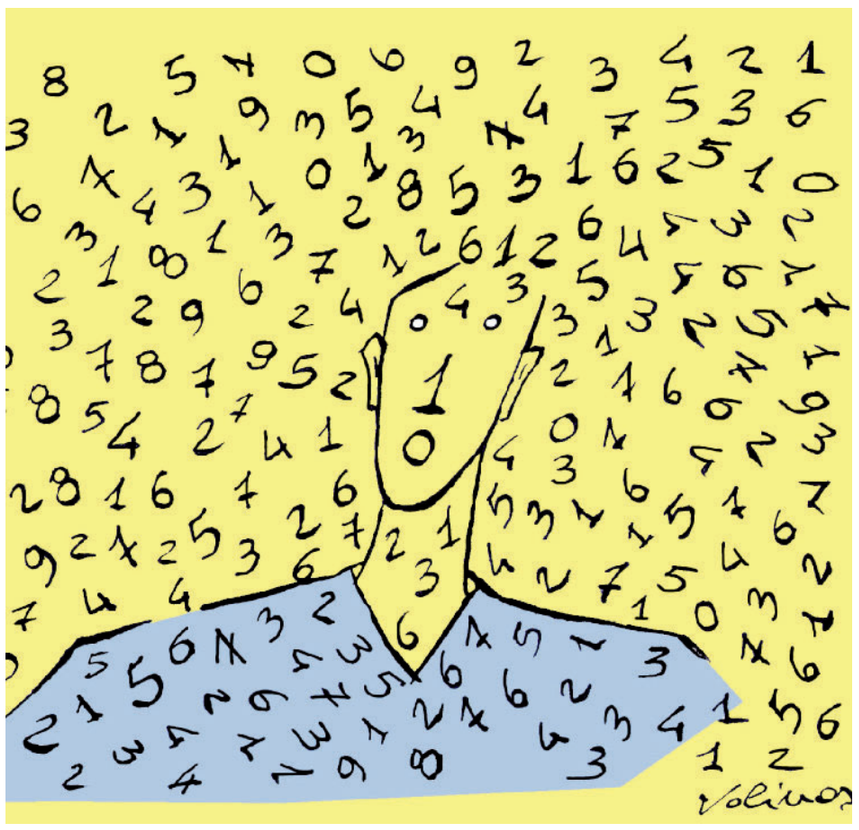
Tecnologia

Il problema è antico, però oggi la sicurezza della trasmissione di dati sensibili non è più appannaggio esclusivo degli ambienti diplomatici e militari, ma fa parte della quotidianità di tutti

CRITTOGRAFIA

Una vita in codice tra banche e social

Silvia Camisasca



Accade ormai frequentemente che organi di stampa, e non solo, si debbano occupare di aspetti tecnologici legati alla sicurezza di trasmissione di dati sensibili, quali, banalmente, i codici bancari delle transazioni elettroniche. Il problema della trasmissione sicura delle informazioni è, però, antico quanto la storia dell'Umanità, come suggerisce l'origine stessa del nome della disciplina – crittografia deriva, infatti, dalla fusione dei vocaboli greci *kryptos* (nascosto) e *graphein* (scrittura) – che si occupa di studiare i metodi necessari per trasmettere informazioni tra due persone – o enti – in maniera da non consentire a terzi di accedervi. L'elemento di novità rispetto al passato, caratterizzante della nostra epoca, è piuttosto l'enorme rilevanza sociale assunta dalla crittografia, non più appannaggio esclusivo di ambienti diplomatici e militari – e, quindi, accessibile solo alle classi più abbienti e istruite – ma strumento alla portata di tutti, come avviene in una società "digitalizzata" che costantemente ricorre a codici crittografici (pagamenti, comunicazioni, social network, computer) con ripercussioni sulla vita quotidiana. Ciò richiederebbe una maggiore consapevolezza del suo uso da parte degli utenti, anche se non è semplicissimo, perché le attuali applicazioni sono conseguenti alla scoperta – circa a metà degli anni '70 – dei cosiddetti crittosistemi a chiave pubblica, i cui punti di forza e debolezze implicano la conoscenza della Teoria Computazionale dei Numeri, ovvero degli oggetti matematici coinvolti a monte.

