CRITTOGRAFIA

Book Series

3

100 tesi di Crittografia e Codici in Italia
2008–2017

a cura di
Daniele Bartoli
Nadir Murru
Francesco Pavese
Massimiliano Sala

Prefazione di
Michele Elia
Massimiliano Sala

Contributi di

Francesco Abbruzzese, Andrea Agnesse, Francesco Aldà, Alessandro Amadori, Federica Baiocchi
Marco Baldi, Daniele Bartoli, Paolo Bartolucci, Massimo Battaglioni, Alberto Bedodi
Emanuele Bellini, Silvia Berlanda, Margherita Bertè, David Bertoldi, Valeria Bodrone
Matteo Bonini, Domenica Borra, Cecilia Boschini, Giulia Bossi, Cecilia Bracuto
Alessandro Budroni, Marco Calderini, Cristina Califano, Simon Calimani, Gianluca Caparra
Wiliam Capraro, Marco Carolla, Luca Casati, Silvia Ceccato, Emanuele Cesena
Michele Ciampi, Pierpaolo Colagè, Chiara Della Corte, Micaela De Santis, Francesco Devito
Laura Donizetti, Michele Elia, Mohamad El laz, Stefania Fanali, Edoardo Fasano
Maria Angela Federici, Sebastiano Ferraris, Emanuela Franzè, Daniele Friolo, Andrea Frisoni
Giacomo Giuliari, Massimo Giulietti, Federico Carlo Gorla, Francesco Gozzini, Riccardo Grimi
Stefano Guarino, Andrea Guidolin, Gábor Korchmáros, Valentino Lanzone, Stefania Lippiello
Riccardo Longo, Mario Mancusi, Rita Manzo, Giulia Maragnani, Valeria Marelli
Luca Mariot, Annalisa Marrone, Marco Martinoli, Pasqua Valentina Mauri, Silvia Mella
Ferdinando Montecuollo, Rocco Mora, Nadir Murru, Luca Nizzardo, Ginetta Paladino
Luca Palmulli, Filomena Panico, Francesco Pavese, Francesco Peverini, Daniel Pinter
Pierpaolo Polo, Lorenzo Principi, Orazio Puglisi, Gabriele Pulvano, Rosanna Reibaldi
Francesco Renna, Paolo Riccardi, Giacomo Ricciutelli, Francesco Romeo, Beatrice Rossi
Matteo Sabbatini Peverieri, Massimiliano Sala, Giordano Santilli, Paolo Santini, Maurizia Saraullo
Alessandra Scafuro, Daniele Sciarroni, Davide Schipani, Linda Senigagliesi, Simona Silvestri
Luisa Siniscalchi, Chiara Spadafora, Christopher Spennato, Marco Timpanella
Salvatore Andrea Tinnirello, Barbara Usai, Stefania Vanzetti, Marco Vargiu, Daniele Venturi
Irene Villa, Andrea Visconti, Ivan Visconti, Stéphanie Vuillermoz
Andres Yesid Diaz Pinto, Ferdinando Zullo

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-2752-0

I edizione: gennaio 2020

Indice

Parte III
Tesi di dottorato

Parte IV
Tesi di laurea

Parte I

INTRODUZIONE

100 tesi di Crittografia e Codici in Italia 2008-2017
ISBN 978-88-255-2752-0
DOI 10.4399/97888255275201
pag. 17–18 (gennaio 2020)

Presentazione

Michele Elia, Massimiliano Sala

La rivoluzione culturale e cognitiva nata dall'invenzione di Johannes Gensfleisch zum Gutenberg della stampa a caratteri mobili parse immediatamente ai contemporanei come una meraviglia inaspettata e irripetibile. Non potevano certamente immaginare che la rivoluzione era appena iniziata e che secoli dopo ci saremmo trovati in un mondo dominato da nuove e straordinarie forme di scritture.

In Internet e nel World Wide Web, i messaggi sono della natura più disparata, dal tradizionale testo scritto ai brani musicali, dalla voce alle immagini, da operazioni più astratte quali autorizzazioni e attività notarili, al riconoscimento di persone o al controllo di oggetti volanti. Non è esagerato affermare che l'evoluzione tecnologica verso il digitale dei sistemi di comunicazione e dei calcolatori negli ultimi due secoli ha esteso il significato che si può attribuire ai termini "scrittura" e "messaggio".

