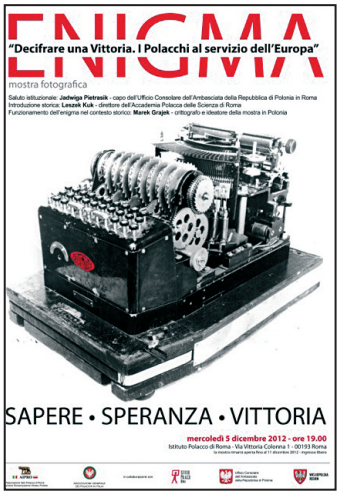
Enigma: decifrare una vittoria

di Giulia Lami, Carlo Mazza, Ottavio Giulio Rizzo



Dal 12 al 20 aprile 2012, il dipartimento di Matematica ha ospitato la mostra **Enigma: decifrare una vittoria. I polacchi (e la matematica) al servizio dell'Europa**, *sponsorizzata dal Consolato generale di Polonia in Milano, dalla regione Wielkopolska, dai dipartimenti di Matematica e Studi Storici e dal Progetto Lauree Scientifiche. Una dozzina di classi di scuole superiori lombarde ha frequentato i laboratori divulgativi costruiti intorno alla mostra, mentre un centinaio di persone ha assistito alla conferenza inaugurale in cui la storica Giulia Lami e i matematici Ottavio Rizzo e Carlo Mazza hanno parlato della storia e del funzionamento della macchina cifrante tedesca e dell'influenza che la sua decifrazione ebbe sul secolo scorso.*

Che cos'è la crittografia?

Per rispondere a questa domanda dobbiamo interpretarne l'etimologia (dal greco κρυπτός *nascosto*) non nel senso che è il messaggio ad essere nascosto — questa è la steganografia! — ma nel senso del nasconderne il significato: «*ut nullum verbum effici posset*» come scrive Svetonio (*Vita di Giulio Cesare*, 56) a proposito del crittosistema ideato da Cesare.

«La crittografia — è la definizione di Ron Rivest, la R di RSA — è comunicare alla presenza del nemico». Nascondere alla vista il contenuto di un messaggio è, a prima vista, la strategia più ovvia; in alcuni contesti è anche l'unica strategia sensata: in una dittatura, inviare un messaggio incomprensibile verso l'Occidente può essere motivo più che sufficiente per passare il resto dei propri giorni in una cella di sicurezza; con del semplice *software*, possiamo invece inserire un testo nella foto del nostro nipotino e inviarla per mail ad un cugino emigrato negli USA con la ragionevole speranza di rimanere sotto traccia.

Nascondere il messaggio, però, richiede una grande fiducia nel messaggero, fiducia che può essere ben posta, mal posta, o impossibile da porre. Supponiamo di inviare un messaggio via radio: chiunque potrà, senza alcun problema, ascoltare la nostra comunicazione! Questo era il problema fondamentale delle comunicazioni militari fra

le due guerre, è un problema serissimo ora che le comunicazioni *wi-fi* sono molto diffuse, è un problema molto serio con le comunicazioni via cavo — che si tratti di un cavo telegrafico che attraversi chilometri e chilometri di aperta campagna, o che si tratti di un cavo ethernet i cui pacchetti sono visibili da qualsiasi dispositivo collegato fisicamente ad esso —, è un problema serio se il messaggero può essere corrotto.

Non solo: la crittografia oggi viene usata anche per garantire l'autore di un messaggio (la firma digitale) così come la sua integrità o il momento in cui è stato redatto; diventa così possibile che il nemico sia una delle due parti che stanno comunicando. Immaginiamo, ad esempio, di poter fabbricare un ordine di vendita di azioni tale che — di fronte ad un magistrato — possa essere interpretato come un ordine di acquisto. In molti di questi casi, diventa addirittura necessario che il *contenuto* del messaggio sia pubblico.

Un *sistema crittografico* è un insieme di regole (algoritmi e protocollo) che permette prima di rendere irriconoscibile un testo (che sia il messaggio vero e proprio, una firma digitale da esso derivato o altro ancora) e poi di ricostruirlo in maniera univoca. Il più semplice sistema crittografico consiste nel sostituire, in maniera apparentemente casuale, un simbolo per ogni segno semantico: il codice Morse, per chi non lo conosce, è un sistema crittografico; così come una qualsiasi trasformazione che scambi in modo biunivoco le lettere dell'alfabeto.

