La crittografia,
uno snodo cruciale per la cybersicurezza

Angelo Luvison

Sommario

Da millenni, l'attività di intelligence è una funzione primaria delle agenzie governative dei più importanti Paesi. Ciò comporta l'impiego di sistemi di crittografia per la protezione di dati riservati, da un lato, e di crittanalisi per carpire tali informazioni, dall'altro. Più recentemente, la sicurezza informatica (cybersicurezza) è diventata un'esigenza di privati e di aziende, a cui si è opposto un incremento speculare dell'ingegno di malintenzionati nell'uso di tecniche crittografiche per fini disonesti, illeciti o illegali. L'articolo esplora alcuni aspetti del complesso problema privacy-sicurezza nel contesto del ruolo che la crittologia gioca in questi temi particolarmente caldi. Si introducono, in modo discorsivo e intuitivo, i principi di base dei sistemi a chiave pubblica, oltre a due recenti sviluppi in crittografia. Si accenna, infine, al cyber rischio dovuto al cosiddetto"fattore umano", se non adeguatamente governato.

Abstract

From millennia, the issue of intelligence has been a major concern of government agencies in many countries. Therefore, cryptology techniques have been emerging in the dual role of cryptography to protect private information and cryptanalysis to get non-authorized access to the same information. In recent times, cybersecurity objectives, as extended to both personal and business sectors, witnessed a dramatic soaring of cybercrime activities, especially malware. The paper investigates a number of items in the intertwined relationship between privacy and security in the framework of the increasing role cryptology is expected to play in the future. The principles of public-key systems and other recent developments of cryptography are introduced in simple tutorial form. A final issue is how to contain the cyber risk stemming from "the human factor", when not properly controlled.

Keywords: Cybersecurity, Public-key cryptography, British Intelligence (GCHQ) priority, Cryptanalysis and birthday attack, Zero-knowledge protocol, Human factor

1. Introduzione[1]

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files
(Bruce Schneier, crittografo statunitense)

Il tema della cybersicurezza è oggi particolarmente caldo poiché rappresenta uno snodo cruciale fra i diritti dei cittadini, l'azione di controllo dei Paesi e l'incalzare di nuove tecnologie. Da millenni, tanto in Occidente quanto in Oriente l'attività di intelligence – un tempo si chiamava "spionaggio", un termine oggi considerato poco elegante – è fonte di occupazione (e preoccupazione) crescente per i principali governi [2]-[4].

La crittografia sembra oggi essere demonizzata da molti come causa rilevante dell'insicurezza della società e del genere umano. L'intera questione è posta con chiarezza da Juan Carlos De Martin del Politecnico di Torino. Su *Nòva24*, l'inserto tecnologico del *Sole 24 Ore* (6 dicembre 2015), egli osserva: "Dopo l'11 settembre, le barriere che fino a quel momento avevano tenuto sotto controllo la tentazione securitaria furono in buona parte spazzate via, prima degli Stati Uniti e poi in Europa e in altre parti del mondo. […]. Per i tecno-entusiasti – e per i politici che li assecondavano – il sacrificio della privacy di milioni di cittadini innocenti era il prezzo trascurabile da pagare se in cambio si poteva ottenere un sistema automatico di prevenzione degli attentati terroristici. In questo ordine di cose la crittografia non poteva che essere un nemico da combattere strenuamente: i bit, infatti, devono essere 'in chiaro' affinché l'intero approccio basato sulla sorveglianza di massa abbia senso. Ciò che è emerso dopo le rivelazioni di Snowden ha seriamente intaccato i presupposti del 'security complex'. […]. [È] stato messo in evidenza che il semplice, ma incontrovertibile, fatto che indebolire la crittografia con l'obiettivo di intercettare più facilmente i terroristi rende ciascuno di noi, nonché le banche e tutte le istituzioni che usano la crittografia, più deboli nei confronti di tutti i criminali del pianeta. È davvero saggio andare in quella direzione? […]. Eppure ormai non ci dovrebbero essere dubbi che la sorveglianza di massa è allo stesso tempo pericolosa e non risolutiva, che la crittografia è troppo importante per volerla indebolire e che la lotta ai terroristi richiede un mix sapiente di vecchie tecniche 'analogiche'? E di nuovi strumenti digitali usati in maniera mirata. Solo così è possibile sperare di essere sia rispettosi dei diritti alla base delle nostre democrazie, sia efficaci nel contrasto ai terroristi".

Un chiarimento concettuale e terminologico può risultare, a questo punto, appropriato. È opportuno distinguere tra *security* (attinente alla protezione e alla privacy dei dati) e *safety* (concernente la sicurezza fisica, l'incolumità): proprio qui si articola il confronto dialettico tra le agenzie di intelligence per garantire la

[1] L'articolo è una continuazione del lavoro [1] del quale conserva lo stile comunicativo; i vari temi sono presentati seguendo un'esposizione parzialmente aneddotica e, soprattutto, narrativa, qua e là in tono leggero, in modo quasi ludico – anche se l'argomento è terribilmente serio, oggi come ieri e, ancor più, in futuro.

safety contro il terrorismo e l'esigenza dei cittadini e delle aziende a proteggere i loro dati, la propria cybersecurity (cfr. anche il paragrafo conclusivo). Data la polisemia della parola italiana "sicurezza", l'uso del lessico inglese, in certi contesti, può essere utile per evitare ambiguità.

Il punto di equilibrio non potrà che essere il frutto di una dialettica costruttiva tra diversi poli d'interesse, pur tenendo conto che l'intera "questione sicurezza" è resa molto articolata, quindi difficilmente componibile, in uno scenario caratterizzato da grande complessità, arduo da controllare, circolare e non lineare, quindi sensibile (vulnerabile) anche a piccoli input o fattori di cambiamento. I principali elementi tecnologici di questo scenario sono: le reti sociali, la raccolta e l'analisi di immense moli di dati (big data), l'Internet delle cose (che integra il mondo fisico con il digitale), i servizi di cloud computing e cloud gaming, nonché delle funzioni di rete virtuale e definite in software. Queste tecnologie – separatamente o nel loro insieme – favoriscono lo sviluppo di nuovi modelli di business, per esempio, basati su complesse piattaforme che legano la domanda e l'offerta, promuovendo la connessione diretta tra consumatori e altri gruppi, e sostituiscono le tradizionali catene del valore del prodotto [5]. In ogni caso, tecnologie e piattaforme si basano sulla condivisione dell'informazione, il che compromette la possibilità di un controllo diretto dei dati proprietari.

I progressi tecnologici hanno prodotto benefici incommensurabili per il nostro mondo, ma c'è una criticità evidente: i criminali sono spesso i più rapidi e innovativi ad adottare la tecnologia e i tempi moderni hanno condotto a crimini moderni. I malintenzionati di oggi sono in grado di rubare identità, prosciugare conti bancari online e azzerare server di computer. È davvero inquietante sapere che è semplice attivare le telecamere dei monitor per spiare le nostre famiglie, che i ladri sono in grado di analizzare i social media per determinare il momento migliore per entrare in casa e che i bioterroristi sono in grado di scaricare la ricetta di malattie epidemiche.

