La crittografia

Una breve storia della scienza che codifica e decodifica i messaggi segreti

La crittografia nasce nel momento in cui comincia la comunicazione fra gli uomini: è insito nella natura umana il desiderio di tenere segrete certe informazioni o avvenimenti, entro un gruppo limitato di persone, senza che il contenuto sia evidente per tutti.
Per secoli i messaggi in codice sono controllati dai governi, usati nelle guerre, applicati negli scambi diplomatici e nello spionaggio. Con il progresso tecnologico odierno, anche i privati cittadini possono disporre di sistemi semplici di cifratura e il boom delle telecomunicazioni, con l'introduzione delle operazioni di pagamento e di esecuzione di operazioni finanziarie su world wide web (www) ha reso indispensabile la crittologia e le sue applicazioni.
Il primo codice cifrato conosciuto è una iscrizione del 1900 a.C. (avanti Cristo), incisa su una pietra da uno scriba egiziano in onore del suo faraone; una altro antico codice cifrato tenta di nascondere un segreto: è riportato su tavoletta risalente al 1500 a.C. ritrovata lungo le sponde del Tigri, che contiene la formula segreta per smaltare la terracotta; anche gli antichi Greci avevano particolari sistemi di codifica dei messaggi. A Sparta, ad esempio per cifrare i messaggi tra le legioni si usava uno strumento chiamato scitala. Lo scitala era un bastone al quale si avvolgeva un nastro di cuoio su cui si scriveva il messaggio: quando il nastro era arrotolato lungo il bastone il messaggio appariva chiaro e leggibile mentre quando era srotolato appariva indecifrabile; ogni generale aveva un bastone con le stesse dimensioni, con il quale leggeva i messaggi scritti sulla striscia di cuoio.
Giulio Cesare cifrava i suoi comunicati militari cambiando ogni lettera del messaggio con la sua corrispettiva terza lettera seguente dell'alfabeto. I suoi più stretti collaboratori militari ovviamente dovevano essere a conoscenza del metodo di cifratura (la chiave) usata da Cesare per poter ricostruire il messaggio originale.
Dopo la caduta dell'impero Romano la crittografia europea cadde in un periodo di oblio che durò circa 1000 anni, ma la scienza della codifica delle informazioni fu sviluppata con il progresso della civiltà araba. Nel 900 d.C. l'espansione musulmana è al suo massimo, non solo per l'espansione territoriale, ma anche dal punto di vista culturale; in ambito matematico quindi si studiano anche problemi di crittografia; gli Arabi inventano un nuovo codice crittografico, aggiungendo alle lettere anche i numeri e i simboli.
In Europa la crittografia riprende il suo progresso durante il **1400**. In questo periodo, l'architetto ***Leon Battista Alberti*** inventa un ingegnoso metodo per creare messaggi criptati: esso consisteva in due dischi concentrici, uno fisso con le lettere maiuscole e alcuni numeri e di uno mobile con le lettere minuscole: ruotando il disco mobile, si otteneva una possibile codifica dei messaggi, che associava alle lettere reali (quelle maiuscole sul disco fisso) quelle da sostituire nella riscrittura del messaggio in codice (minuscole, sul disco mobile). Nel **1586** ***Blaise de Vigenere*** perfeziona e sistema l'invenzione di Leon Battista Alberti creando una griglia di 26 alfabeti cifranti in ognuno dei quali è presente lo scarto di una lettera: per decifrare i messaggi cifrati, basta conoscere la parola chiave.
Nel 1700 tutti i palazzi di governo europei hanno un stanza segreta, un cento operativo dove si decriptano i messaggi e si raccolgono informazioni, ma la vera rivoluzione nel campo della crittografia deve ancora avvenire. Con l'invenzione del telegrafo la scienza della crittologia aumenta ancor più