Fino al 1978, i metodi crittografici erano a chiave privata, ossia la coppia di chiavi di cifratura e decifratura – parametro di codifica, che permette di passare dal messaggio scritto in modo intelligibile e chiaro al testo codificato, e di decodifica (procedimento inverso) – era nota esclusivamente alla coppia di utenti in comunicazione tra loro: era, dunque, essenziale al funzionamento del crittosistema che tali chiavi non fossero note a terzi.

Ne sono esempi celebri il metodo di Cesare, il disco cifrante di Leon Battista Alberti ed Enigma, la macchina della Seconda Guerra Mondiale, la cui violazione da parte dell'inglese Turing è ben più nota al pubblico del fatto che i primi ad identificarne alcune sue debolezze furono, negli anni '30, tre matematici dell'Ufficio Cifra dello stato maggiore dell'esercito polacco. Il limite maggiore del metodo a chiave privata – detto problema di distribuzione delle chiavi – è dato dal fatto che i due utenti, prima di iniziare la comunicazione, devono accordarsi per scambiare la coppia di chiavi codifica/decodifica necessaria per comprendersi: è evidente che ciò impedisce la costruzione di un ampio network di persone in grado di accedere a tali sistemi; si pensi, ad esempio, al grado di organizzazione richiesto negli apparati militari. Inoltre, la necessità di una coppia di chiavi segreta per ogni coppia di utenti, produce un numero di combinazioni tale, per cui, dati N utenti, avremo almeno N(N-1)/2 coppie di chiavi. Questo mette fuori gioco i crittosistemi a chiave privata negli ampi network oggi esistenti.

Nel metodo a chiave pubblica, realizzato per la prima volta nel '78, la chiave di codifica di ogni utente deve essere necessariamente a disposizione di ogni altro utente, semplicemente consultando un elenco, o un archivio, di chiavi pubbliche degli utenti. Ovviamente, anche qui, la chiave di decodifica va mantenuta segreta, in modo che solo il destinatario del messaggio possa rimuovere l'offuscamento della codifica e risalire al testo in chiaro: un intruso che tenti di violare il sistema può utilizzare la chiave di codifica pubblica di un certo utente per risalire a quella di decodifica, ma per farlo dovrebbe essere in grado di risolvere un problema matematico computazionalmente difficile, ovvero, per definizione, proibitivo, allo stato delle conoscenze attuali, per i calcoli richiesti alla risoluzione. Se i presupposti teorici della validità della costruzione di chiavi codifica/decodifica del crittosistema Rsa – dalle iniziali degli autori – risalgono addirittura all'epoca compresa tra il 1600 e il 1780, grazie agli studi di Fermat ed Eulero, che i calcoli previsti in Rsa siano eseguibili in tempi ragionevoli è stato verificato, invece, solo nel 2002, con la dimostrazione che la ricerca dei 2 numeri primi distinti "grandi", richiesta dal metodo, costituisce, in realtà, un problema computazionale semplice. Inoltre la sua realizzabilità pratica è garantita dall'attuale capacità degli strumenti di calcolo disponibili al pubblico di generare, in pochi secondi, due numeri primi distinti dell'ordine di grandezza di 300 cifre in base 10 ognuno. La soglia di sicurezza di Rsa, estremamente alta, è legata alla capacità di determinare i fattori di numeri interi grandi aventi almeno 600 cifre in base 10: un problema che, con gli attuali metodi di calcolo, richiederebbe, al contrario, migliaia di anni. Basti pensare che a oggi il record per interi di tale tipologia è di 220 cifre in base 10! Dai tempi del metodo Rsa, le scoperte matematiche – in ambito teorico e astratto – applicate alla crittografia hanno completamente rivoluzionato la disciplina, consentendo l'affermarsi di quegli strumenti ad oggi, quasi inconsapevolmente, quotidiani e familiari: senza di esse, ad esempio, non esisterebbe il commercio elettronico o la firma digitale. Anche se al momento pare necessario ancora molto lavoro per rendere obsoleto Rsa, si sta anche lavorando alla costruzione di sistemi alternativi, a seguito della dimostrazione di un nuovo metodo di calcolo quantistico – per ora solo teorico – in grado di decodificare – in tempi ragionevoli – le chiavi Rsa.

