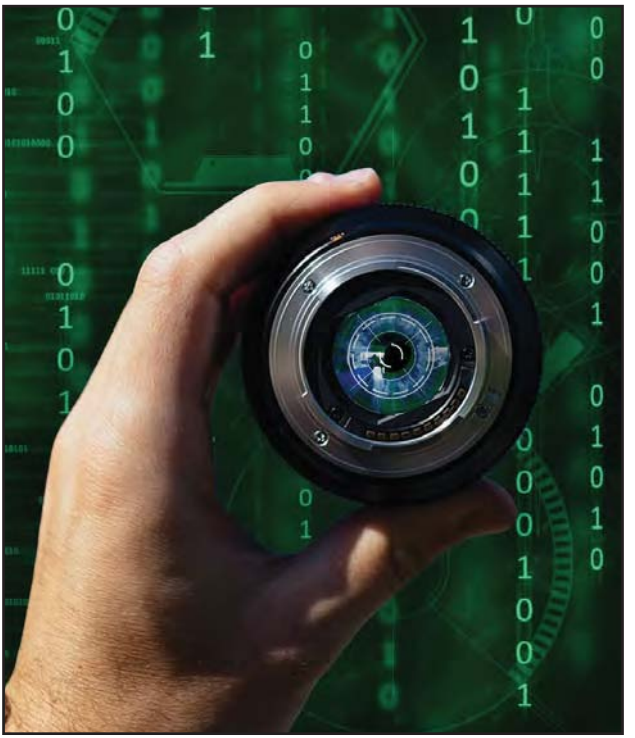
Stefano Leonesi

LA MATEMATICA DI JAMES BOND

Alla scoperta della crittografia

scienza FA



FrancoAngeli

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

scienza FA

Una collana di saggi per il lettore non specialista:
per comprendere la realtà che ci circonda

Stefano Leonesi

LA MATEMATICA DI JAMES BOND

Alla scoperta della crittografia

scienza FA

FrancoAngeli

Progetto grafico di copertina: Géraldine D'Alessandris

1a edizione.

Dedicato a Maddalena e Rodolfo

Indice

Parte 2
Crittografia e società

Ringraziamenti

Sono particolarmente riconoscente all'amico e curatore della collana Renato Betti per avermi proposto la stesura di questo testo, aver avuto la pazienza di leggerne versioni precedenti e fornito suggerimenti preziosi su come arricchirle.

Ringrazio la direzione e la redazione di *Lettera matematica Pristem* che ha ospitato quei miei articoli che sono poi divenuti l'embrione del libro.

Sono grato infine a Carlo Toffalori perché le collaborazioni che ho avuto il privilegio di condividere con lui in questi anni mi hanno consentito di affrontare nuove sfide e ulteriori traguardi.

Resta inteso che ogni errore o svista presenti nel libro sono imputabili esclusivamente a me.

San Severino Marche, 15 giugno 2018

Stefano Leonesi

Premessa per non matematici

Voglio rassicurare il lettore meno esperto in matematica esortandolo a non scoraggiarsi quando si imbatterà nelle parti più dense di formule. Il testo è stato infatti concepito per poterne seguire il filo logico anche senza avventurarsi in esse o decidendo di saltarle qualora risultassero troppo ostiche.

Tuttavia i noccioli matematicamente più duri del libro costituiscono una presenza necessaria e un atto dovuto a quei lettori più esperti che volessero approfondire le tematiche e godere appieno delle bellezze che riservano le sublimi arti della matematica e della crittografia.

Parte 1

Codici segreti e matematica

1
Gli scandali *WikiLeaks* e il misterioso file *insurance.aes256*

WikiLeaks e i suoi scoop sono oramai da diversi anni nell'occhio del ciclone perché capaci di provocare tra i maggiori scandali politici, militari, economici a livello planetario. Non pochi sono i governi che hanno tremato quando Assange e soci hanno diffuso informazioni riservate e compromettenti scoprendo i tanti vasi di Pandora in circolazione. Tutto ciò ha messo in crisi relazioni diplomatiche oramai collaudate e sconfessato pubblicamente le ipocrite dichiarazioni ufficiali di leader governativi e manager di multinazionali.