In ogni caso, un punto saldo per imprese e cittadini è rappresentato dalla consapevolezza della protezione – information security – che i moderni sistemi di crittografia possono dare. Quindi, il conflitto tra sicurezza e riservatezza degli individui, come pure delle imprese, e l'esigenza di contrastare il cybercrimine in tutte le sue forme rende più evidente non solo il ruolo delle tecniche crittografiche quanto anche la necessità ineludibile di un'attenzione maggiore al cosiddetto "fattore umano".

Nell'articolo si considera – ancorché in termini divulgativi (ossia senza formule), metaforici e con il ricorso all'analogia (immagini mentali) – il punto di svolta che ha aperto la strada ai sistemi più avanzati: la crittografia a chiave pubblica (paragrafo 2). Essa rappresenta il più recente passo verso la matematizzazione e la formalizzazione della crittologia, che può perciò rivendicare un proprio statuto di disciplina scientifica autonoma. Il paragrafo 2 è articolato in più punti, in particolare il 2.3 riassume la vicenda dell'ormai accertata priorità dei crittografi britannici nell'invenzione della crittografia a chiave pubblica, da loro chiamata cifratura non segreta [3]. Il paradosso del compleanno con il suo risultato del tutto controintuitivo rientra nella categoria delle sorprese che il

calcolo delle probabilità ci riserva. Uno dei più famosi ed emblematici attacchi di crittanalisi sfrutta proprio questo paradosso ed è oggetto del paragrafo 3. Nel paragrafo 4, si riferirà di due importanti recenti contributi da parte di ricercatori italiani, che continuano così una nostra tradizione secolare a partire da Leon Battista Alberti, Girolamo Cardano, Giovanni Battista della Porta per arrivare, nel Novecento, a Luigi Sacco [1]. Nel conclusivo paragrafo 5, si sottolinea la rilevanza del "fattore umano" nella cybesicurezza, oltre alla tecnologia crittografica. Il riquadro finale sviluppa alcune considerazioni sulla rappresentazione pubblica e mediatica dei servizi di intelligence degli USA e del Regno Unito. La bibliografia integra e completa quella già riportata in [1], benché alcuni riferimenti fondamentali siano necessariamente ripetuti in entrambi gli articoli.

2. La crittografia a chiave pubblica, ultima pietra miliare della crittografia

Siamo nani sulle spalle di giganti
(Bernardo di Chartres)

Se ho visto più lontano, è perché stavo sulle spalle di giganti
(Isaac Newton)

Nel precedente lavoro [1], abbiamo delineato i passi che, a giudizio degli studiosi, rappresentano altrettante pietre miliari verso la matematizzazione della crittologia contemporanea:

1. il principio di Kerchoff;
2. il cifrario a blocco monouso (*one-time pad*) di Vernam;
3. il fondamentale lavoro di Shannon sulle comunicazioni segrete [6].

(Per una discussione approfondita e analitica a livello universitario di questi e altri punti attinenti all'intera disciplina si consigliano i testi [7] e [8]). A proposito di Shannon, il cui centenario della nascita cade quest'anno, tra le varie motivazioni per celebrarlo adeguatamente, l'esperto di innovazione e comunicazione Pascal Zachary (su *IEEE Spectrum* di aprile 2016) avanza la seguente: "Shannon ha dimostrato che la tecnica ingegneristica crea nuove conoscenze tanto rapidamente quanto la scienza e che la pratica ingegneristica può *precedere* una teoria scientifica". Una stoccata non indifferente alla credenza diffusa che l'applicazione viene sempre *dopo* la ricerca di base. L'avanzamento della tecnologia dell'informazione e delle comunicazioni (ICT), a partire da Shannon, Turing, John von Neumann e Norbert Wiener, è la prova evidente della correttezza di questa asserzione. (Un'altra vulgata corrente è, a nostro avviso, l'asserita separatezza statutaria tra matematica pura e matematica applicata – cfr. anche *infra*, nota 5).

La quarta, e più recente, scoperta basilare è la crittografia a chiave pubblica – o cifratura non segreta – il cui principio di funzionamento può essere ricondotto al seguente esempio, adattato dal divertente libro di enigmistica e giochi matematici [9]. La schematizzazione proposta è una fra le più semplici, intuitive

e, allo stesso tempo, istruttive, perché consente di comprendere la logica del principio che sta alla base del sistema[2]:

> Alice vuole inviare un oggetto a Bob[3]. È un oggetto privato che non deve essere aperto da nessuno se non da lui. Alice decide di spedirlo in un cofanetto, ma l'unico modo per chiuderlo è di usare un lucchetto. Scambiarsi le chiavi sarebbe troppo rischioso. Però entrambi dispongono di lucchetti, ciascuno con la propria chiave. Come può Alice essere sicura che il prezioso contenitore possa essere aperto solo da Bob?

Prendete un po' di tempo per escogitare una possibile soluzione al quesito!

Se vi pare di avere riflettuto abbastanza, ecco la successione di passaggi per assicurare che lo scambio avvenga in modo sicuro:

1. Alice chiude il cofanetto con un lucchetto e lo invia a Bob.
2. Bob chiude il cofanetto con un altro lucchetto e lo rispedisce ad Alice.
3. Alice rimuove il proprio lucchetto e rispedisce il cofanetto a Bob.
4. Bob riceve il cofanetto (ora protetto solo dal lucchetto apposto da lui stesso) e lo apre con la propria chiave.

Nei passaggi tra Alice e Bob, nessuno è in grado di aprire il cofanetto – senza manometterlo – poiché non c'è scambio o distribuzione di chiavi (*no-key protocol*), ma solo andirivieni di lucchetti.

(Si può notare che i passaggi potrebbero essere ridotti se Alice e Bob si scambiassero i rispettivi lucchetti *a priori*, cioè prima dell'invio del messaggio. Tuttavia, questa soluzione presenta almeno una controindicazione, infatti si basa sull'aspettativa di una continuità temporale della relazione tra Alice e Bob, i quali nel futuro potrebbero non rimanere così amici… Sarebbe un po' come scambiarsi permanentemente le proprie chiavi di casa, anziché imprestarle per l'uso all'occorrenza).

Partendo da questo concetto, Adi Shamir ha sviluppato (intorno al 1980) il "protocollo a tre passi" per comunicare segretamente in un contesto che permette ad Alice di inviare un messaggio alla controparte Bob in modo sicuro e senza la necessità di scambiare, o distribuire, chiavi di cifratura (per un'elegante formalizzazione matematica del protocollo si può vedere [11]). L'idea di base è che ciascuna delle due parti, possedendo entrambe una chiave privata di cifratura e una privata di decifrazione, usa le proprie chiavi indipendentemente, prima per cifrare il messaggio e poi per decifrarlo. Sembrerebbe plausibile utilizzare in questo scambio la chiave di cifratura di Vernam, cioè una chiave scelta casualmente e utilizzata una e una sola volta (monouso) [1]. È facile però

---

[2] Sul Web sono disponibili molti tutorial utili e interessanti. Fra questi, suggeriamo la registrazione video della conferenza di James Massey [10], che riporta esempi di "trucchi" utilizzabili per verificare se la crittografia sia "scienza" (cioè, può provare ciò che sembra fare) oppure "magia" (cioè, quanto essa sembra fare, o essere, è frutto di mera illusione).