> Estremamente delicati sono i casi legati al corretto funzionamento dei sistemi democratici come il voto elettronico: la dematerializzazione rende molto più difficile la verifica degli errori

Premesso che l'unico modo per mantenere segreta un'informazione è non comunicarla ad alcuno, il fatto che i metodi crittografici vengano continuamente esaminati e messi in discussione – in cerca di loro vulnerabilità – va inquadrato nell'ambito del "metodo scientifico", per cui ogni verità è valida solamente all'interno di un ben preciso ambito di assunzioni e regole – una teoria – che costituiscano un modello del mondo reale: modello criticabile con l'introduzione di novità sperimentali o teoriche, in presenza delle quali risulta compromessa la corrispondenza con qualche specifico aspetto del mondo reale. Da qui i rischi legati a un uso acritico della crittografia, proprio perché il suo impatto sociale è sempre maggiore. Estremamente delicati sono i casi legati al corretto funzionamento dei sistemi democratici, quali l'utilizzo del voto elettronico, valutando attentamente che la dematerializzazione del supporto, su cui si esprime il voto (in forma di una sequenza di bit), rende molto più complessa la verifica – a posteriori – di eventuali brogli o errori.

LIBRI E FILM

IL VIAGGIO DI VERNE E LO SCARABEO DI POE

Un testo cifrato in caratteri runici viene ritrovato in un vecchio libro: decodificato, si scopre indicare come raggiungere il centro della terra…e l'avventura comincia! È proprio da un messaggio in codice che Jules Verne parte per il *Viaggio al centro della Terra*. Nella storia della letteratura e del cinema Verne è in buona compagnia. «Ciò che un uomo può inventare, un altro può scoprire», fa dire Conan Doyle (*L'avventura degli omini danzanti*) a Sherlock Holmes che, decifrando un crittogramma, risolve un omicidio. Con la spy-story *Enigma*, Robert Harris si sposta su una vicenda di spionaggio della seconda guerra mondiale, anche se – per contenuto crittografico – è Edgar Allan Poe con *Lo scarabeo d'oro* a fornire il caso letterario più interessante: passo per passo è descritto come applicare l'analisi di frequenza delle lettere di una data lingua per decodificare un testo cifrato, che conduce al tesoro! Un elemento, però, è del tutto inverosimile: la mancanza dei "vicoli ciechi", degli errori –inevitabili – nei tentativi di risoluzione del crittogramma. Ipersfruttata nel cinema – visto che ormai è inserita in ogni film di spionaggio o azione – la crittografia è qui trattata, per lo più secondo stereotipi, con esperti in materia descritti come disadattati sociali o dotati di poteri "semidivinatori" (*Codice Mercury*) o, ancora, supponendo tecnologie capaci di violare tutti i sistemi crittati (*I signori della truffa*). Poche pellicole hanno saputo andare oltre, tra cui – recentemente – *The Imitation Game*, e la trasposizione del romanzo *Enigma* già citato. (S.Cam.)

L'esperto

Languasco: «Manca la consapevolezza di questi strumenti»

Docente all'Università di Padova, esperto di Teoria analitica dei numeri, Alessandro Languasco, da ormai 15 anni, titolare del corso di crittografia, più di chiunque altro può "illuminarci" sul percorso oscuro di questa disciplina. Il suo corso fa parte del Master internazionale Algant, che – essendo frequentato da studenti di varie nazionalità – è tenuto in inglese.