Apparentemente — la storia della crittografia è costellata di idee che in apparenza funzionano — quest'ultimo è un ottimo sistema: le possibili trasformazioni fra le 26 lettere dell'alfabeto sono 26 (!): un numero di 27 cifre decimali, decisamente troppe perché sia possibile provare tutte le possibili trasformazioni allo scopo di ricostruire il messaggio originale. Eppure, sfruttando le ridondanze delle lingue naturali — quasi ogni parola italiana termina per 'a', 'e', 'i' oppure 'o'; le 't' compaiono spesso raddoppiate; la 'h' compare nel 90% dei casi preceduta dalla 'c' mentre la 'q' è praticamente sempre seguita dalla 'u'; ecc. ecc. — un crittografo esperto è capace di decifrare a colpo sicuro un messaggio di poche decine di lettere.

La soluzione a questo problema è dovuta a Leon Battista Alberti, che oltre a scoprire la prospettiva inventò l'idea di crittografia polialfabetica: lettere in posizione diversa vengono cifrate in modo diverso! Ad esempio, possiamo decidere di cifrare tutte le lettere di posizione pari in un modo, tutte quelle in posizione dispari in un altro (Claude Shannon dimostrò matematicamente nel 1949 che una generalizzazione opportuna di questo principio — difficilmente realizzabile nella pratica — è l'unico crittosistema perfettamente sicuro).

Un'altra invenzione fondamentale per la storia della crittografia è dovuta all'Alberti: la macchina cifrante. Il suo disco, composto da due corone in grado di ruotare una intorno all'altra, permette di cifrare e decifrare più semplicemente e rapidamente.

Avanziamo rapidamente a fine '800: il telegrafo permette di trasmettere rapidamente e molto economicamente messaggi a migliaia di chilometri di distanza. Peccato solo che tali messaggi siano facilmente conoscibili: basta arrampicarsi su un palo in mezzo alla campagna o — per i più pigri — allungare una mancia sufficiente all'impiegato del telegrafo.

Lo sviluppo della crittografia subisce un forte impulso ed è Auguste Kerckhoffs a formalizzare il principio eponimo: «La sicurezza di un sistema deve dipendere solo dalla chiave, e non dalla segretezza del sistema stesso». Vedremo come l'aver voluto ignorare questo principio è stata la principale causa del fallimento di Enigma (l'esercito tedesco è però in ottima compagnia: ci sono cascati tra gli altri anche gli autori dello standard cellulare GSM, gli estensori dei protocolli anticopia di DVD e Blue-ray, i realizzatori di macchine per il voto elettronico).

Con l'invenzione della radio da parte di Marconi nel 1895 la crittografia diventa fondamentale: qualsiasi comunicazione può essere ascoltata da chiunque in qualsiasi parte del globo! Nella prima guerra mondiale, la decifrazione francese del codice ADFGVX ha pesanti ripercussioni sull'efficacia dell'Offensiva di Primavera delle truppe tedesche.

Quando nel dopoguerra vennero sviluppate le prime macchine cifranti elettromeccaniche, gli eserciti ne furono subito interessati: oltre alla rapidità operativa, offrivano una ragionevole compattezza. Soprattutto, permettevano facilmente di avere una quantità *gigantesca* di chiavi.

Il funzionamento di Enigma

Enigma è una macchina elettromeccanica: esternamente è una specie di telescrivente in cui, schiacciando un tasto, s'illumina una lettera. Internamente è costituita da tre rotori che, in contatto elettrico fra di loro, girano ad ogni passaggio. Ogni volta che viene schiacciato un tasto, viene chiuso un circuito elettrico che attraverso i tre rotori arriva ad accendere la lampadina corrispondente alla lettera cifrata: poiché i rotori girano, ogni lettera è cifrata in modo totalmente scorrelato dalla precedente. La costruzione interna, che usava un riflettore in modo da far passare due volte i segnali all'interno dei rotori, faceva sì che la macchina fosse completamente simmetrica: cifrando il testo cifrato si otteneva il testo in chiaro.