[3] Gli studiosi della crittografia hanno il vezzo di illustrare il funzionamento dei vari schemi attraverso problemi che hanno come protagonisti due personaggi convenzionalmente denominati Alice e Bob.

provare che in tal caso il protocollo diventerebbe totalmente insicuro [10], [11]. È possibile, invece, ricorrere ad algoritmi più sofisticati che sfruttano i risultati della complessità computazionale applicati alla teoria dei numeri, in particolare dei numeri primi (cfr. i successivi punti 2.1 e 2.2).

Peraltro, il protocollo come descritto non fornisce alcuna forma di autenticazione del mittente, senza la quale lo schema sarebbe suscettibile dell'attacco da parte di un cosiddetto "uomo in mezzo", potenzialmente in grado di creare falsi messaggi, in sostituzione di quelli originalmente trasmessi.

Concetti di questo tipo, apparentemente ovvi e banali, hanno rappresentato il punto di partenza per prospettive del tutto inedite della crittografia scientifica negli ultimi quarant'anni.

A metà degli anni 1970, Whitfield Diffie e Martin Hellman, a partire da un'idea di Ralph Merkle, hanno sviluppato il concetto di *crittografia asimmetrica*, o *a chiave pubblica* [12]. Ogni utilizzatore tiene segreta la sua chiave di decrifazione e rende nota la sua chiave di cifratura in un elenco (*directory*) pubblico. La crittografia a chiave pubblica permette a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave: chiunque (Alice) desideri comunicare privatamente con un utilizzatore (Bob) la cui chiave sia in elenco deve solo leggere la chiave pubblica di Bob per cifrare il messaggio che unicamente Bob potrà decifrare con una chiave diversa, la propria chiave segreta.

Come prima, si può visualizzare il principio con un'analogia fisica, il funzionamento di una cassaforte meccanica o della cassetta postale di servizio:

1. Bob spedisce ad Alice il suo lucchetto aperto (non necessariamente su un canale sicuro).
2. Alice deposita il proprio messaggio in una cassaforte chiudendola con il lucchetto di Bob.
3. Solo Bob ha la chiave per aprire il proprio lucchetto, quindi per recuperare e leggere il messaggio inviatogli da Alice.

Le possibilità legate alle metafore esemplificate sono molteplici. Nel 1977, Donald Rivest, Adi Shamir e Leonard Adleman hanno proposto la crittografia a chiave pubblica basata sulla teoria della complessità e sulle proprietà dei numeri primi. Oggi, lo schema – denominato RSA dalle iniziali dei cognomi degli inventori – è comunemente impiegato per garantire la firma digitale, cioè l'autenticazione del mittente, oppure l'integrità del messaggio. Per consentire di svolgere queste funzioni in modo sicuro, tecniche di crittografia a chiave pubblica si trovano anche nei protocolli di Bitcoin, sistema dedicato alle transazioni commerciali-finanziarie che impiegano la e-currency, o moneta virtuale, bitcoin (dove la "b" iniziale della valuta dovrebbe essere scritta in minuscolo). Ulteriori approfondimenti e particolari operazionali su Bitcoin sono disponibili alla pagina Web https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained.

2.1 La sfida dell'RSA

L'obiettivo principale del progetto di un cifrario efficace è di rendere l'operazione (illegale) di decrittazione, o forzatura, praticamente equivalente alla soluzione di

problemi laboriosi (cioè complessi) dal punto di vista computazionale. Caso molto comune è oggi quello della fattorizzazione del prodotto *n* di due numeri primi *p* e *q*, dove *n* è costituito, per esempio, da 250 cifre decimali, benché il calcolo di *n* sia rapidamente effettuabile se *p* e *q* sono entrambi noti. L'operazione diretta (il prodotto) è facile, l'inversa (la fattorizzazione) tutt'altro: siamo nel campo della complessità computazionale[4].

Prima di pubblicare i loro lavori in una rivista scientifica, nel 1977, Rivest, Shamir e Adleman scrissero a Martin Gardner – autore della celebre rubrica di "Giochi matematici" su *Scientific American/Le Scienze* – allo scopo di coinvolgere in modo rapido e capillare un uditorio più vasto di quello strettamente accademico. Nella sua rubrica, Gardner lanciò ai lettori la sfida, denominata RSA Factoring Challenge [13], di decrittare un messaggio che avrebbe richiesto la scomposizione in fattori primi di un numero di 129 cifre, impresa che all'epoca era considerata impensabile stante le macchine disponibili. "A new kind of cipher that would take millions of years to break", era l'iperbolico titolo dell'articolo di Gardner. Ma nel 1994 gli sforzi congiunti di 1600 computer e di 600 utenti connessi a Internet per sei mesi, e coordinati dal matematico olandese Arjen Lenstra, permisero di trovare i due fattori per decrittare il messaggio originale: "The magic words are squeamish ossifrage" ("Le parole magiche sono gipeto schizzinoso"). La sfida si chiuse ufficialmente nel 2007 dopo che si era ottenuta la fattorizzazione di numeri di 160 cifre, anche se poi ci si è spinti oltre: oggi la barriera da superare è di 250 cifre.

Si può osservare che la vicenda capitanata da Lenstra rientra a buon diritto in quei casi che Michael Nielsen ne *Le nuove vie della scoperta scientifica* descrive come passaggi dall'intelligenza singola all'intelligenza connessa e collettiva grazie alla condivisione in rete dei risultati di ricerche scientifiche. Un altro esempio è quello dei matematici che nel "Polymath Project", pilotato da Tim Gowers, collaborano e si confrontano online per trovare soluzioni a problemi ancora insoluti.

2.2 Turing e i numeri primi

La teoria dei numeri primi è dunque uno dei capisaldi dell'odierna crittografia a chiave pubblica, e di questa matematica Turing si è occupato a fondo prima e dopo la Seconda guerra mondiale. Perciò, Turing può essere considerato un precursore, sia pure in senso lato, della crittografia a chiave pubblica, sebbene non un contributore diretto. Nel periodo bellico, ebbe invece, a Bletchley Park, il ruolo di crittanalista principe nel decrittare (forzare) la macchina tedesca Enigma [1].

L'inglese G. H. Hardy è spesso citato per aver sostenuto – in *Apologia di un matematico* (1940) – che questa branca della matematica pura è uno dei più ovvi esempi della sua inutilità pratica, una visione oggi alquanto datata[5]. A

[4] Per esempio, i numeri primi sono correntemente usati nelle chiavi di cifratura dei PIN delle carte bancarie.

[5] Nel documentario di Olivier Peyon dal titolo *Comment j'ai détesté les maths* (2013), Cedric Villani, noto matematico e direttore dell'Institut Henri Poincaré di Parigi, sostiene – d'accordo con molti altri studiosi contemporanei – che la distinzione tra matematica pura e matematica applicata è da considerare puramente accademica.

Oxford, Hardy era seguace di una concezione sostanzialmente platonica della matematica, secondo la quale essa e i suoi risultati costituirebbero "scoperte" ma non "invenzioni"; quindi la teoria dei numeri primi "è così e basta", senza implicazioni ulteriori. Questa impostazione caratterizzò l'Università di Oxford fin dalla fondazione (verso la fine dell'XI secolo); infatti, il suo magistero filosofico-matematico fu opera di eminenti studiosi francescani quali Roberto Grossatesta e Ruggero Bacone nel XIII secolo e poi, all'inizio del successivo Trecento, di Guglielmo di Occam. Essi improntarono l'insegnamento oxoniano in modo fondamentalmente platonico, almeno fino al termine del medioevo [14]. È probabile che Hardy oggi si ricrederebbe vedendo i progressi della scienza dei segreti, consentiti proprio dalle basi di teoria dei numeri. Peraltro, Hardy non era autorizzato a sapere, per evidenti ragioni di sicurezza nazionale, che matematici, fisici, ingegneri stavano lavorando insieme in un team formidabile contro la presunta inviolabilità di Enigma.