La segretezza di qualsiasi tipo di messaggio è diventata una caratteristica indispensabile, anzi vitale, in un mondo globalmente connesso sia elettronicamente, sia per mobilità di persone. Le millenarie tecniche di protezione dei dispacci militari e diplomatici sono così entrate in modo pervasivo nel quotidiano di ogni attività sociale, industriale ed economica. La "parola magica" è crittografia, la cui definizione classica, di arte delle scritture segrete, è molto più propriamente diventata l'arte per la protezione dei messaggi. Abbiamo allora assistito al singolare fenomeno di come tale arte, nel passaggio dalle corti alle genti comuni, sia diventata una disciplina scientifica. In questo scenario, sono richiesti algoritmi sempre più astratti, e l'invenzione di paradigmi per impredicibili applicazioni.

Questa situazione mondiale coinvolge senza eccezioni anche il nostro paese Italia. Con la speranza di far cosa utile alla comunità nazionale scientifica e di governo, ha preso corpo, nella comunità De Componendis Cyfris, il progetto di raccogliere i sommari di 100 tesi (Laurea, Laurea Magistrale e Dottorato) sulla crittografia prodotte negli ultimi dieci anni nelle università italiane. Il duplice scopo è stato sia ottenere in modo indiretto un censimento, se pur parziale, di

quanti hanno lavorato e ancora si occupano di crittografia, sia fornire un quadro degli interessi, competenze e stato dell'arte crittografica nell'accademia e indirettamente, nell'industria italiana.

I tre giovani curatori del libro hanno svolto un lavoro egregio, avvicinando relatori e tesisti, estraendo dalle tesi le bibliografie, raccolte poi in una sintesi posta al termine del volume, e accompagnando ogni sommario di tesi, scritto dall'autore, con una sua succinta biografia che include anche il cammino lavorativo o di carriera dopo la laurea.

Inoltre sono rimarchevoli cinque capitoli, posti a preambolo dei sommari di tesi, scritti da esperti del settore che illustrano i principali argomenti trattati e che si presentano come una panoramica succinta, ma non banale, dello stato dell'arte concernente la crittografia. Tali capitoli sono La Tecnologia Blockchain e le Cryptocurrency di Ivan Visconti, Crittografia Asimmetrica: Un Viaggio a Cavallo tra Minicritto e Crittomania di Daniele Venturi, Block Cipher di Andrea Visconti, Codici di Marco Baldi e Massimo Giulietti, Elliptic Curve Cryptography di Gabor Korchmaros e Massimo Giulietti. Come si evince dai titoli, sono coperti gli aspetti principali sia della crittografia classica, sia della relazione tra crittografia e codici, sia dell'uso della crittografia contemporanea.

I professori Daniele Bartoli, Nadir Murru e Francesco Pavese hanno curato un'opera che ha ampiamente superato le aspettative del progetto iniziale. Ne emergono un quadro confortante sullo status della crittografia in Italia, una miriade di spunti di ricerca, nonché un'indicazione degli sviluppi futuri.

100 tesi di Crittografia e Codici in Italia 2008-2017
ISBN 978-88-255-2752-0
DOI 10.4399/97888255275202
pag. 19–31 (gennaio 2020)

Introduzione alla crittografia con cenni storici

Daniele Bartoli, Nadir Murru, Francesco Pavese

Fin dall'antichità uno dei maggiori problemi, fondamentale almeno quanto quello di conservare mediante la scrittura informazioni importanti, è consistito nell'evitare l'accesso a dati sensibili da parte di soggetti non autorizzati. In innumerevoli situazioni la segretezza con la quale messaggi di una certa rilevanza dovevano raggiungere il destinatario o i destinatari senza poter essere comprese da qualsiasi altro agente è stata di fondamentale importanza ed ha determinato la vittoria o la sconfitta in guerre e battaglie, la vita e la morte di molte persone, la riuscita o meno di rivoluzioni.