I tre rotori potevano essere disposti in qualsiasi ordine, e la loro posizione iniziale poteva variare fra le 26 lettere dell'alfabeto: questo offre $3! \times 26^3 = 105\,456$ diverse combinazioni, non poche, ma neanche tantissime.

Per aumentare significativamente le possibili chiavi, venne implementato uno scambiatore: quattro cavetti collegavano su un *plugboard* quattro coppie di lettere. Se, ad esempio, la A era collegata alla F, ogni volta che veniva schiacciato il tasto A sulla tastiera, la macchina avrebbe visto una F. In questo modo vengono aggiunte $26 \times 25 \times \cdots \times 19 = 62\,990\,928\,000$ combinazioni, portandone il totale ad un numero a 16 cifre.

Questa era la macchina degli anni Venti: nel corso della seconda guerra mondiale si arrivò a sei rotori e 10 coppie di scambiatori, portanto così le chiavi a più di 10^{30} eppure…

Eppure… la grandissima quantità di chiavi date dallo scambiatore erano assolutamente irrilevanti: si trattava di un banale cifrario monoalfabetico (*ogni* A era sostituita da una F); rimanevano solo le 105 456 possibili combinazioni dei rotori, abbastanza poche da poter essere affrontate con l'ausilio di macchine.

L'unica vera difficoltà nel decifrare Enigma stava nello scoprire la configurazione interna dei rotori: una volta ottenuta questa tramite la soluzione di complicate equazioni matematiche (possibilmente aiutate da operazioni di intelligence o banali errori degli operatori tedeschi) la sicurezza delle macchine era totalmente compromessa.

Il grande contributo di M. Rejewski, e degli altri matematici polacchi del Biuro Szyfrów, fu la comprensione della struttura della macchina Enigma da un punto di vista astratto: in questo modo non solo riuscirono a ricostruire la configurazione interna della macchina, ma misero in grado gli Inglesi di adattare le loro tecniche alle nuove macchine Enigma prodotte durante la guerra.

Potete trovare al seguente collegamento[1] (oppure qui[2]) le diapositive della presentazione "La matematica di Enigma" tenuta nel giorno dell'inaugurazione della mostra presso il Dipartimento di Matematica "Federigo Enriques" dell'Università di Milano. Nella prima parte della presentazione esploriamo in grande generalità il problema della cifratura e decifratura dei messaggi, e illustriamo il motivo della grande fiducia dei tedeschi nella macchina Enigma, la cui decodifica dei messaggi in maniera naif risulta praticamente impossibile, o meglio, impossibile da un punto di vista pratico. Proseguendo, mostriamo come l'utilizzo di concetti e tecniche introdotte da M. Rejewski, che oggigiorno vengono esplorati al primo anno del corso di laurea in Matematica, riuscirono a far diventare il problema da impossibile a (solo) molto difficile e permisero ai matematici polacchi di poter riprodurre una macchina Enigma avendo a disposizione solo i messaggi crittografati da essa.

La storia di Enigma

La storia di Enigma è anche la storia della crittografia polacca, che ebbe un ruolo fondamentale non solo nella vittoria degli Alleati nella seconda guerra mondiale, ma già nella vittoria dei polacchi sui bolscevichi nella guerra del 1919-1920, conclusasi con la pace di Riga del 1921.

[1] http://goo.gl/dYyS7
[2] http://users.unimi.it/mazza/wp-content/uploads/Presentazione-per-mostra-Enigma.pdf

I polacchi già negli anni Venti incominciarono ad applicarsi scientificamente alla crittografia, rendendosi presto conto che i tedeschi avevano messo a punto un sistema meccanico per codificare i loro messaggi radio, grazie ad una versione modificata della macchina cifrante elettronica portatile Enigma, inventata, a fini commerciali, dall'ingegnere tedesco Arthur Scherbius.