la sua importanza, e ancor di più ciò avviene dopo l'invenzione della radio, lo strumento ha rivoluzionato la comunicazione nel Ventesimo Secolo.
Le possibilità che offriva la nuova invenzione non sfuggì ai comandanti militari: la rapidità che i nuovi mezzi di comunicazione offrivano nelle comunicazioni degli ordini aumentava l'efficacia delle operazioni di guerra. Allo scoppio della Prima Guerra Mondiale, lo scambio delle informazioni in ambito militare rende quindi necessario lo studio di nuovi sistemi di codifica, sempre più difficili da decifrare, perché il nemico è sempre più efficace nella scoperta del contenuto dei messaggi in codice.
Il 5 agosto 1904 i sommozzatori inglesi tagliano i cavi sottomarini per le comunicazioni telefoniche dei Tedeschi nell'Atlantico del Nord. Gli inglesi volevano rendere più difficili le comunicazioni per la Germania; in realtà i Tedeschi ovviarono abbastanza facilmente al problema che si era creato, con la trasmissione dei loro messaggi via radio, ma questo consentì agli Inglesi di intercettare enormi flussi di informazioni, cosa che senza quel sabotaggio non si sarebbe mai verificata. Tutte le comunicazioni intercettate finivano nella cosidetta **"Room 14"**, la sezione di criptanalisi dell'ammiragliato inglese, dove una numerosa squadra di matematici, linguisti e campioni di scacchi lavoravano per decriptare i messaggi nemici.
Il **28 Luglio 1914** comincia la 1ª Guerra Mondiale, con l'attentato di Sarajevo all'arciduca austriaco Francesco Ferdinando; solo poche settimane dopo, nel **Settembre** del **1914**, una isolata azione di guerra in mare determina il più clamoroso dei successi per l'Intelligence della Marina Reale Inglese: gli alleati Russi catturano nel Mar Baltico una nave tedesca, l'**incrociatore Magdeburg**, sul quale fu trovato il più importante codice navale tedesco allora in uso; il cifrario, consegnato agli Inglesi, fu subito inviato alla gruppo di lavoro della "Room 14"; dalla decodifica dei messaggi inviati dal Comando della Marina Tedesca, gli Inglesi, per l'intera durata della 1ª Guerra Mondiale, furono a conoscenza di tutte le comunicazioni della Kaiserliche Marine, praticamente in tempo reale, poco dopo la loro trasmissione; questo permise alla Regia Marina Inglese di impedire qualsiasi azione navale di rilievo da parte tedesca: dopo le battaglie del Dogger Bank e dello Jutland, la Marina della Germania non si impegnò più in scontri diretti, lasciando la guerra sul mare alle sole azioni dei sottomarini. Lo spionaggio e la criptologia avevano cambiato le regole delle guerre moderne, per sempre.
Nella storia dello spionaggio militare, l'avvenimento più importante nella 1ª Guerra Mondiale accade il **17 gennaio 1917**, quando gli inglesi intercettano un telegramma cifrato secondo il codice classificato "0075". Il **codice "0075"** era riservato alle comunicazioni diplomatiche della Germania: si trattava di un complicato sistema costituito da diecimila (10000) parole e frasi cifrate, con mille (1000) gruppi numerici, che non era ancora stato violato e compromesso. Dal tipo di codice utilizzato gli inglesi compresero subito l'importanza della comunicazione; infatti, il telegramma era un documento riservato al Presidente del Messico, spedito dal Ministro degli Esteri tedesco all'Ambasciata Imperiale Tedesca in Messico, dove l'Ambasciatore doveva decriptare il messaggio e consegnarlo direttamente al Presidente messicano. L'ambasciatore tedesco ricevette come previsto il telegramma, cifrato con il codice cifrato "0075", ma commise un errore fatale: prima di inviarlo a Città del Messico via telegrafo trascrisse il messaggio criptato con un altro tipo di codifica già violata dagli Inglesi e questo permise agli inglesi di conoscere del contenuto del messaggio. Esso rivelò informazioni utilissime agli inglesi e agli americani: la Germania voleva riprendere la guerra sottoma-

rina, nonostante il patto firmato con gli U.S.A. che aveva proibito l'assalto al traffico mercantile, e nel messaggio si chiedeva l'intervento in guerra del Messico, che doveva invadere gli Stati Uniti, auspicando anche il conseguente intervento del Giappone contro gli U.S.A., a sostegno degli Imperi Centrali europei. Tale messaggio fu fondamentale per l'entrata in guerra degli U.S.A., che al momento dell'affondamento del transatlantico civile "Lusitania" dichiararono guerra alla Germania, avvalendosi del contenuto della lettera diplomatica per dimostrare il mancato rispetto del patto siglato sui limiti della guerra sottomarina.