Quale è l'impostazione nell'insegnamento di una materia che – a noi profani – appare piuttosto ostica?

«Cerco di fornire a una classe cosí variegata un terreno comune di lavoro, evidenziando che i metodi crittografici non possono essere usati "alla cieca", come "scatole chiuse": vanno comprese le basi matematico-algoritmiche teoriche su cui poggia il loro corretto funzionamento, per evitare usi impropri rispetto agli scopi di una certa situazione. E questo è anche il messaggio che sottende ai miei testi, come al libro, recentemente pubblicato, *Manuale di Crittografia* (Hoepli, con Alessandro Zaccagnini)».

Mi pare di capire che è un approccio squisitamente teorico. O sbaglio?

«Essenzialmente sí: non sono previste esercitazioni al computer, perché ritengo che la parte più difficile di questa materia sia carpirne l'intimo funzionamento, in modo da giustificarne punti di forza e debolezze e motivare certe scelte, piuttosto di altre, nel design dei crittosistemi usati. Lo scopo è quello di far maturare un atteggiamento autonomo e critico, necessario a sviluppare un approccio che eviti errori nella progettazione di nuovi protocolli crittografici».

Quale è l'impatto sociale della crittografia?

«È evidente che le sue applicazioni siano presenti in moltissimi aspetti della vita di tutti noi. Ritengo importante che almeno i fondamenti vengano – per quanto possibile – divulgati al più ampio pubblico, perché ci si comporti con cognizione di causa di fronte a strumenti informatici basati sulla crittografia, che rendono "trasparente" – ossia non evidente all'utente finale – come la usano: intendo dire che il programma che consente il prelievo al bancomat o una transazione elettronica non rende evidente quali e quanti passaggi siano effettuati. Un'infarinatura di che cosa accada in questi frangenti aiuterebbe a non incorrere in spiacevoli inconvenienti. Inoltre i moderni crittosistemi a chiave pubblica rendono possibili anche altre applicazioni non direttamente legate al commercio quali la firma digitale e il voto elettronico: avere consapevolezza di cosa significhi firmare digitalmente un impegno – e perché tale azione comporti dei vincoli nel mondo reale – o quali problematiche siano insite nel votare elettronicamente porterebbe utente finale e legislatore, che regola la materia, a scelte più attente».

La generazione dei cosiddetti "millennials" avrà, secondo lei, una gestione consapevole di questi strumenti?

«Non sono particolarmente ottimista in merito. Per molti dei "nati" attorno al 2000, a una impressionante dimestichezza nell'uso – come utenti finali – di apparecchi informatici sviluppati da altri, non corrisponde un'altrettanta capacità, o volontà, di scavare più in profondità, fino a carpire come e perché i sistemi operino. Manca il "guardare dentro alla scatola", per scoprire gli "ingranaggi" contenuti. Temo che a molti di loro manchi la consapevolezza delle complesse implicazioni delle loro azioni nell'uso degli strumenti che la crittografia ha reso possibili nel nostro periodo storico».

Silvia Camisasca

Oltre la notte. Borgna: la «grande speranza», arcobaleno della vita

Nel suo ultimo libro lo psichiatra indaga sulla fiducia trascendente, puntuale come una stella del mattino, capace di resistere ai naufragi delle «piccole speranze» mondane. Il rapporto con la misericordia, per sostenere le attese degli altri

Marina Corradi

«La speranza è l'arcobaleno gettato al di sopra del ruscello precipitoso e repentino della vita, inghiottito centinaia di volte dalla spuma e sempre ogni volta ricomponentesi: continuamente lo supera con delicata bella temerarietà, proprio là dove rumoreggia più selvaggiamente e pericolosamente». Questa è la speranza, secondo Nietzsche, e a questa frase si ispira il titolo dell'ultimo saggio di Eugenio Borgna, *L'arcobaleno sul ruscello – Figure della speranza* (Raffaello Cortina, pagine 130, euro 11,00).