2.3 Le priorità dei crittografi britannici

I due capisaldi della crittografia a chiave pubblica sono dunque il protocollo di scambio delle chiavi di Diffie-Hellman e il sistema di cifratura RSA, proposti entrambi in ambiente accademico, rispettivamente, nel 1976 a Stanford e nel 1978 al MIT.

Molto presto, peraltro, si diffuse la voce che entrambe le tecniche fossero già note, da anni, ai crittografi del governo britannico. Si è effettivamente accertato [3] che la loro scoperta, risalente all'inizio degli anni Settanta, è da attribuire al CESG (Communications-Electronics Security Group), il centro di sicurezza delle informazione del GCHQ (Government Communications Headquarter) – pressappoco l'equivalente britannico della NSA statunitense. Solo nel dicembre 1997, ne fu data la conferma ufficiale con il contestuale rilascio di un articolo sulla storia della scoperta, scritto nel 1978 dal suo artefice James Ellis [15]. Purtroppo, Ellis morì neppure un mese prima che la memoria potesse essere letta a un uditorio di crittanalisti dal collega Cliff Cocks il 18 dicembre 1997, dopo quasi tre decenni di segretezza tipicamente *British*.

"Cifratura non segreta" (*non-secret encryption*) è la locuzione adottata da Ellis per l'idea di risolvere il problema della distribuzione delle chiavi in crittografia [15][6]. Il presupposto che due parti dovessero prima scambiarsi un segreto condiviso per poter comunicare in modo sicuro era sempre stato considerato come ovvio, fin dai tempi di Giulio Cesare. Ellis infranse questa convinzione con

[6] In [15], Ellis riferisce di un documento intitolato "Final Report on Project C-43" dei celebri Bell Telephone Laboratories (BTL) senza, peraltro, fornirne informazioni aggiuntive utili all'identificazione. *En passant*, questo particolare ha incuriosito per anni la comunità crittografica per la possibilità che i ricercatori dei BTL avessero fatto importanti progressi sulla crittografia a chiave pubblica addirittura negli anni 1940. Il misterioso rapporto (del 1944) sulla cifratura del segnale vocale in realtà esiste ed è perfino disponibile online. È firmato da Walter Koenig Jr., l'ingegnere-capo del progetto; non è perciò chiaro perché Ellis parli di un "autore sconosciuto". Il Progetto C-43 – commissionato dal National Defense Research Committee (NDRC) statunitense ai BTL fu sviluppato in parallelo, ma con nessuno o pochi contatti, con il più famoso Progetto X (o SIGSALY) sulla segretezza del linguaggio parlato, che vide impegnati anche Shannon e Turing (cfr. riquadro 2 di [1]).

l'ipotesi che il ricevente potesse giocare un ruolo nel processo di cifratura, un'idea decisamente rivoluzionaria.

La soluzione, equivalente a quella che oggi è chiamata crittografia a chiave pubblica, si basa sullo stesso concetto proposto da Diffie e Hellman, ma Ellis, come anche Diffie e Hellman, non riuscì ad arrivare a una realizzazione concreta dell'idea di base. Ellis, tuttavia, fu perseverante, senza curarsi dei dubbi avanzati da molti colleghi. Memorabile è il commento di Shaun Wylie (capo di Ellis ed egli stesso codebreaker a Bletchley Park durante la guerra): "Sfortunatamente non posso trovare niente di sbagliato in tutto ciò".

Tre anni dopo, nel 1973, il rapporto venne dato da esaminare all'appena assunto Cocks, il quale, in un tempo brevissimo, inventò l'algoritmo (oggi noto come RSA) che sarebbe stato concepito quattro anni dopo da Rivest, Shamir e Adleman. Malcolm Williamson, compagno di liceo di Cocks, fu contestualmente assunto nel GCHQ e pervenne, poco dopo, a quello che oggi conosciamo con il nome di protocollo di Diffie-Hellman. Quindi, entro il 1973, Ellis, Cocks e Williamson avevano ideato *in nuce* tutte le componenti della crittografia a chiave pubblica, che i ricercatori USA avrebbero messo insieme quattro anni dopo.

La comunità degli studiosi di crittografia, all'annuncio del 1997, fu subito in grado di riconoscere la priorità di quanto realizzato dai britannici: l'IEEE nella pagina "Milestones: Invention of Public-key Cryptography, 1965-1975" del suo sito (http://ethw.org/Milestones:Invention_of_Public-key_Cryptography,_1969_-_1975) tributa il giusto riconoscimento ai tre ricercatori britannici[7]. Tuttavia, non è inusuale per pubblicazioni che descrivono l'origine della crittografia a chiave pubblica continuare a sminuire, o ignorare completamente, la scoperta del GCHQ. Lo stesso Hellman, in occasione della ristampa nel 2002 del suo articolo di rassegna [12], nel nuovo commento retrospettivo non ha certamente seguito la norma di bon ton di menzionare i lavori prioritari del GCHQ. Questo disinteresse dei nordamericani verso altri si può riscontrare anche nello scarso o nullo riconoscimento della paternità dell'invenzione del telefono di Antonio Meucci (rispetto ad Alexander Graham Bell), nonostante che una risoluzione della Camera dei Rappresentanti USA l'abbia ufficialmente dichiarata nel 2002.

3. L'attacco del compleanno in crittanalisi

Corruzione, ricatti, inganni e metodi classici di intelligence e ingegneria sociale possono essere impiegati per ottenere informazioni riservate dalle persone – uomini o donne, indifferentemente. Per esempio, costringere qualcuno a rivelare la propria chiave segreta con minacce è illegale ma tecnicamente fattibile. Un altro tipo di attacco, meno aggressivo, è l'uso di telefonate o email capziose per carpire (*phishing*) le password a soggetti disattenti o ingenui.

Anche la lista degli attacchi contro i sistemi informatici non finisce mai [16]-[18]. Si possono usare metodi furtivi basati sull'overflow dei buffer o su *malware* – software malevolo – per rivelare chiavi segrete in sistemi di software.

[7] Su proposta, peraltro, della sua Sezione britannica e irlandese: IEEE United Kingdom and Republic of Ireland Section.

Ransomware è un tipo di malware che, nella variante *crypto*, blocca il computer della vittima prescelta, cifrandone illecitamente e illegalmente le informazioni per impedirne l'uso finché la vittima non paga un riscatto (ransom) ai cybercriminali per avere la chiave di decifrazione che consente di accedere ai propri dati. Un esempio di ransomware è CryptoLocker (dal 2013), per il quale la chiave costa circa 300 euro. CryptoLocker agisce come la pesca a strascico: cifre relativamente basse ma un numero elevato di obiettivi potenziali. Nuovi ransomware si dimostrano ancor più esosi e aggressivi.

Decrittare le trasmissioni cifrate può dimostrarsi un gioco lungo, complicato e costoso. Altri attacchi informatici si basano allora su un'intuizione assai semplice: cercano di intrufolarsi con un virus in un PC o in uno smartphone. Un pezzetto di codice che, una volta installatosi, quatto quatto assume progressivamente il controllo del dispositivo aggredito e si appropria di tutte le informazioni sensibili.