La Seconda Guerra Mondiale fu il periodo d'oro per la crittografia: si utilizzarono le prime macchine cifranti automatiche, prima meccaniche e poi elettroniche, con lo scopo di codificare di messaggi cifrati sempre più complessi. La macchina di cifratura più famosa di quel periodo fu "Enigma", utilizzata dalle forze armate del terzo Reich, e altrettanto famosa fu la Macchina di Turing, il primo calcolatore elettronico, realizzato con lo scopo di decodificare i messaggi cifrati.

I servizi segreti francesi erano arrivati ad un passo da svelare il segreto di "Enigma"; grazie ad un infiltrato nelle forze armate tedesche, l'intelligence francese riuscì a mettere le mani su due documenti riguardanti "Enigma" che avrebbero permesso anche la costruzione della macchina. Il progetto però fu abbandonato, perché la macchina fu ritenuta troppo complessa da realizzare. I documenti furono quindi venduti ai servizi segreti polacchi. Nel periodo fra le due Guerre Mondiali il nuovo stato della Polonia, nato a seguito dei trattai di pace che chiusero la Prima Guerra Mondiale, sentiva fortemente minacciata la sua esistenza, a causa della sua posizione geografica, che la vedeva stretta fra due potenze come Russia e Germania: per gli alti vertici militari polacchi, questo costituiva una minaccia mortale per l'indipendenza della loro nazione. Fra i vari provvedimenti che la Polonia adottò per la sicurezza nazionale, vi fu quello di rinforzare la propria squadra di crittografi: Fu costituito il Biuro Szyfrów, per il quale furono reclutati allo scopo i migliori matematici, alcuni di fama mondiale, fra i quali **Marian Rejewski**. Rejewski sapeva che una macchina cifrante a rotori doveva lavorare seguendo una ben precisa regola matematica: doveva esistere una corrispondenza tra il modo in cui la macchina cifrava una lettera in una posizione e il modo in cui a tale cifra corrispondeva una lettera nella posizione successiva della sequenza. Egli riuscì a ricostruire le sequenze di codifica ottenute con il sistema di rotori utilizzato da "Enigma", e poté costruire una versione di "Enigma" senza mai averne vista una di quelle tedesche, che erano gelosamente custodite e segregate dalle Forze Armate del Terzo Reich.

Nel 1931 un traditore tedesco passò a Rejewski il libretto di utilizzo della macchina enigma e il matematico ebbe la conferma delle sue ipotesi. I tedeschi però cambiavano la chiave di cifratura ogni giorno, e Rejewski, per riuscire a decifrare i messaggi, mise a lavorare in serie 6 macchine simili a "Enigma", che potevano operare con più di 17000 chiavi di cifratura; chiamò la macchina così ottenuta la **"Bomba"**, anche a causa del ticchettio emesso dai rotori durante il funzionamento.

Venuti a conoscenza di questi attacchi alla segretezza delle loro comunicazioni, I Tedeschi modificarono la versione originale di "Enigma", e aggiunsero due nuovi rotori alla macchina, rendendo ancora più complessa crittazione delle informazioni. Le modifiche apportate misero in grande difficoltà i crittografi polacchi, che chiesero aiuto agli "007" inglesi. Le “bombe” costruite da Rejewski furono portarle a Betchley Park giusto due settimane prima dell'invasione da parte della Germania in Polonia, fatto che avvenne il 1 Settembre del 1939.

I primi modelli della "Bomba" riuscivano a criptare solo alcune parti dei messaggi così furono co-

