

Sistemi Di Cifratura Storia, Principi, Algoritmi E Tecniche Di Crittografia

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.

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.

Working Conference of the Ifip Wg 10.3, April 25-29, 1994

atti del Convegno di studi sui ceti dirigenti nelle istituzioni della Repubblica di Genova ...

Storia della Guardia di finanza

La storia dei genovesi

Codici cifrati

Storia della scienza

La varietà e l'interesse dei contributi alla Lettera Matematica Pristem hanno spinto i curatori, d'accordo con il comitato di redazione, a proporre in questa raccolta alcuni articoli apparsi sulla rivista dalla sua fondazione ad oggi. atica Pristem è una rivista, edita dalla Springer-Verlag Italia, che affronta temi legati alla ricerca matematica, ai fondamenti di questa disciplina, alla sua storia e alle sue applicazioni negli ambiti più vari. La sfida è quella di interessare e divertire il lettore, riuscendo allo stesso tempo a convincerlo che la matematica, di solito ritenuta affare di pochi iniziati, lontana dagli interessi della gente comune, arido esercizio di astrusi calcoli, è invece fondamentale nella nostra vita quotidiana, ed è davvero dappertutto attorno a noi: nelle carte di credito, nella posta elettronica, in internet, nell'arte, nei giochi, nelle scelte (anche di tipo etico) che facciamo in situazioni conflittuali, e perfino in politica.

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.

L'enigma dei numeri primi. L'ipotesi di Riemann, il più grande mistero della matematica Guida alla net economy. Cosa conoscere e come prepararsi per entrare con successo nell'economia digitale

Storia universale della musica

Pittura su tavola dalle collezioni dei Civici musei di storia ed arte di Trieste, Comune di Trieste, Museo civico Sartorio, 18 gennaio-4 novembre 1975

i protagonisti e le macchine della storia dell'informatica

Information Warfare 2012. Armi cibernetiche e processo decisionale

Le applicazioni informatiche hanno assunto negli ultimi decenni un ruolo fondamentale in tutte le attività scientifiche e pratiche. È perciò per gli studenti, anche quelli di materie umanistiche, oltre ad avere una conoscenza di base di Informatica, acquisiscano familiarità con applicazioni che possono utilizzare per i loro studi e ricerche e nella loro futura attività lavorativa.

Lineamenti di tecnologie dell'informazione e della comunicazione. Politiche italiane e dell'Unione europea nel campo dell'economia digitale Trasformazioni delle imprese, dei modelli di business e dei mercati attraverso le varie forme della net economy, del commercio elettronico business. Formazione e nuove professionalità del Web.

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

Teoria, algoritmi e protocolli

Bibliografia nazionale italiana

Storia delle telecomunicazioni

Dai Faraoni alla CIA

Sistemi alternativi di risoluzione delle controversie nella società dell'informazione

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 precludendo a qualcosa che sarebbe andata insinuandosi sempre di più in ogni anfratto della nostra esistenza: l'informatica.

Massively Parallel Systems (MPSs) with their scalable computation and storage space promises are becoming increasingly important for high-performance computing. The growing acceptance of MPSs in academia is clearly apparent. However, in industrial companies, their usage remains low. The programming of MPSs is still the big obstacle, and solving this software problem is sometimes referred to as one of the most challenging tasks of the 1990's. The 1994 working conference on "Programming Environments for Massively Parallel Systems" was the latest event of the working group WG 10.3 of the International Federation for Information Processing (IFIP) in this field. It succeeded the 1992 conference in Edinburgh on "Programming Environments for Parallel Computing." The research and development work discussed at the conference addresses the entire spectrum of software problems including virtual machines which are less cumbersome to program; more convenient programming models; advanced programming languages, and especially more sophisticated programming tools; but also algorithms and applications.

Storia dei trattati e politica internazionale

Quaderni del Bobbio n. 4 anno 2012-2013

Matematica

La matematica ovunque

Programming Environments for Massively Parallel Distributed Systems

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.