Si potrebbe ritenere che questi attacchi alla sicurezza, specialmente quelli basati su logiche di ingegneria sociale e/o sull'implementazione del sistema di cifratura, siano sleali, ma il mondo della crittanalisi è caratterizzato da scarsissima correttezza: se qualcuno vuole attaccare un sistema informatico, sta già comportandosi in modo disonesto e infrangendo le regole. Se un opponente di solito prova ad attaccare il punto più debole di un sistema, allora chi vuole difendersi deve cercare di scegliere gli algoritmi più resistenti per avere una ragionevole sicurezza che l'azione illegale sia resa difficilmente praticabile e che, quindi, sia scoraggiata.

Vediamo ora i fondamenti matematici di uno degli attacchi di crittanalisi fra i più temuti: l'attacco del compleanno. In teoria della probabilità, il problema, o paradosso, omonimo riguarda la probabilità che almeno due persone di un medesimo gruppo compiano gli anni lo stesso giorno (non occorre che gli anni di nascita coincidano). Il paradosso, proposto nel 1939 da Richard von Mises – da non confondere con Ludwig von Mises, uno dei padri del neoliberismo – sta nel fatto che la "probabilità di collisione" è molto maggiore di quanto si possa intuitivamente immaginare. Infatti, in un gruppo di 23 persone tale probabilità è già del 50%; con 30 persone supera il 70% e il 97% con 50; il 99% di probabilità si raggiunge con 57 persone. All'evento certo, tenendo conto della possibilità di anni bisestili, si arriva con almeno 367 persone per il principio dei buchi della piccionaia (o legge delle cassette postali). La dimostrazione analitica della soluzione è reperibile in letteratura a diversi livelli di approfondimento, anche se è consigliabile il volume [19] per completezza di trattazione (oltre che per molti altri stimolanti quesiti probabilistici).

Questo problema ha ispirato la realizzazione dell'attacco del compleanno in casi in cui la firma digitale impiega funzioni crittografiche cosiddette *hash* (illustrate, per esempio, in [7]). In linea di principio, le funzioni (o algoritmi) hash in crittografia costituiscono un modo per assicurare la sicurezza dell'informazione. Esse sono tipicamente usate nelle firme digitali e nello stabilire connessioni sicure tra i siti Web. I dati, fatti passare in un algoritmo di hash, producono una successione di bit più breve; questa stringa opera come una sorta di *message*

digest (estratto del messaggio)[8]. Ogni cambiamento dei dati originali cambia la stringa dei bit estratti. La stringa risultante agisce perciò come impronta digitale dei dati, garantendo che nessuno abbia interferito con essi.

Le funzioni hash svolgono un ruolo essenziale in crittografia per verificare l'integrità di un messaggio, infatti, l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un estratto completamente differente rispetto a quello calcolato sul testo originale, rivelando così una tentata frode. Esse possono essere anche utilizzate per la creazione di firme digitali, in quanto, non richiedendo calcoli lunghi e complessi, permettono di realizzare rapidamente la firma anche per file di grosse dimensioni. È certamente più conveniente eseguire un hashing del testo da firmare per poi autenticare solo questo, evitando così l'applicazione di complessi schemi di crittografia asimmetrica su moli di dati molto grandi.

Si noti che il paradosso del compleanno si basa su coppie che "collidono" (stesso giorno di compleanno), ed è esattamente quello che si propone di ottenere l'omonimo attacco: trovare coppie diverse di sequenze binarie che collidono, ossia che producono lo stesso output. Le firme digitali possono essere vulnerabili a questo tipo di attacco, poiché i risultati del paradosso sono utilizzabili per generare un contratto fraudolento contro chi ha apposto la propria firma digitale a una versione corretta del contratto. Per evitarlo, la lunghezza dell'output della funzione hash deve essere sufficientemente grande, cioè resistente alle collisioni, così da rendere l'attacco computazionalmente impraticabile. Sulla base di approfondimenti teorici della robustezza rispetto a questo tipo di attacco, risulta che una funzione di hash dovrebbe avere una lunghezza di almeno 128 bit e, in un prossimo futuro, anche di 256 bit [7].

4. Riconoscimenti a studiosi italiani

Accenniamo qui a due recenti sviluppi in settori di frontiera della crittologia, che hanno visto il sostanziale apporto di ricercatori italiani, sia pure non da soli.

4.1 "Il re degli algoritmi di sicurezza"

Si è prima ricordato che gli algoritmi hash sono utilizzati in applicazioni crittografiche che garantiscono l'autenticità dei documenti digitali: per esempio, le firme digitali. Guido Bertoni, laureato al Politecnico di Milano, è uno degli inventori di SHA-3 (Secure Hash Algorithm-3), un inedito algoritmo hash di crittografia, anche conosciuto con il nome di Keccak – pronunciato "catch-ack" – e in [20] definito "Il re degli algoritmi di sicurezza".

Il National Institute of Standards and Technology (NIST) degli USA ha selezionato nel 2012, dopo una competizione durata cinque anni, l'algoritmo studiato dai ricercatori della STMicroelectronics Guido Bertoni, Joan Daemen, Gilles Van Assche e Michaël Peeters. La loro proposta ha superato altre 63 offerte ricevute dal NIST in seguito alla gara bandita nel 2007, quando si temeva

[8] *Hash* significa letteralmente "polpetta fatta con avanzi di cibo sminuzzati".

che lo standard SHA-2 potesse essere minacciato entro breve tempo (preoccupazione poi rivelatasi eccessiva).

Keccak, basandosi su una generalizzazione del concetto delle funzioni hash crittografiche, non sembra suscettibile di forzature con metodi tradizionali. Inoltre, il progetto hardware lo rende particolarmente adatto a sistemi *embedded*, dedicati ad applicazioni speciali che richiedano chip di piccole dimensioni e con basso consumo di potenza[9].

4.2 Il premio Turing 2012

Silvio Micali – laureato alla Sapienza di Roma e oggi al MIT – è stato insignito con la collega Shafi Goldwasser del "2012 A.M. Turing Award" per lavori fondamentali di scienza della crittografia basati sulla teoria della complessità e per metodi pionieristici di verifica delle dimostrazioni matematiche. Forse, stiamo per assistere a un nuovo balzo in avanti della disciplina, dopo Shannon, Turing e i sistemi DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA. Il conferimento del premio risulta ancora più significativo se si ricorda che il 2012 ha segnato l'anno del centenario della nascita di Turing.

Nella motivazione del premio appare anche il riferimento all'interessante caso dei protocolli di autenticazione a conoscenza zero (*zero-knowledge protocol* o *zero-knowledge proof*). Si tratta di protocolli raffinati che consentono di verificare l'identità del mittente, evitando l'impiego diretto dell'informazione d'identificazione, che potrebbe essere intercettata e successivamente utilizzata da un terzo protagonista per cercare di far credere di essere il mittente autorizzato.