struite nuove macchine, sotto la guida del matematico Alan Turing, capaci di decifrare la maggior parte dei messaggi. L'esercito Inglese costituì a **Betchley Park** un gruppo di centinaia di persone, matematici, militari, ufficiali, sottufficiali, che lavoravano costantemente alla decrittazione dei messaggi, sotto il nome in codice "Ultra". Gli analisti inglesi si accorsero che i messaggi delle 6 del mattino riguardavano le condizioni meteorologiche l'identificazione di qualche parola riduceva notevolmente le combinazioni dei codici di cifratura da analizzare. Alcune operazioni belliche portarono alla cattura di codici cifrati e di modelli aggiornati di "Enigma".
Nel **1943** un ingegnere inglese, Tommy Flower realizza **"Colossus"**, una macchina progettata dal matematico **Max Newmann** molto più veloce poiché trasforma la decrittazione da elettromeccanica a elettronica, con la possibilità di violare il codice di macchine meccaniche che contenevano fino a 12 rotori.
La decrittazione dei codici tedeschi fu di fondamentale importanza per gli alleati, e permise di accelerare la sconfitta del Terzo Reich, con importanti successi nelle battaglie chiave, che ridussero la capacità di resistenza della Germania e accelerarono la fine del conflitto, risparmiando con ogni probabilità migliaia di vite umane. Il gruppo "Ultra" non ebbe notorietà, neppure nel dopoguerra. Nessun merito fu pubblicamente riconosciuto agli uomini di Betchley Park: Turing restò nell'ombra, e la "Bomba" fu smantellata, una volta terminato il conflitto.

La crittografia e la segretezza delle informazioni

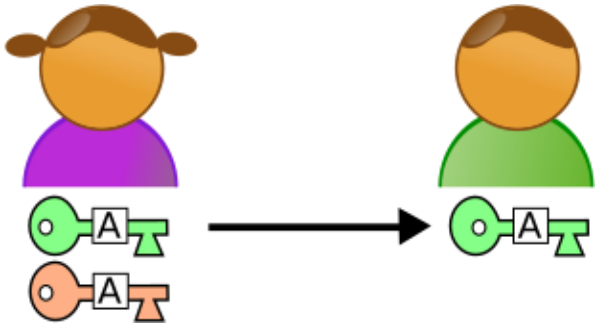
Sono molti i metodi che si possono usare per nascondere un messaggio. Ne elenchiamo alcuni.

- Scrittura invisibile (tramite inchiostri "magici", inchiostri che si rendevano visibili solo attraverso determinate reazioni chimiche o fisiche).
- Scrittura convenzionale, dove la frase è leggibile ma il significato apparente è diverso da quello reale. Il mittente e il destinatario del messaggio conoscono il significato non convenzionale delle frasi usate.
- Scrittura cifrata, dove il testo non ha significato logico ed appare come combinazione di lettere, numeri, e simboli decifrabili solo da chi riceve. Il messaggio cifrato si chiama crittogramma; per creare un crittogramma si utilizza una "chiave", e tale chiave serve per cifrare e decifrare il messaggio.

Si possono individuare più tipi di crittografia:

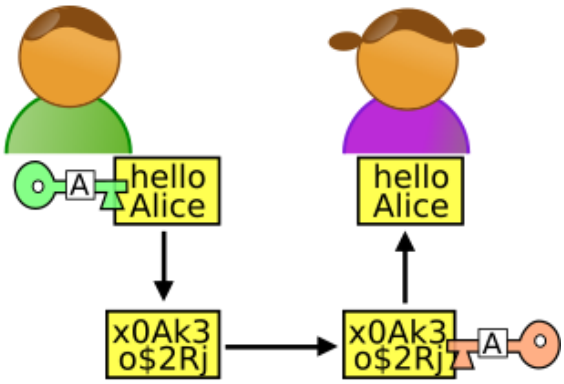
1. crittografia a chiave simmetrica
2. crittografia a chiave asimmetrica
3. crittografia quantistica

La *crittografia a chiave simmetrica* è stata ,fino a poco tempo fa, l'unica forma di crittografia utilizzata. Si chiama simmetrica poiché la chiave utilizzata per cifrare il messaggio è la stessa utilizzata per decifrarlo; il problema di tale tipologia è quello di dover condividere la stessa chiave di cifratura con il destinatario. Con Enigma, la , questo problema si risolve con la crittografia asimmetria.



La *crittografia a chiave asimmetrica* è una vera e propria scoperta rivoluzionaria: infatti non era più il mittente a dover generare e ad inviare la copia della chiave di cifratura e decifratura ma bensì il destinatario. Il destinatario possiede due chiavi; la prima è la *chiave di cifratura del messaggio* (detta *chiave globale*); la scoperta di questa chiave non determina la scoperta del sistema di crittografia, perché senza la seconda chiave, detta *chiave di decifratura*, essa è completamente inutile. La chiave di decifratura è conosciuta dal solo destinatario, e generata in conseguenza della chiave di cifratura.