Il comandante Gwido Langer e il capitano Maksymilian Ciężki, responsabili dell'ufficio cifra polacco, ebbero allora l'idea di tenere un corso di crittografia alla Facoltà di matematica di Poznań, da cui emersero alcuni veri talenti, come Marian Rejewski, Jerzy Różycki e Henryk Zygalski. Nel 1932 il capitano Maksymilian Ciężki li trasferì a Varsavia e proprio a Rejewski rivelò che si trattava di capire come funzionasse il sistema di cifratura di Enigma. Rejewski si applicò allo studio del problema, creando un modello matematico della macchina che permettesse di ricostruirla e di riprodurre le chiavi per decifrare i dispacci di parte tedesca, anche perché i tedeschi perfezionavano continuamente le loro trasmissioni. Così nel 1935 i polacchi costruirono una macchina denominata ciclometro, cui fece seguito quella denominata la bomba di Rejewski, mentre Zygalski concepiva schede perforate che, individuando particolarità della cifratura di Enigma, permettevano di trovare la chiave di cifratura utilizzata in un dato giorno.

Alla vigilia della guerra i crittografi polacchi erano gli unici a possedere il *know-how* indispensabile per affrontare Enigma. Nel luglio del 1939, in un centro segreto dei servizi d'informazione a Pyry, vicino a Varsavia, Rejewski ed i suoi collaboratori illustrarono a francesi e inglesi i risultati del loro lavoro: le basi matematiche del sistema, l'individuazione delle chiavi, gli apparecchi di decrittaggio ormai messi a punto. I polacchi fornirono alle delegazioni tutta la documentazione nonché copia della macchina. Quando la Polonia fu invasa congiuntamente da sovietici e nazisti, la maggioranza del gruppo dei crittografi polacchi si trasferì in Francia, ma nel 1943 una parte di loro cadde in mano tedesca, finendo nei campi di prigionia. Purtroppo da tempo i crittografi polacchi erano stati emarginati: è questo un episodio significativo di una certa arroganza che i polacchi hanno dovuto subire dai loro tradizionali alleati. Per fortuna delle sorti della guerra, gli inglesi avevano continuato con serietà il lavoro iniziato dai polacchi. Anch'essi erano giunti alla conclusione che bisognava avvalersi del lavoro dei matematici. Già il 4 settembre 1939 giungeva a Bletchley Park il matematico e logico di Cambridge Alan Turing, che elaborava la sua famosa e vincente "bomba" da sfruttare contro Enigma.

I polacchi insomma vennero messi da parte dagli inglesi, nonostante il loro Governo finisse in esilio proprio in Inghilterra; e vennero traditi dai francesi, tanto che del loro contributo si tacque per anni. Basti pensare al destino di Langer e Ciężki, i quali, liberati dalla prigionia, nel 1945 giunsero a Londra, ma furono ignorati, tanto da morire in povertà e solitudine; a Rejewski e Zigalski che seppero di Bletchey Park solo trent'anni dopo. Anche Turing però ebbe un destino amaro: nonostante i suoi meriti, sulla base di un'accusa di omosessualità lo si volle obbligare per legge alla castrazione

chimica. Turing si tolse la vita, sconvolto da quel tipo di cure coatte e dai loro effetti deleteri. Di recente si sono avute le scuse ufficiali espresse da Gordon Brown con queste parole: «Così, per conto del governo britannico, e di tutti coloro che vivono liberi grazie al lavoro di Alan, sono orgoglioso di dire: ci dispiace, avresti meritato di meglio».

Una spiegazione sul silenzio che ha circondato a lungo sia la vicenda di Enigma sia il contributo polacco alla vittoria, è stata fornita da uno dei protagonisti dell'impresa di Bletchley Park, Sir Philip Stuart Milner-Barry, celebre giocatore di scacchi inglese, che fu a capo dal settembre del 1943 dello HUT 6, la sezione di Bletchley Park responsabile di decifrare i messaggi di Enigma che riguardavano l'esercito e l'aviazione tedeschi.

In una recensione del 1986 su "The international history review" (vol. 8, n. 1, pp. 144-147), al libro di Władysław Kozaczuk del 1979, tradotto in inglese nel 1984 con il titolo *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two* (Frederick, Maryland, University Publications of America) si rammarica del risentimento che l'autore mostra proprio a proposito della sottovalutazione del ruolo dei polacchi nella decrittazione di Enigma. Egli sostiene che nessuno che sia stato legato ad Enigma durante la guerra in Inghilterra o altrove ha il minimo dubbio sull'importanza del contributo polacco fino al 1939.

