INDAGINE SU ENIGMA

di Claire Ellis

http://plus.maths.org.uk/issue34/features/ellis/
Traduzione di Eleonora Bazzo

Già dal tempo degli antichi Greci, gli eserciti in guerra cifravano le loro comunicazioni, nel tentativo di mantenere segreti i loro piani di battaglia. Di conseguenza, mentre da una parte si inventavano nuovi e ingegnosi metodi per cifrare i propri messaggi, dall'altra i nemici tentavano di spezzare i nuovi codici. In tal modo, nel tempo, i codici ed i sistemi di cifratura sono diventati sempre più complessi e difficili da interpretare e si è così innescata una battaglia intellettuale tra gli inventori dei codici e quelli che li volevano infrangere. Il confronto tra le intelligenze non fu mai così serrato come durante la seconda guerra mondiale, quando i Tedeschi utilizzarono la famosa macchina **Enigma** – che ritenevano indecifrabile – per codificare i messaggi, mentre gli Alleati lavoravano a **Bletchley Park** per forzare il loro codice.

LA NASCITA DI UN ENIGMA

Fino alla seconda guerra mondiale, le forme più diffuse di crittografia usavano semplici tecniche di carta e matita. Ma gli addetti alla sicurezza di entrambi gli schieramenti, già durante la prima guerra mondiale, sentirono l'esigenza di un maggiore livello di segretezza, da conseguire con metodi più avanzati di cifratura. Sia gli Alleati che i paesi dell'Asse cercarono nuovi metodi per cifrare i messaggi – per trovare un procedimento che fornisse una sicurezza totale.

Nel 1915, due ufficiali della marina olandese inventarono una nuova macchina per cifrare i messaggi. E questa è divenuta una delle più famose di tutti i tempi: la macchina cifrante Enigma. Arthur Scherbius, un uomo d'affari tedesco, la brevettò nel 1918 e cominciò a venderla alle banche e alle aziende. Il posto di Enigma nella storia, però, venne garantito nel 1924, quando le forze armate tedesche iniziarono ad utilizzarne una versione adattata alle esigenze militari per cifrare le loro comunicazioni. E continuarono a fare affidamento su questa macchina anche durante la seconda guerra mondiale, credendo che fosse assolutamente sicura.

Fig. 1 Soldati tedeschi al lavoro con Enigma durante la seconda guerra mondiale.

COME FUNZIONA LA MACCHINA ENIGMA

Quando un carattere di un testo in chiaro viene battuto sulla tastiera, una corrente elettrica attraversa i vari elementi codificatori e fa accendere una lettera del testo cifrato sul "pannello luminoso". Ma ciò che rendeva Enigma così speciale era il fatto che ogni volta che una lettera veniva battuta sulla tastiera, le parti mobili della macchina ruotavano, cambiando la loro posizione in modo che una successiva pressione del tasto corrispondente alla stessa lettera quasi certamente sarebbe stata cifrata in altro modo. Ciò significa che non era possibile impiegare metodi tradizionali per tentare di forzare la famigerata cifratura.
Per rendere le cose ancor più difficili, alcune parti mobili della macchina si potevano posizionare in diversi modi ed ogni regolazione produceva una stringa di lettere cifrate sempre diversa. A meno che non si conoscessero le esatte impostazioni della macchina, non sarebbe stato possibile decifrare i messaggi.

IN QUANTI MODI E' POSSIBILE INIZIALIZZARE UNA MACCHINA ENIGMA?

Figura 2 una rappresentazione schematica di una macchina Enigma.

Figura 3 Un rotore della macchina Enigma.

Rotori mobili
Le macchine Enigma nella versione per l'esercito avevano tre "dischi" rotanti o "rotori" che potevano essere estratti e cambiati. Il primo compito per un operatore di Enigma era di decidere in quale posizione andava impostato ogni singolo rotore. C'erano cinque rotori tra cui scegliere e che potevano essere inseriti nei tre alloggiamenti di Enigma.

> Domanda n. 1: Quanti sono i possibili modi in cui posizionare 5 rotori nei tre alloggiamenti di Enigma?
> Per il primo alloggiamento si può scegliere uno qualunque dei 5 rotori. Per il secondo uno dei 4 rimasti. Per l'ultimo si può scegliere uno tra gli ultimi 3. Ci sono quindi 5x4x3= 60 modi per posizionare 5 rotori nei 3 alloggiamenti.