Il destinatario genera con la chiave di decifratura (colore arancio ne nelle figure) la chiave di cifratura (verde nelle figure), quindi la invia al mittente, che in base a tale chiave codifica il messaggio da inviare e lo trasmette al destinatario. Il destinatario decodifica il messaggio con la chiave di decifratura.
In questo modo solo il destinatario può leggere il messaggio e non ci sono rischi di perdita o furto della chiave di decifratura, dato che essa non è mai spedita.



La *crittografia quantistica* si basa sulle leggi della fisica quantistica per la fase di scambio della chiave; l'applicazione di questo metodo permette di individuare il caso in cui la chiave entra in possesso di un soggetto diverso da chi trasmette da chi deve ricevere le informazioni. Se la chiave entra in possesso di una terza persona che non deve essere interessata allo scambio di informazioni, sia chi invia la chiave che chi la riceve sono avvisati del fatto che la chiave è stata violata e non è più sicura.

Enigma - storia e contesto

"Enigma" era una macchina elettromeccanica in grado di cifrare e decifrare dei messaggi. La macchina era stata costruita all'inizi degli anni 20 come sistema per uomini d'affari allo scopo di tenere segrete informazioni di natura commerciale. la sviluppò Arthur Scherbius, nel 1918 ispirandosi al disco cifrante di Leon Battista Alberti con l'intento di commercializzarla nel 1923, fondando anche una società a Berlino, la Scherbius & Ritter. Tale progetto fu però un fallimento a causa dei costi elevati del prodotto, che ne determinarono l'impossibilità di diffonderla in ambito civile.
Nel 1923 però la Marina Militare Tedesca si interessò al progetto della macchina: la Kriegsmarine iniziò ad usare una propria versione di "Enigma", che a meta degli anni '30 era diventato un equipaggiamento standard di tutti i servizi militari e dei dipartimenti dei servizi segreti tedeschi: ne furono fabbricate circa centomila (100.000) unità.
Essa assomigliava molto ad una macchina da scrivere ed era alimentata da una batteria elettrica. La macchina non produceva la sua risposta stampata con i caratteri dell'alfabeto occidentale: i messaggi cifrati erano trasmessi in codice morse e poi erano decifrati dal destinatario con un'altra macchina dello stesso tipo.

Il fatto che Enigma fosse stata adottata dai vertici militari tedeschi come sistema per occultare al nemico le comunicazioni relative alle operazioni di guerra era noto anche ai servizi segreti britannici e francesi.

Un esemplare di "Enigma" nella parte grigia si nota il quadro sinottico con il "display" a matrice delle lettere, retroilluminate. Quindi la tastiera, e sul lato frontale, il pannello con le connessioni cablate.

Lo Stato Maggiore delle forze armate di Hitler pensava di possedere uno strumento importantissimo, in grado di decidere le sorti del conflitto: "Enigma" era trasportabile, relativamente piccolo e semplice da usare; in realtà, il funzionamento di "Enigma" è la combinazione di più sistemi ma tutti a chiave simmetrica: la prima chiave è la macchina stessa con i suoi sistemi elettromeccanici di codifica, le altre chiavi sono codici riguardanti il giorno di trasmissione, il codice del comando interessato dalla comunicazione, trasmessi con il messaggio stesso, cambiati ogni mese, e distribuite ai vari comandi delle forze armate del Reich su apposite guide.

Quindi, se gli Inglesi volevano riuscire a decifrare i messaggi criptati avevano bisogno di due cose: dovevano entrare in possesso della macchina e della serie dei codici giornalieri e dei codici relativi ai diversi comandi delle forze armate tedesche. L'anno chiave in questo senso è il 1941: in Aprile, nell'Oceano Atlantico, fra l'Islanda e la Norvegia, la Marina Inglese abbordò e catturò la nave del servizio meteorologico della Kriegsmarine "*München*", la cui missione era quella di monitorare le condizioni del tempo che dovevano servire alla imminente prima missione della corazzata *Bismarck* per l'attacco ai convogli in Atlantico (operazione *Rheinübung*). Sulla "*München*" gli inglesi si impadronirono del primo esemplare di Enigma, una versione semplificata in uso nella Kriegsmarine.

