Sistemi Di Cifratura Storia Principi Algoritmi E Tecniche Di Crittografia

Negli ultimi decenni il rapido sviluppo delle tecnologie IT ha influito in maniera determinante nella vita dell'uomo, trasformando, spesso inconsapevolmente il suo lavoro, le sue abitudini, il suo modo di interagire con il mondo che lo circonda. Il fenomeno della "globalizzazione" dei mercati è solo una delle trasformazioni che l'intero pianeta sta attraversando. Anche se i vantaggi derivanti dall'utilizzo delle moderne tecnologie di comunicazione ci facilitano nel lavoro e nella attività ludiche e personali, molte sono le perplessità e i dubbi che attanagliano tutti coloro che le utilizzano. Se l'Information Technology rappresenta il "combustibile" indispensabile per la sopravvivenza delle aziende e delle attività dell'uomo, nel contempo può generare problematicità di grande rilievo. Il testo tratta alcune delle problematiche che destano preoccupazioni rilevanti nel mondo intero come il consumo energetico dei sistemi informatici (incontrollabili e inquinanti), il problema della garanzia della privacy e dell'integrità dei dati su Internet, l'utilizzo della rete Internet come strumento di controllo delle masse, la possibile sparizione degli attuali sistemi operativi che potranno essere sostituiti dal sistema operativo Web Operating System.
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.
Il futuro dell'Information & Communication Technology
I principi fondamentali della antropologia criminale
Intelligence e Sicurezza del Cyberspazio
Bibliografia nazionale italiana
Dai Faraoni alla CIA
Reti di calcolatori e Internet. Un approccio top-down

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.

La realtà della parola è la realtà intellettuale. Non è la realtà demoniaca sospettata dalla demonologia.

dall'abaco all'intelligenza artificiale

Storia universale della musica

1: L'arte dell'evo antico

guida per i giudizi medico-forensi nelle questioni di imputabilità

Monografie

Introduzione alla crittografia. Algoritmi, protocolli, sicurezza informatica

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.

Nell'ambito della continua evoluzione dell'intelligence e del cyberspazio, in un mondo sempre più globalizzato, il libro analizza come il sistema Paese stia riconfigurando la propria postura e il proprio profilo di sicurezza per contrastare le nuove criticità e garantire competitività. In questo contesto, l'intelligence diventa cruciale, modellando i campi di azione alle sempre più variabili e molteplici esigenze del mercato globale. La sua applicazione anche nel settore economico ne costituisce un baluardo a difesa della politica produttiva e commerciale del Paese. Il contrasto alle minacce cyber rappresenta una delle sfide più impegnative di questo secolo, nella quale sono in palio lo sviluppo e la sicurezza della Nazione. La piena sinergia tra Pubblico e Privato è tuttavia l'unico strumento in grado di garantire al sistema Paese una cornice di sicurezza omogenea ed efficace, che consenta alle nostre imprese di operare al meglio nel mercato sia nazionale sia internazionale. Il cyberspazio è e sarà l'Heartland del paradigma mackinderiano, il cui controllo condizionerà l'egemonia di una potenza sulle altre.

Guglielmo Marconi
genio, storia e modernità

Informatica giuridica

I servizi segreti di Venezia. Spionaggio e controspionaggio ai tempi della Serenissima

L'orecchio di Dio. Anatomia e storia della National Security Agency

Codici cifrati

Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografiaMaggioli EditoreIntelligence e Sicurezza del CyberspazioYoucanprint

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.

Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografia

Non solo enigma
Genesi e apologia di un genio matematico
Archivio storico lombardo
Bullettino senese di storia patria

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. 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.

La posta elettronica. Tecnica & best practice
La grande storia del computer
Storia dei servizi segreti
Prontuario per la cubatura dei legnami, rotondi e squadrati, secondo il sistema metrico decimale
Come difendersi dalla violazione dei dati su internet. Diritti e responsabilità
La divulgazione musicale in Italia oggi

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.

Il commercio elettronico. Dall'immagine al profitto
Corso elementare di storia dell'arte
Traduzione italiana del Enrico Bongioanni
Teoria, algoritmi e protocolli
Statistica
Storie delle guerre nascoste