Le posizioni iniziali dei rotori

> Domanda n. 2: Una volta che è stato scelto l'ordine dei rotori, quante sono le loro possibili posizioni iniziali?
> Poiché ci sono 26 lettere dell'alfabeto, ciascuno dei tre rotori potrebbe essere inizializzato in una qualunque delle 26 differenti posizioni. Così si ottiene un totale di 26x26x26 = 17.576 diverse posizioni iniziali.

Le regolazioni del disco
Ogni volta che una lettera viene battuta sulla tastiera, il rotore di estrema destra avanza di una posizione. Una volta completato un giro (il rotore si è spostato di 26 posizioni), viene dato un impulso al rotore centrale, che avanza di una posizione. Quando viene completato un ulteriore giro, viene dato un nuovo impulso al rotore centrale, che avanza di un'altra posizione. Quando anche il rotore centrale ha

completato un giro, viene inviato un segnale al rotore di sinistra che ruota a sua volta. Il momento in cui un rotore invia un impulso al rotore posto a fianco potrebbe essere variato. Questa operazione è chiamata "impostazione del disco".

> Domanda n. 3: Quante sono le possibili "impostazioni del disco" per un Enigma dell'esercito?
> Il primo disco può essere impostato in una delle 26 posizioni, come pure il secondo, così ci sono 26x26=676 modi per posizionare i 2 dischi in un Enigma dell'esercito, a 3 rotori.

Pannello dei collegamenti

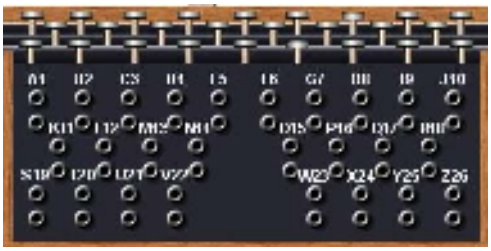

Figura 4 Una rappresentazione schematica del pannello dei collegamenti.

Nella parte anteriore della macchina c'era un'altra sezione denominata "pannello dei collegamenti". Enigma aveva parecchi cavi, con uno spinotto a entrambe le estremità che servivano per collegare tra loro coppie di lettere. Se A era collegata a B allora, alla pressione sulla tastiera della lettera A, la corrente avrebbe seguito il percorso che normalmente era associato alla lettera B e viceversa. Le macchine Enigma avevano 10 cavi con cui poter collegare coppie di lettere.

Domanda n. 4: Quanti modi ci sono per collegare coppie di lettere sulla macchina Enigma?

> La risposta è che circa di 150.000.000.000.000 – cioè 150 milioni di milioni – di possibili combinazioni di 10 accoppiamenti tra le 26 lettere sul pannello dei collegamenti. La matematica dietro a questo calcolo è complessa, ma una spiegazione esaustiva è fornita al sito http://www.codesandciphers.co.uk/enigma/steckercount.htm, una pagina tratta dal sito di Tony Sale.

Di conseguenza, il numero totale dei possibili modi in cui una macchina standard Enigma dell'esercito poteva essere impostata era di:

60x17.576x676x150.738.274.937.250

che è circa 158 milioni di milioni di milioni.

DECIFRARE[1] ENIGMA

Quando Enigma viene utilizzata, è la stessa macchina Enigma l'algoritmo; il modo in cui viene inizializzata è la chiave. Proprio come un qualunque altro tipo di cifrario, a condizione che il destinatario ne conosca la chiave, il processo di decodifica di un messaggio cifrato con Enigma è incredibilmente semplice. Un soldato tedesco che riceveva un messaggio cifrato doveva semplicemente batterne le lettere sulla tastiera della propria Enigma. Se la sua macchina era stata impostata esattamente come quella del mittente del messaggio, allora le lettere del testo in chiaro si sarebbero illuminate sul pannello.
Tuttavia, come con qualunque altro sistema cifrante, se non si conosce la chiave, è veramente difficile decrittare un messaggio - anche se si conosce quale sia stato il sistema usato per cifrarlo.
I Britannici avevano installato stazioni di ascolto (denominate Y Station) in tutta la Gran Bretagna per poter intercettare le comunicazioni dei militari tedeschi. Anche se gli Alleati erano riusciti a procurarsi macchine Enigma, per decrittare i messaggi intercettati avevano bisogno di conoscere la chiave. Per rendere il più difficile possibile la decifrazione dei messaggi, i Tedeschi cambiavano la chiave ogni giorno, resettando puntualmente le loro macchine Enigma alla mezzanotte di ogni giorno.