L'idea di base della prova a conoscenza zero può essere visivamente illustrata ricorrendo alla "metafora della caverna spiegata ai bambini" [21]. La buffa caverna di figura 1 è formata da due tunnel A e B separati da una porta che può essere aperta solo usando una frase segreta, o password. Peggy[10] vuole convincere Victor di essere a conoscenza del segreto d'accesso alla caverna senza però rivelarglielo. A questo scopo, Peggy raccomanda a Victor di restare fuori dal tunnel ed entra in uno qualsiasi dei due punti d'accesso. Ora, Victor avanza all'ingresso della caverna e chiede a Peggy di uscire o dal tunnel A o dal tunnel B. Peggy ci riesce aprendo, qualora necessario, la porta con la password. Peggy ha solo il 50% di probabilità di trovarsi già nel tunnel giusto e di non avere perciò bisogno della password. Ovviamente, la prova deve essere ripetuta più volte. Dopo N volte, la probabilità che Peggy goda solo di una fortuna sfacciata scende a 2^{-N}, diventa cioè esponenzialmente trascurabile. Peggy avrà così dimostrato a Victor di conoscere la chiave segreta senza avergliela rivelata[11]. Ricorrendo a un significato secondario, ma non scomparso,

[9] Per una descrizione tecnica aggiornata di Keccak si rinvia al link http://keccak.noekeon.org/index.html/.

[10] In questo contesto, Peggy denota chi ha l'onere di provare l'affermazione e Victor chi la verifica.

[11] Anche gli scambi di crittovaluta bitcoin possono avvenire senza che gli indirizzi siano rivelati, usando la prova a conoscenza zero (https://en.wikipedia.org/wiki/Bitcoin).

dell'aggettivo qualificativo, potremmo dire che Peggy dimostra altresì di essere una persona "probabile"[12].

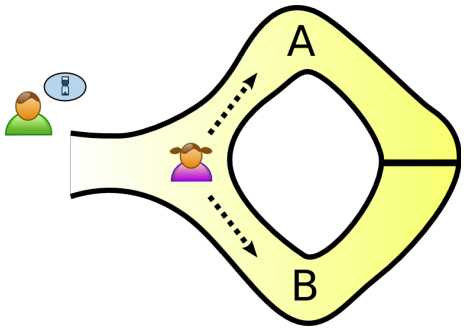

Figura 1.
Metafora della caverna in una "prova a conoscenza zero" (Adattamento da Wikipedia).

È importante, infine, sottolineare che gli studi di Micali e Goldwasser sulla complessità computazionale possono trovare impiego, oltre che in crittografia, in altri settori importanti dell'informatica teorica.

5. Conclusioni: il fattore umano e la cybersicurezza

Un giornalista chiese ad Albert Einstein di spiegare la formula del suo successo. Dopo una breve riflessione, Einstein rispose: "Se A *è il successo, direi che la formula è* A = X + Y + Z*, dove* X *rappresenta il lavoro e* Y *il gioco".*
"E Z *cosa rappresenta?", chiese il giornalista.*
"Tenere la bocca chiusa", replicò lo scienziato.
(Aneddoto tratto da [22]).

Dopo lo scandalo metadati – la raccolta di informazioni personali da parte della NSA – risulta sempre più chiaro che la vera battaglia tra privacy e intelligence sta nella crittologia (crittografia e crittanalisi). L'antica arte crittologica – a partire, soprattutto, da Shannon e Turing – è diventata una disciplina autonoma dallo

[12] Può essere motivo di curiosità, ancorché marginale, il sottile quanto apprezzabile slittamento del significato dell'inglese "*probable*" che fino a circa due secoli fa designava argomentazioni "verificabili e persuasive" o "degne e meritevoli di approvazioni". Allora, per esempio, l'espressione "*a probable doctor*" denotava un medico autorevole in cui riporre fiducia. La questione è ben spiegata da Ian Hacking in *The Emergence of Probability*, a partire dall'apparentemente contraddittoria asserzione dello storico Edward Gibbon: "*Such a fact is probable but undoubtedly false*", frase che, tuttavia, acquista un senso compiuto quando *probable* sia inteso come "plausibile", "verosimile". Oggi, l'aggettivo qualifica un giudizio attendibile confortato da motivi ragionevoli ma non conclusivi. I linguisti direbbero che il "significante" *probable* è sempre lo stesso ma che il suo "significato" è cambiato nel tempo a partire dall'equivalente latino. Infatti, nel trattato di logica *De inventione dialectica libri tres* (1479) dell'olandese Rodolphus Agricola l'avverbio *probabiliter* equivaleva a "persuasivamente". Ovviamente, anche in italiano si è assistito a un analogo fenomeno diacronico per il senso di "probabile" e derivati.

statuto scientifico: non è quindi strano che la usino agenzie di intelligence, governi, aziende, cittadini, come pure, purtroppo, lestofanti e cybercriminali della peggior risma.

A questo punto, diventa opportuno fare due osservazioni. La prima è che questa contesa apre la strada alla ricerca su diritto e cybersicurezza, ben al di là delle facili analisi sinora condotte da spiriti passatisti e tecnofobi, per i quali la tecnologia (crittologia) è da condannare in linea di principio, nonostante che essa sia uno snodo fondamentale per garantire privacy e sicurezza informatica nella vita digitale di tutti gli utilizzatori di Internet.

La seconda è che la tecnologia da sola, pur necessaria, non è sufficiente; infatti, la cifratura è solo un aspetto della sicurezza nelle comunicazioni. Altrettanto importanti sono i nostri comportamenti, da come custodiamo i dispositivi che abbiamo a come ci proteggiamo con PIN e password. Già in [1] abbiamo accennato all'imprescindibilità del fattore umano. Per esempio, l'ingenuità comportamentale dei tedeschi si è intrecciata quasi indissolubilmente con la genialità del team di Turing nel portare a violare la potentissima macchina cifrante Enigma [23]. Oggi il fattore umano risulta, se possibile, ancora più cruciale [17], [18]. Nel monito di Einstein, all'inizio del paragrafo, sta tutta la saggezza per assicurare la privacy dei nostri dati sensibili proteggendoli, per esempio, da tecniche di ingegneria sociale. Saper "tenere la bocca chiusa" – essere cauti, attenti e riservati – è la chiave per tenere sotto controllo il fattore umano.

Da più parti è stato fatto notare che il maggior pericolo per la cybersicurezza non sia tanto l'ignoranza tecnologica quanto la presunzione di non essere nel mirino di malintenzionati. Nell'Internet delle cose e della casa intelligente, sensori, frigoriferi, televisori, smartphone, auto, gli oggetti più disparati sono dei computer collegati alla Rete e gestiti a distanza: nuovi ecosistemi rispettosi dell'ambiente ma che nascondono molti pericoli per privacy e sicurezza. Marc Goodman, autore dell'esauriente (circa 400 pagine) *Future Crimes* [17], osserva che l'attenzione dei cittadini nei confronti di privacy e sicurezza sta evidenziando la fragilità della tecnologia. Egli fornisce tutta una serie di dati statistici stupefacenti: il migliore software antivirus intercetta solo il 5% delle minacce online; l'80% degli hacker lavora per il crimine organizzato. Un esempio del 2013 sarebbe gustoso se non facesse rabbrividire, ed è quello dei ferri da stiro e dei bollitori cinesi, illecitamente equipaggiati con schede Wi-Fi, che consentirono a questi elettrodomestici di accedere alle reti domestiche dei loro acquirenti, diffondendo in tal modo virus e spam.