Milner-Barry loda il coraggio e la determinazione con cui dopo il 1939 il piccolo contingente polacco cercò di rimanere in gioco, una volta in Francia, ma sottolinea che fino a tutto il 1973, quando furono pubblicati i libri di altri protagonisti della guerra d'intelligence quali Winterbotham (F. Winterbotham, *The Ultra Secret*, London, Weidenfeld and Nicolson, 1974) e Bertrand (G. Bertrand, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Paris, Librairie Plon, 1973) non fu riconosciuto il contributo di nessuno, tanto più che il fatto stesso che Bletchley Park leggeva Enigma durante la guerra era un segreto strettamente preservato. Ancora nel 1986 egli sosteneva che non si poteva affrontare il tema delle tecniche criptoanalitiche adottate da Hut 6 e Hut 8 (la sezione di Bletchley Park che si occupava della marina tedesca) per le disposizioni restrittive che vigevano in Inghilterra, come invece aveva fatto, parzialmente, il suo collega G. Welchman nel suo *The Hut six story* (G. Welchman, *The Hut Six Story: Breaking the Enigma Codes*, London, Allen Lane & New York, McGraw-Hill, 1982) grazie al fatto d'essere diventato ormai cittadino americano.

Ora, come dimostra il monumento eretto a Poznań ai matematici polacchi, il tempo del silenzio è finito: le complesse vicende che circondano Enigma e che fanno parte della storia dello spionaggio durante la seconda guerra mondiale possono, in buona parte, essere studiate anche con il supporto di documenti nuovi, come ha mostrato Jan Medrala, ricostruendo l'avventura umana "*prestigieuse et dramatique*" dei crittografi polacchi[3].

[3] www.bibliotheque-polonaise-paris-shlp.fr/medias/enigma.pdf.

Giulia Lami, è professore ordinario di Storia dei Paesi slavi presso l'Università degli Studi di Milano. Membro di molte commissioni e associazioni internazionali, le sue pubblicazioni riguardano la storia e la storiografia dell'Europa centro-orientale in epoca moderna e contemporanea. Tra queste si possono ricordare da ultimo per la casa ed. Cuem di Milano: *La questione ucraina fra '800 e '900*, nel 2005; *Ucraina 1921-1956*, nel 2008, e, a sua cura, *1905: L'altra rivoluzione russa*, nel 2007. A breve uscirà presso la casa editrice Honoré Champion *L'Europe centrale et orientale au XIXe siècle d'après les voyages du romancier et journaliste suisse Victor Tissot*.

Carlo Mazza nasce a Genova dove consegue la Laurea in Matematica. Continua gli studi per il Ph.D. in Matematica presso la Rutgers University, a New Brunswick nel New Jersey (Stati Uniti). Prosegue con una borsa post dottorato presso l'Universitè Paris 7 a Parigi (Francia) e presso lo Institute for Advanced Study a Princeton, New Jersey, e durante quest'ultimo periodo porta a completamento la stesura del libro *Lecture Notes on Motivic Cohomology* in collaborazione col prof. Charles Weibel e il prof. Vladimir Voevodsky (pubblicato dalla American Mathematical Society come secondo volume dei Clay Mathematica Monographs nel 2006). È attualmente ricercatore presso il Dipartimento di Matematica "Federigo Enriques" dell'Università di Milano e continua lo studio dei motivi di Grothendeick e Voevodsky, e delle applicazioni alla geometria algebrica. Il suo sito web è **http://users.unimi.it/mazza**.

Ottavio Giulio Rizzo si è laureato in matematica a Pavia nel 1993, dottorato alla Brown University (Providence, Rhode Island, USA) nel 1997 con una tesi di geometria aritmetica. È stato *visiting professor* alla Queen's University di Kingston, Ontario e per due anni ha avuto una borsa post-dottorato dell'UE presso l'università di Rennes 1, in Bretagna. Dal 2000 è ricercatore di geometria presso l'università degli studi di Milano dove si occupa di applicazioni alla crittografia della geometria aritmetica e di utilizzo dei calcolatori nella didattica della matematica. Vive a Pavia.