CONCORDARE LA CHIAVE

Figura 5 Un foglio mensile delle chiavi.

Agli operatori addetti alla cifratura ogni mese veniva distribuito un foglio con le chiavi che servivano per preparare le loro macchine Enigma, ogni giorno del mese. C'era un evidente problema di sicurezza: se gli Alleati avessero recuperato un foglio delle chiavi, sarebbero stati in grado di leggere i messaggi di Enigma.
Per questo motivo, i fogli delle chiavi erano custoditi con estrema attenzione ed erano anche stampati con inchiostro solubile. Quando si presentava il rischio che un foglio delle chiavi potesse cadere nelle mani degli Alleati, i soldati tedeschi lo dovevano gettare in acqua, eliminando così tutte le informazioni.
I Tedeschi avevano molta fiducia nell'efficacia della configurazione di Enigma, poiché era impossibile individuare una chiave tra i miliardi di miliardi di possibili chiavi utilizzabili ogni giorno. Finché gli Alleati non fossero riusciti a procurarsi il foglio delle chiavi, le comunicazioni tedesche sarebbero rimaste sicure.

IL LAVORO A BLETCHLEY PARK

Nell'agosto del 1939 i Britannici costituirono la scuola dei codici e dei cifrari a **Bletchley Park** nel Buckinghamshire. Le persone chiamate a lavorare al progetto, erano esperti in molti settori diversi. C'erano esperti nella violazione dei codici, ufficiali dei servizi segreti, matematici, scienziati, esperti di parole crociate, giocatori internazionali di scacchi, attrici e perfino astrologi.

Figura 6 Bletchley Park

Fortunatamente per gli addetti britannici alla decodifica dei messaggi cifrati, negli anni che precedettero la guerra, in Polonia si erano già sperimentate varie tecniche per forzare Enigma. Poco prima dell'invasione tedesca della Polonia, il loro lavoro venne condiviso con gli alleati britannici. Il governo della Polonia fu il primo a impiegare i matematici come decrittatori e le menti logiche dei matematici dimostrarono proprio quello che era necessario sapere per affrontare Enigma
Questo vantaggio essenziale dei Polacchi, unito alle abilità per la risoluzione di problemi e le capacità intuitive delle reclute di Bletchley, portarono alla decifratura del codice Enigma all'inizio del 1940: una tecnica particolare, per decifrare Enigma, aveva avuto finalmente successo. I decrittatori britannici lavorarono in squadre, 24 ore su 24, per tutta la durata della guerra, usando carta e matita, come pure nuove tecnologie meccaniche appena inventate per elaborare specifiche impostazioni di Enigma, per ogni singolo giorno.

Inconsapevolmente gli stessi Tedeschi aiutarono i Britannici a decifrare Enigma. Per esempio:

- I messaggi spesso cominciavano con lo stesso testo di apertura – molti cominciavano con la parola *Spruchnummer* (messaggio numero), e molti messaggi dell'aeronautica cominciavano con la frase *An die Gruppe* (al gruppo).
- Messaggi cifrati spesso riportavano informazioni di routine come rapporti sul tempo e frasi quali *Kienebesondere Ereignisse* (niente da segnalare).
- I messaggi spesso terminavano con *Heil Hitler*!
- I Tedeschi spesso trasmettevano più di una volta lo stesso messaggio, con una diversa versione di cifratura.

Queste disattenzioni fornirono ai decifratori gli indizi, denominati *cribs* (mangiatoie), sul modo in cui Enigma era stato impostato quel giorno. Questi *cribs* erano essenziali per forzare i cifrari. Per esempio, senza un *crib*, ancora oggi si sarebbero impiegati parecchi mesi per decifrare un testo lungo una pagina formato A4, utilizzando un PC moderno, con procedimenti di verifica e di controllo degli errori.
Tuttavia, i *cribs* da soli non erano sufficienti. I decrittatori di Bletchley Park svilupparono nuove procedure e algoritmi per la determinazione della messa a punto di Enigma e svilupparono anche dispositivi di calcolo elettronico per implementare questi metodi.
Oggi gli storici ritengono che il lavoro dei decrittatori a Bletchley Park abbia ridotto la guerra di due anni.