Goodman osserva che essendo ogni dispositivo connesso (nell'Internet delle cose), tutti noi risultiamo vulnerabili. Nel volume, oltre a investigare le incombenti minacce dei pirati tecnologici, propone una varietà di modi per ridurne i rischi. I protocolli comportamentali pratici e quotidiani suggeriti per difendersi dai pericoli più comuni sono consigli di buon senso, gli equivalenti di chiudere la porta di casa, non lasciare le chiavi inserite nell'avviamento dell'auto, ecc. Lo specifico protocollo normativo stilato da Goodman è sintetizzabile nell'acronimo-acrostico ***UPDATE***: effettuare frequenti ***U****pdate*; utilizzare ***P****asswords* robuste di protezione; eseguire ***D****ownload* del software solo da siti ufficiali; usare i privilegi di ***A****dministrator* con attenzione e parsimonia; spegnere (***T****urn off*) il computer

quando non lo si usa; usare tecniche di cifratura (***E**ncrypt*) nella propria vita digitale per proteggere i dati sia localmente sia trasferendoli attraverso il Web. In questo modo – secondo Goodman – si può evitare più dell'85% delle minacce che incombono dalla Rete.

Nella direzione dei rischi legati al fattore umano, si muove anche il lavoro [18], specificatamente dedicato alla protezione delle reti informatiche di imprese e aziende. Gli autori enunciano e commentano con una certa ampiezza gli errori più legati a debolezze e pecche nel comportamento umano. Per mitigare l'impatto negativo di questo fattore – secondo l'articolo di *Harvard Business Review* – la cultura aziendale deve giocare un ruolo a tutto campo: dall'eccellenza (conformità) operativa e procedurale alla formazione mirata e continua del personale, dall'ispezione sia sistematica sia episodica dei mezzi e dei processi di calcolo alla responsabilizzazione dei dipendenti, ecc. Affinché il cambiamento culturale sia effettivo ed efficace, occorre che i vertici aziendali facciano empaticamente propri obiettivi condivisi di cybersicurezza, agevolandone il percolare in tutti i settori aziendali, dall'information technology alle risorse umane, in modo da garantire "a psychologically safe workplace" (Amy Edmondson, Harvard Business School).

Un'impresa può impiegare anche altri accorgimenti, come rilevare alterazioni significative nei pattern del traffico entrante nelle proprie reti; nel qual caso, occorre usare le tecniche matematiche più aggiornate di analisi dei big data (data science). Per una rassegna approfondita dei metodi, degli algoritmi e delle applicazioni nel settore "grandi moli di dati", si segnalano i due aggiornatissimi fascicoli monografici dei *Proceedings of the IEEE* [24].

In definitiva, l'opposizione privacy-sicurezza pare essere una questione eccessivamente amplificata e semplificata, soprattutto dai mass media. Su *Nòva24* (20 marzo 2016), quanto al dilemma "liberi o connessi", il giornalista esperto di nuove tecnologie, Luca De Biase, acutamente osserva: "Si può coltivare l'obiettivo di vivere in modo pieno la vita in rete e salvaguardare la libertà. Di certo c'è che la rete facilita la sorveglianza più che la privacy e che la raccolta di dati personali [Ndr, metadati] concentra il potere in poche grandi piattaforme private e pubbliche, lasciando i cittadini in una condizione di asimmetria informativa. La privacy è un obiettivo di libertà. La redistribuzione della conoscenza è un obiettivo di giustizia".

La privacy quindi non è certamente morta, ma le scelte che facciamo oggi avranno conseguenze di portata enorme per il futuro. Secondo l'esperto informatico di Microsoft Jaron Lanier dovremmo evitare di parlare della privacy come di uno scambio in cui meno privacy corrisponde a più sicurezza quanto piuttosto dovremmo potere scegliere il livello di privacy desiderato [25]. Non è quindi ineluttabile che la privacy (o cybersecurity) individuale debba essere limitata a beneficio della sicurezza (nel senso di safety) collettiva.

È peraltro da notare che tanto le minacce quanto gli strumenti di protezione cambiano frequentemente interagendo in modo dinamico, accelerato e inarrestabile, perciò la sicurezza informatica, o privacy, assoluta è un obiettivo utopistico. Non c'è quindi da stupirsi se la lezione fondamentale sia che la

crittografia si può scardinare con la crittanalisi, come è accaduto nella recente disputa FBI-Apple sullo sblocco dell'iPhone cifrato dell'autore di una strage negli USA. A prevalere sono sempre le tecnologie e chi le possiede o le sa usare meglio. Occorre, pertanto, definire nuovi equilibri: diventiamo sempre tecnologicamente più potenti ma resta difficile stabilire il confine tra il bene e il male, per questo motivo bisogna riscoprire l'arte del limite [26]. E occorre tenere sempre a mente che l'uso di una tecnologia – o scienza – è ambivalente: gli esiti possono essere costruttivi o no, etici o no, buoni o no. Di per sé una tecnologia non è mai neutrale – recita una ben nota legge formulata dallo storico Melvin Krantzberg (1917-1995). In ultima istanza, le conseguenze dipendono esclusivamente dalla specie *Homo sapiens*, cioè da noi stessi.

Riquadro 1 – L'immagine delle agenzie di intelligence nei media

Why shouldn't I work for the NSA?
(Matt Damon, nel film *Will Hunting – Genio ribelle*, 1997, di Gus Van Sant)

L'ossessione per la segretezza e la security delle organizzazioni di intelligence nordamericane – così come quella delle analoghe britanniche – è risaputa. La NSA spende da sola un terzo dell'intero budget dell'intelligence USA (66,8 miliardi di dollari nel 2015) per un'attività di sorveglianza di massa con la raccolta incontrollata di metadati riguardanti politici, imprese, semplici cittadini. I dubbi riguardano la liceità e la compatibilità con la democrazia di questo comportamento, nonché l'efficacia a prevenire atti di terrorismo sempre più minacciosi e diffusi.

La NSA, a differenza del suo corrispettivo britannico, ha generalmente una pessima reputazione presso tutti i media. Collerico, paranoico, disilluso il ventenne genio matematico Will Hunting (l'attore Matt Damon), quando gli si offre un promettente e ben remunerato lavoro come crittografo presso la NSA, risponde – nel film prima citato – con un'invettiva antimilitarista alla proposta, agendo contro il proprio interesse economico. La sua filippica snocciola tutti i principali guai del mondo, con la NSA che sembra esserne la causa prima, se non l'unica.

Un altro esempio è il film *Nemico pubblico* (1998) dove l'innocente protagonista, impersonato dall'attore Will Smith, viene perseguitato dalla NSA per fini non certamente commendevoli. Essa, peraltro, sembra fare di tutto per meritarsi questa nomea: basta pensare alle vicende di Edward Snowden, l'ex analista dell'NSA che, nel maggio del 2013, ha rivelato le pratiche dell'Agenzia di azioni capillari ed estese di intercettazioni e spionaggio rivolte tanto ad alleati quanto a nemici, tramite la sua rete mondiale di satelliti, fibre ottiche, server. Al di là dell'imbarazzo diplomatico, la giustificazione è che gli amici si controllano tra loro da millenni ("così fan tutti"), come dimostra la celebre vicenda Yardley-Stimson sull'apertura della corrispondenza altrui, riportata in [27] e ricordata in [1]. Lo spionaggio – oggi, più elegantemente, chiamato intelligence – non è certamente equiparabile alla diplomazia che André Maurois definiva "l'arte di esporre le ostilità con cortesia".

