati nel nord Europa, le cui linee passavano per la Svezia. In tal modo, durante la fase più critica della guerra la direzione politica e militare svedese era in grado di seguire i piani e le disposizioni dei Tedeschi, venendo a conoscenza dei più arditi progetti per modificare la propria politica, tenendo la Svezia fuori dalla guerra. La violazione del codice tedesco è narrata in dettaglio, per la prima volta, con elementi che gli permettono di essere un’ottima introduzione al campo della crittografia, oltre che un ritratto vitale e umano della società del tempo: una disperata condizione bellica, l'intrigo politico e spionistico, il genio del matematico Arne Beurling, le difficoltà e i trucchi del mestiere, e il lavoro sistematico e oscuro di una folla di decrittatori.
La Seconda guerra mondiale si è combattuta anche su un fronte più nascosto, tra coloro che volevano rendere illeggibili al nemico i propri messaggi e coloro che cercavano in ogni modo di svelarli. La storia è rimasta segreta per quasi trent’anni dalla fine del conflitto e una grande mole di informazioni è stata resa disponibile soltanto negli anni '90 del Novecento grazie alle leggi sulla trasparenza entrate in vigore negli Stati Uniti e nel Regno Unito, i Freedom of Information Act. I crittologi non furono alle prese solo con Enigma, la macchina cifrante tedesca, che Alan Turing contribuì a decriptare. La storia è costellata di sconfitte e trionfi, dei contributi di decine di menti geniali e del duro lavoro di un esercito di collaboratori, in gran parte donne. L’uso estensivo di macchine per cifrare e per decifrare è stato uno degli elementi decisivi per la nascita dell’informatica moderna.
The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts. Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field. After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography. An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography Shows you how to build cryptography into products from the start Examines updates and changes to cryptography Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more Cryptography Engineering gets you up to speed in the ever-evolving field of cryptography.
La storia dell'informatica a partire dai primi passi compiuti dall'uomo nel campo della matematica e del calcolo assistito, per arrivare a Internet e ai supercalcolatori; un cammino lungo il quale si incontrano personaggi animati da passione e voglia di conoscenza, uomini che hanno saputo produrre invenzioni geniali o creare aziende oggi conosciute a livello mondiale. Un libro attraverso cui ogni lettore potrà soddisfare innumerevoli curiosità e nel quale l'esperto e l'appassionato troveranno notizie e approfondimenti su argomenti poco trattati dalla stampa specializzata, con uno sguardo approfondito sulla storia dell'informatica italiana corredato dai documenti e dalle immagini fotografiche dell'archivio storico di IBM Italia.