Nove storie vere – tra hacking di Stato, spionaggio, ricercatori a caccia di software malevoli, gruppi parastatali o schiettamente criminali, persone comuni e inconsapevoli coinvolte – che ci raccontano come la Rete si stia trasformando in un vero e proprio campo di battaglia. La fotografia densa di un presente inquietante e contraddittorio che potrebbe trasformarsi a breve in un futuro distopico. Dai retroscena sulla prima 'arma digitale' usata da hacker al soldo dei governi per sabotare un impianto industriale ai ricercatori di cyber-sicurezza finiti al centro di intrighi internazionali degni di James Bond; dai virus informatici usati per le estorsioni di massa fino al mercato sotterraneo dei dati personali degli utenti. Guerre di Rete racconta come Internet stia diventando sempre di più un luogo nel quale governi, agenzie, broker di attacchi informatici e cyber-criminali ora si contrappongono, ora si rimescolano in uno sfuggente gioco delle parti. A farne le spese sono soprattutto gli utenti normali – anche quelli che dicono «non ho nulla da nascondere» –, carne da cannone di un crescente scenario di (in)sicurezza informatica dove ai primi virus artigianali si sono sostituite articolate filiere cyber-criminali in continua ricerca di modelli di business e vittime da spolpare. In questo contesto emergono costantemente nuove domande. La crittografia è davvero un problema per l'antiterrorismo? Quali sono le frontiere della sorveglianza statale? Esiste davvero una contrapposizione tra privacy e sicurezza? Carola Frediani scava in alcune delle storie più significative di questo mondo nascosto, intervistando ricercatori, attivisti, hacker, cyber-criminali, incontrandoli nei loro raduni fisici e nelle loro chat.

Arne Beurling e la crittografia nella II guerra mondiale

L'enigma di Turing

Un mondo di idee

L'officina del meccanico quantistico. Dal gatto di Schrödinger al quantum computing

L'altra Resistenza. Servizi segreti, partigiani e guerra di liberazione nel racconto di un protagonista

Storie di Posta n. 12

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. Con la matematica abbiamo avuto tutti quanti a che fare, se non altro per averla studiata fin dai primi anni di scuola. Che la si sia amata o meno, con la matematica abbiamo tutti a che fare nella vita di tutti i giorni. Ma che cos'è la matematica? Quanto teoria e quanto pratica, nel suo costruire modelli per spiegare la realtà? Guerraggio ci conduce per mano alla scoperta del fascino di una disciplina che tutt'altro che un arido sistema di calcoli, intrecciata forse più di ogni altra alla storia del pensiero e allo sviluppo di arti e mestieri. L'autore parte dal presupposto che il matematico risolve problemi, suoi o di altri, tuttavia per venirne a capo, deve essere sufficientemente curioso e sensibile a diverse tematiche, le deve tradurre in uno dei dialetti che compongono la lingua matematica, deve saper inventare una nuova Matematica qualora quella conosciuta non sia sufficiente e ugualmente conoscere gli strumenti di calcolo ed essere in grado di ritradurre in termini reali quanto ottenuto.

Guerre di Rete

Manuale di crittografia

Sul senso della storia

Storia dei servizi segreti

Da @ a Zorch. Storia, parole, date, luoghi e protagonisti del Web che i manager devono conoscere

Armi cibernetiche e processo decisionale

La rivista da collezione! Edita da UNIFICATO in collaborazione con l'Accademia Italiana di Filatelia e Storia Postale.

Contributi per la Storia della Resistenza in Liguria

File sharing. Trovare, scaricare e condividere i file in Internet

Intelligence e Sicurezza del Cyberspazio

Storia dei trattati e politica internazionale: Parte generale. Introduzione al lo studio della "storia dei trattati e politica internazionale." Le fonti documentarie e memorialistiche

Accesso non autorizzato

Archivi per la storia