EROI DIMENTICATI

Tra i più famosi violatori di codici di Bletchley Park c'era un matematico dell'università di Cambridge, Alan Turing che molti già allora consideravano un genio. Svolse un ruolo guida nel forzare il più complesso cifrario dell'Enigma navale (denominato *shark* - squalo) e contemporaneamente definì i principi che sono alla base del moderno calcolatore.
Malgrado il loro notevole lavoro, tuttavia, per molto tempo nessuno dei decifratori di codici della seconda guerra mondiale ha ricevuto pubblici riconoscimenti, come sarebbe stato giusto. Per garantire la sicurezza britannica, la forzatura di Enigma è rimasto un segreto, molto protetto, per tutta la durata della guerra e per i successivi 30 anni. Alla gente che aveva lavorato a Bletchley Park è stato proibito di parlare di quello che avevano fatto e, di conseguenza, il loro contributo determinante per la soluzione della guerra è stato completamente dimenticato. Ma in questi ultimi 30 anni molte informazioni sull'incredibile storia di Bletchley Park sono state rese note.
Tragicamente tuttavia, per qualcuno i ringraziamenti arrivano troppo tardi. Alan Turing si suicidò prima che gli fosse pubblicamente riconosciuta la sua straordinaria parte nella guerra e prima che i suoi contributi alla scienza della cifratura e decifrazione fossero completamente capiti.
Il governo britannico ha ancora in funzione un reparto di decifrazione alla "Direzione del Ministero delle Comunicazioni" (GCHQ) in Cheltenham. Fa sempre affidamento sui matematici per le loro abilità e per la loro capacità logica nella soluzione dei problemi: GCHQ vanta la più alta concentrazione di matematici puri del paese. Gli odierni codici segreti sono molto più sofisticati della cifrante Enigma e la loro resistenza risiede nell'impossibilità di scomporre i grandi numeri in fattori, così oggi, con i timori per il terrorismo globale, il ruolo dei nostri decrittatori di codici risulta tanto importante quanto quello svolto durante la seconda guerra mondiale.

MAGGIORI INFORMAZIONI

- Il progetto Enigma (http://www.mmp.maths.org/projects/enigma.html):
  Il MMP (Millennium Mathematics Project) prevede la possibilità di portare una vera macchina Enigma della seconda guerra mondiale, codici e cifrari in una scuola.
- Bletchley Park (http://www.bletchleypark.org.uk/):

Scoprire gli eroi della seconda guerra mondiale che decrittarono i codici e conoscere le informazioni sul forzamento di Enigma. Bletchley Park ora è un museo e le informazioni sulla visita possono anche essere trovate sul loro sito web.

- NRICH Matematica:
  L'edizione del marzo 2004 (che è disponibile attraverso questo link http://www.nrich.maths.org/public/index.php) è interamente dedicata a differenti codici segreti e ad alcuni problemi da risolvere.
- Museo Nazionale della Crittografia (http://www.nsa.gov/museum/):
  Il Museo di Crittografia dell'Agenzia di Sicurezza Nazionale degli Stati Uniti.
- Angolo della crittografia di Simon Singh (http://www.simonsingh.net/Crypto_Corner.html):
  Informazioni su una miriade di codici differenti. La storia della sfida della cifratura sul libro The Code Book: chi l'ha vinta e come. Link con altri siti di crittografia. Seguire il link per la "Black Chamber" (camera oscura) per trovare problemi in linea e gli strumenti per decifrare. E' possibile anche scaricare liberamente copie del "The Code Book".
- Memorial di Alan Turing (http://www.btinternet.com/~glynhughes/sculpture/turing.htm):
  Informazioni sulla statua commemorativa di Alan Turing a Manchester.
- Codici e cifrari (http://www.codesandciphers.co.uk/):
  Tutto ciò che si desidera conoscere sui codici e sui cifrari della seconda guerra mondiale.

---

[1]In ogni cifratura ci sono due parti che bisogna conoscere per decifrare i messaggi:
Cifra = Algoritmo + Chiave
dove un "**Algoritmo**" è, in questo caso, un generico metodo di cifratura, per esempio "cambia ogni lettera con un simbolo", oppure "mescola tutte le lettere in modo circolare". Una "**Chiave**" è il particolare modo di cifrare un messaggio in quel momento, ad esempio "cambia A con $, B con &", oppure "sposta davanti l'ultima lettera di ogni parola".