Tradizionalmente, l'ambiente accademico USA rivendica orgogliosamente autonomia e indipendenza dalle organizzazioni governative di intelligence. Per questa ragione, i risultati delle ricerche crittologiche ottenuti in ambito universitario vengono prontamente pubblicati, suscitando talora aspre reazioni polemiche da parte governativa per "superiori ragioni di sicurezza della nazione". I pur validi crittologi della NSA sono invece soggetti a stringenti vincoli di segretezza.

È bensì corretto osservare che a partire dal 2009, con l'amministrazione Obama, anche il Central Security Service (CSS) della NSA ha cominciato a mettere a disposizioni una gran mole di pubblicazioni e documenti inediti, d'interesse storico*.

Infine, un gustoso aneddoto sulla Seconda guerra mondiale, questa volta riguardante l'intelligence britannica e l'insigne giallista Agatha Christie, è ricordato in [1]. Al contrario dell'intelligence statunitense, quella britannica pare avere, in linea di massima, una più favorevole reputazione presso l'opinione pubblica e i media. Stranamente, perché sono gli USA che hanno coniato il patriottico motto "My country, wright or wrong" (del commodoro Stephen Decatur, 1779-1820): sembra quasi che i britannici, sempre molto pragmatici, abbiano fatta propria l'icastica espressione di amor patrio.

---

* Cfr. la sua politica di "Declassification and Transparency" in https://www.nsa.gov/public_info/declass/index.shtml.

Bibliografia

[1] Luvison, A. (2015). "La crittologia da arte a scienza: l'eredità di Shannon e Turing", *Mondo Digitale – Rassegna critica del settore ICT*, anno XIV, n. 60, 1-31, http://mondodigitale.aicanet.net/2015-5/articoli/03_crittologia_da_arte_a_scienza.pdf (ultimo accesso marzo 2016).

[2] Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet* (Nuova edizione), Scribner. Prima edizione (1967). Macmillan. Tr. it. parziale della prima edizione (1969). *La guerra dei codici. La storia dei codici segreti*, Mondadori.

[3] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday Books. Tr. it. (1999). *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Rizzoli.

[4] Massey, J.L. (2008). "A review of series on Arabic origins of cryptology", *Cryptologia*, vol. 32, n. 3, 280-283.

[5] VV. AA. (2016). Spotlight on "How Platforms Are Reshaping Business", *Harvard Business Review*, vol. 94, n. 4.

[6] Shannon, C.E. (1949). "Communications theory of secrecy systems", *Bell System Technical Journal*, vol. 48, n. 4, 656-715.

[7] Paar C., Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer.

[8] Simmons, G.J. (a cura di) (1992). C*ontemporary Cryptology: The Science of Information Integrity, IEEE* Press-Wiley.

[9] Peres, E. (2012). *È l'enigmistica, bellezza! Lettere e cifre per allenare la mente*, Ponte alle Grazie.

[10] Massey, J.L. (2001). "Cryptography – Science or magic?", MIT-EECS Colloquium, http://videolectures.net/mitworld_massey_csom/ (ultimo accesso marzo 2016).

[11] Massey, J.L. (1992). "Contemporary cryptology: An introduction", in [8], 1-39.

[12] Hellman, M.E. (1978). "An overview of public-key cryptography", *IEEE Communications Magazine*, vol. 16, n. 6, 24-31. Ristampa Id. (2002). *IEEE Communications Magazine 50th Anniversary Issue: Landmark 10 Papers*, vol. 40, n. 5, 42-49 [con una nuova'introduzione che, tuttavia, non cita neppure i lavori del GCHQ].

[13] Gardner, M. (1977). "Mathematical games: A new kind of cipher that would take millions of years to break", *Scientific American*, vol. 237, n. 2, 120-124.

[14] Strumia, A. (2003). *Le scienze e la pienezza della razionalità*, Cantagalli.

[15] Ellis, J.H. (1999). "The history of non-secret encryption" (Prefazione di Cliff Cocks), *Cryptologia*, vol. 23, n. 3, 267-27. [Il documento originale di Ellis è disponibile al link: https://web.archive.org/web/20030610193721/http://jya.com/ellisdoc.htm (ultimo accesso marzo 2016)].

[16] Mezzalama, M., Lioy, A., Metwalley, H. (2013). "Anatomia del malware", *Mondo Digitale – Rassegna critica del settore ICT*, vol. XII, n. 47, pp. 1-20, http://mondodigitale.aicanet.net/2013-3/articoli/02_Anatomiadelmalware.pdf (ultimo accesso marzo 2016).

[17] Goodman, M. (2015). Future Crimes: *A Journey to the Dark Side of Technology – and How to Survive It*, Bantam Press.

[18] Winnefeld, J.A., Jr., Kirchoff, C., Upton, D.M. (2015). "Cybersecurity's human factor: Lessons from the Pentagon", *Harvard Business Review*, vol. 93, n. 9, 86-95.

[19] Mosteller, F. (1987). *Fifty Challenging Problems in Probability with Solutions*, Dover.

[20] Harbert, T. (2012). "New king of security algorithms crowned", *IEEE Spectrum*, vol. 49, n. 12, 10-11.

[21] Quisquater, J.J. *et al.* (1990). "How to explain zero-knowledge protocols to your children", in Brassard, G. (a cura di), *Advances in Cryptology – CRYPTO '89: Proceedings (Lecture Notes in Computer Science 435*), 9th

Annual International Cryptology Conference, Santa Barbara, California, USA, 20-24 August 1989, Springer-Verlag, 628-631.

[22] Kaku, M. (2016). *Il cosmo di Einstein*, Codice Edizioni.

[23] Ratcliff, R.A. (2006). *Delusions of Intelligence. Enigma, Ultra, and the End of Secure Cyphers*, Cambridge University Press.

[24] VV. AA. (2016). Special Issue on "Big Data: Theoretical Aspects", *Proceedings of the IEEE*, vol. 104, n. 1; Special Issue on "Big Data: Applications", *ibid.*, in corso di pubblicazione.

[25] Lanier, J. (2014). "Il senso della privacy al tempo di Internet", *Le Scienze*, n. 546, 50-57.

[26] Bodei, R. (2016). *Limite*, il Mulino.

[27] Kahn, D. (2004). *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*, Yale University Press.

Biografia

Angelo Luvison è ingegnere elettronico dal 1969 (Politecnico di Torino), con successivi perfezionamenti in teoria statistica delle comunicazioni al MIT e in management aziendale all'INSEAD-CEDEP di Fontainebleau. Per oltre trent'anni in CSELT, ha svolto e coordinato ricerche in teoria delle comunicazioni, reti di fibre ottiche ad alta velocità, società dell'informazione, anche nell'ambito di progetti cooperativi internazionali. È stato professore di "Teoria dell'informazione e della trasmissione" all'Università di Torino. Ha ricoperto la posizione di segretario generale dell'AEIT. È stato consulente per la formazione permanente dei dirigenti d'azienda. Detiene sette brevetti ed è autore, o coautore, di quasi 200 lavori, uno dei quali è stato ripubblicato (2007) nel volume celebrativo *The Best of the Best* della IEEE Communications Society. È *Life Member* dell'IEEE e membro del Comitato scientifico di *Mondo Digitale*. Si occupa e scrive di temi di innovazione per le tecnologie informatiche e di telecomunicazioni (ICT).

Email: angelo.luvison@alice.it