Tanto clamore non poteva che attirare l'ira di una nutrita schiera di governi e imprese, sbugiardati pubblicamente, che stanno facendo di tutto per far tacere Assange e la sua creatura, *WikiLeaks*. Dal pari loro, questi ultimi, il 30 luglio del 2010, ai tempi della guerra in Afghanistan, ritennero opportuno tutelarsi pubblicando e facendo circolare un corposo file criptato di 1,4 gigabyte, chiamato *insurance.aes256*, a mo' di assicurazione sulle loro vite: il nome stesso, "insurance", testimonia esplicitamente questo scopo. Assange in persona dichiarò che qualora fosse capitato qualcosa a lui o ai suoi collaboratori, sarebbero state rese immediatamente pubbliche le chiavi per decifrare il contenuto del documento, offrendolo alla vista del mondo intero. D'altra parte, nel nome *insurance.aes256* del file c'è anche un suffisso, "aes256", che ai più apparirà oscuro, ma che in realtà vuole anch'esso essere un manifesto rimando. Ma a cosa? Per giunta come può un file fungere da garanzia per la propria incolumità? E, nella pratica, come si può cifrare un messaggio e così ren-

derlo incomprensibile ai non autorizzati? O anche, come si costruiscono chiavi di codifica e decodifica? E che rapporto c'è tra di esse? Ebbene, le pagine che seguono ce lo sveleranno facendo emergere la centralità e l'importanza che la matematica riveste per tali questioni.

Ma intanto chiariamo che cosa sia effettivamente *WikiLeaks* e quali a grandi linee i fondamenti scientifici e tecnologici alla base del suo funzionamento. Apprendiamo direttamente dal suo sito ufficiale che *WikiLeaks* è un'organizzazione i cui fini sono di pubblicare senza autorizzazione e analizzare informazioni coperte da segreto o tenute celate, il tutto attraverso un normale sito con interfaccia simile a quella di *Wikipedia*. Il nome "WikiLeaks" discende appunto dalla fusione del termine "Wikipedia" e del verbo "to leak" che in inglese significa avere la capacità di far trapelare notizie permettendone la "fuga". L'intento dichiarato sarebbe quello di smascherare azioni di regimi oppressivi e svelare comportamenti non etici o addirittura illegali di governanti e aziende. Sta infatti nella trasparenza e nella possibilità di controllo e informazione da parte dei cittadini – si legge nel documento – la speranza di ridurre la corruzione, migliorare l'azione dei capi di Stato e rafforzare giustizia e democrazia – e non è certo difficile trovarsi in accordo con simili intenzioni. L'idea è che *WikiLeaks* diventi un forum dove l'intera comunità globale possa esaminare credibilità, plausibilità, veridicità del materiale pubblicato.

Nel corso della storia, l'informazione ha sempre dovuto pagare un prezzo salatissimo in termini di assassinii, intimidazioni e rappresaglie. Ma oggi – dichiara *WikiLeaks* – svelare notizie è divenuto più sicuro grazie a Internet e alla crittografia. In effetti, per dirla in breve, il nocciolo del sistema *WikiLeaks* è costituito da un "contenitore" virtuale in rete protetto da un potente sistema di cifratura in grado di accogliere documenti segreti preservando l'anonimato e l'irrintracciabilità degli informatori che vi inviano documenti.

Ebbene, questo testo intende svelare e divulgare – "to leak" appunto – i retroscena matematici e informatici che sono a fondamento della crittografia e che consentono di cifrare e decifrare messaggi segreti, garantire l'anonimato, firmare digitalmente un documento, ma anche assicurare che un impegno online venga mantenuto,

giocare a testa o croce al telefono, o creare banconote digitali, votare elettronicamente e compiere a distanza e con sicurezza tante altre stupefacenti quanto utili azioni di cui avremo modo di discutere passeggiando informalmente intorno a questi temi.

Quelli appena elencati sono argomenti che, se fino ad un po' di anni fa erano prerogativa di imperatori, capi di Stato, militari e spie alla James Bond, oggi, con lo sviluppo della tecnologia e delle opportunità telematiche, sono divenuti appannaggio irrinunciabile del cittadino comune, fosse anche per un innocente acquisto via Internet o per gestire il proprio conto in banca online.

Il linguaggio e il tono che vogliamo usare saranno per quanto possibile colloquiali e discorsivi, consapevoli che questo fatalmente potrà condurre talora a semplificazioni o imprecisioni, delle quali ci scusiamo sin d'ora con i gentili lettori.