Come un rabdomante Borgna, psichiatra emerito dell'Ospedale Maggiore di Novara, ha voluto andare alla ricerca della speranza oscurata, della speranza che come acqua carsica scorre pure sotto le più opache sofferenze della vita. Stiamo parlando della "grande speranza", colonna fondante del vivere, e non delle piccole speranze quotidiane, che non di rado si dissolvono, oppure ci tradiscono. (E qui le parole di Borgna richiamano alla mente la medesima distinzione, fatta da Benedetto XVI nella *Spe salvi*). La grande speranza, scrive l'autore, resiste ai naufragi delle piccole speranze. Dal franare delle speranze mondane rinasce, indistruttibile, la speranza trascendente, fedele e puntuale come una stella del mattino. La speranza può risorgere nel fondo di una malattia, che ci costringe a tornare alla nostra interiorità: così che dalla sofferenza possono venirci nuove capacità di comprensione della vita, ma anche di immedesimazione negli altri. Quasi che anche nelle avversità la speranza fosse un dovere morale, come disse Walter Benjamin, un «ascolto dell'infinito che è in noi».

E nella malinconia, o nella oscurità della depressione, dove si va a cercare la speranza? Borgna si rifà alla distinzione kierkegaardiana di «malinconia buona» e «malinconia maligna». Perché esiste una tristezza che è come una radiazione primitiva – l'espressione è di Schelling – e che pure è creativa. Eugenio Borgna ci ricorda il Rilke delle *Lettere a un giovane poeta*. Queste tristezze sarebbero, scrive Rilke, «i momenti, in cui qualcosa di nuovo è entrato in noi, qualcosa di sconosciuto; i nostri sentimenti ammutoliscono in casta timidezza, tutto in noi indietreggia, sorge una calma, e il nuovo, che nessuno conosce, vi sta nel mezzo e tace». La malinconia maligna, invece, è quella in cui ci si allontana dal mondo delle persone e delle cose, e si resta prigionieri di un silenzio impenetrabile. Eppure anche questa malinconia, testimonia lo psichiatra che per decenni ha curato le malate dell'Ospedale di Novara, a un certo punto può dissolversi, e lasciare timidamente riaprirsi un soffio di speranza.

E nella notte oscura dell'anima sperimentata da tanti santi, nell'algido silenzio di Dio, dove può essere l'orma della speranza? Forse una risposta è in Santa Teresa d'Avila, «Dio conduce coloro che vuole salvare lungo i sentieri dell'angoscia». L'angoscia dunque, commenta Borgna, come una lampada sempre accesa, nel fondo del buio, e non così lontana dalla speranza.

Un capitolo è dedicato infine al rapporto fra speranza e misericordia, nell'eco dell'insegnamento di Francesco: perché in ogni nostra giornata secondo Borgna siamo «circondati da sciami di attese e speranze», da una folla di sguardi che tacitamente domandano o mendicano una parola di conforto. Parole che a loro volta sono «pozzi artesiani», mai inerti, ma capaci di ridestare vita e risonanze. La misericordia aiuta la speranza a rinascere, anche nel fondo del dolore. E qui la riflessione dell'autore si sofferma sulla straziante condizione di chi, «venendo da terre straniere, si arena in luoghi sconosciuti o ostili, non avendo nemmeno parole che possano creare ponti». «Siamo toccati – si domanda Borgna – siamo almeno lambiti, dalla percezione delle solitudini desertiche in cui vivono e muoiono infinite persone?».

Sperare, come una militanza doverosa per noi e per gli altri. Sempre chiamati a guardarci dentro, negli abissi della nostra interiorità, sempre chiamati a cercare; mai chiudendo gli occhi, o affogando nel rumore quella domanda ostinata che abita nel fondo di noi.