La parola "crittografia" deriva dall'unione di due parole greche: "kryptós" che significa nascosto, e "gráphein" che significa scrivere. Con il termine crittografia quindi si intende un insieme di tecniche e algoritmi che consentono di trasformare un messaggio in modo da renderlo comprensibile solamente alle persone che sono a conoscenza del metodo tramite cui si è codificato il messaggio stesso.

I primi esempi a noi noti dell'utilizzo di una modalità per modificare il significato di un messaggio risalgono addirittura all'antico Egitto durante il periodo dell'Antico Regno. Sono stati infatti rinvenuti alcuni geroglifici, scolpiti sopra antichi monumenti, non standard o parzialmente riprodotti. Rimane il mistero se tali modifiche avessero lo scopo di occultare una qualche informazione oppure appartenessero più in generale ad un particolare culto misterico.

Secondo gli storici, anche i Babilonesi avrebbero potuto utilizzare un'arcaico sistema crittografico: sono state rinvenute tavolette risalenti al 2500 a.C. nelle quali manca la prima consonante delle parole e si ipotizza che ciò sia stato fatto per proteggere un possibile segreto industriale relativo alla produzione di ceramica vetrificata.

Chiaramente l'utilizzo della crittografia viaggia di pari passo con il diffondersi della scrittura e assume nel corso dei secoli forme via via più complicate. Si assiste quindi ad una corsa alla sicurezza che vede opposti chi vuole conservare e diffondere una certa informazione e chi invece cerca in tutti modo di venire a conoscenza di tale segreto. Questa lotta antitetica si avvale chiaramente dei più moderni

ritrovati tecnologici di ogni epoca: l'uomo ha chiaro fin dall'antichità il ruolo centrale di comunicazioni sicure e chi ha il controllo su di esse ha una posizione di vantaggio spesso decisiva sui concorrenti.

La crittografia non deve tuttavia essere confusa con la steganografia, il cui scopo è quello di nascondere l'intero messaggio a individui non autorizzati: la crittografia infatti non vuole celare il messaggio stesso ma il suo significato. Lo stesso Erodoto nelle sue "Storie" ci racconta ingegnosi esempi di steganografia. Uno di essi permise, secondo la tradizione, al re spartano Demarato, esiliato in Persia, di avvertire i suoi compatrioti del progetto di invasione ideato dal re persiano Serse: incise sul legno di una tavoletta il messaggio e poi ricoprì con della cera la tavoletta stessa, facendola apparire nuova. Una volta recapitata a Sparta, solo dopo molte riflessioni gli Spartani capirono di dover rimuovere la cera e poterono quindi leggere l'importante messaggio recapitatogli dal loro re. Un esempio più moderno di Steganografia è rappresentato dall'utilizzo di inchiostro invisibile, di solito succo di limone o linfa di piante, che una volta sottoposto ad un modesto calore diventa visibile, mostrando il messaggio celato. Come già accennato tutti questi esempi non costituiscono espedienti crittografici, ma hanno sicuramente rivestito una notevole importanza storica.

Considerando ancora il mondo greco, durante la guerra tra ateniesi e spartani per l'egemonia sul Peloponneso, un espediente utilizzato fornisce uno dei primi esempi della cosiddetta crittografia per trasposizione. Il messaggio iniziale (detto nel gergo moderno "messaggio in chiaro") veniva trasformato nel "messaggio cifrato" attraverso l'inserzione di simboli superflui. Tale messaggio cifrato veniva poi inviato al destinatario che doveva essere in grado di risalire al messaggio originale. L'operazione di cifratura (ovvero il passaggio da messaggio in chiaro a messaggio cifrato) e di decifratura (da messaggio cifrato a messaggio in chiaro) era resa possibile da particolari bastoni (detti scitali): i caratteri aggiunti infatti scomparivano una volta che il messaggio cifrato, scritto su di una lunga striscia di tela, veniva arrotolato su tale bastone. Di fondamentale importanza in questo processo è che, nonostante la tecnica utilizzata fosse conosciuta da tutti, solo la conoscenza esatta delle dimensioni del bastone utilizzato avrebbe potuto permettere la decodifica corretta del messaggio cifrato.