Nel Maggio del 1941, in Atlantico, ha luogo l'Operazione "Primrose": seguendo un piano già elaborato dall'Ammiragliato Inglese, il cacciatorpediniere inglese HMS *Bulldog* abbordò e catturò l'U-110, un U-Boot tedesco, sorpreso dalle unità della scorta del convoglio alleato che aveva attaccato. Gli inglesi lo danneggiarono gravemente, e prima che il battello affondasse i mariani inglesi lo abbordarono, catturarono l'equipaggio, che fu portato sul cacciatorpediniere HMS *Bulldog* e fu subito segregato; gli inglesi riuscirono a impossessarsi di una macchina "Enigma", ma soprattutto del preziosissimo manuale con le tavole per il posizionamento dei rotori relative al codice "Hydra" utilizzato dalla Kriegsmarine, in condizioni perfette.

Il risultato di queste operazioni aprì la strada alla decodifica dei messaggi della marina tedesca; più complessa risulterà la decifratura dei messaggi degli altri comandi delle Forze Armate Tedesche, ma la sopravvenuta conoscenza del metodo e il possesso della macchina originale agevolarono questi compiti al gruppo di lavoro di Betchley Park e a Turing; anche se in molti casi si ebbe solo una decodifica parziale delle comunicazioni militari, questo risultò già sufficiente per eliminare

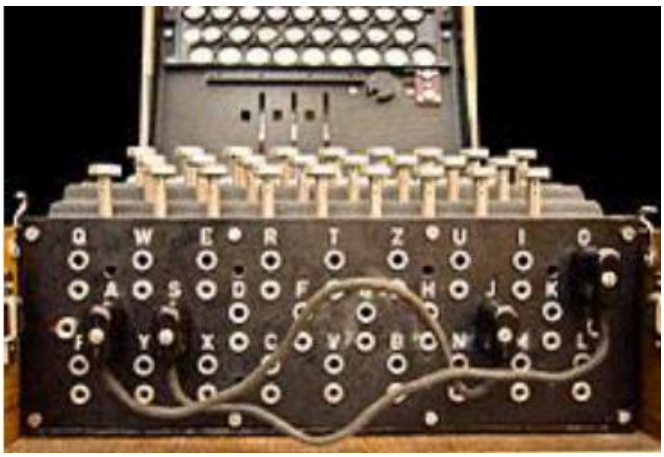
qualsiasi "effetto sorpresa" per le operazioni militari del Terzo Reich. I risultati dell'Intelligence inglese da soli non sarebbero stati sufficienti per vincere la guerra, ma la conoscenza anticipata delle azioni nemiche pose le Forze Alleate in una situazione di superiorità costante.

Enigma - cos'è e come funziona

La macchina era costituita da una tastiera, un pannello (plugboard), i rotori e la meccanica e le connessioni elettriche necessarie per l'interfacciamento e il funzionamento della macchina.

La Tastiera QWERTZ era l'interfaccia uomo-macchina, la periferica di input, come si direbbe oggi: non appena si premeva un tasto, una lampadina si accendeva su una lettera diversa da quella premuta sulla tastiera, indicando la codifica della lettera iniziale; in fase di decodifica, sul quadro sinottico si accendeva la lettera originale del messaggio.

I ***rotori*** sono determinanti per la codifica dei messaggi. La prima versione di "Enigma" possedeva 3 rotori, contenenti le 26 lettere dell'alfabeto
Il movimento dei rotori era di questo tipo: quando il primo rotore completava un giro (26 scatti, tanti quanti le lettere dell'alfabeto), il secondo rotore si spostava di una lettera e cosi via. L'ultimo rotore dava la codifica della lettera.



La ***plugboard*** o ***pannello con connettori a spina***: esso consisteva in una disposizione di connettori a spina (di tipo "jack", nella dizione odierna) in cui è possibile inserire dei cavi che determinavano fino a dieci scambi fra altrettante lettere, attraverso un sistema di connessioni elettriche che agiva sulla posizione del primo rotore; il pannello costituiva una come ulteriore chiave di codifica.

Ognuno di questi componenti riportava le ventisei lettere dell'alfabeto; quando l'operatore premeva un tasto, inviava un impulso elettrico al meccanismo della macchina, che attraversava la scheda

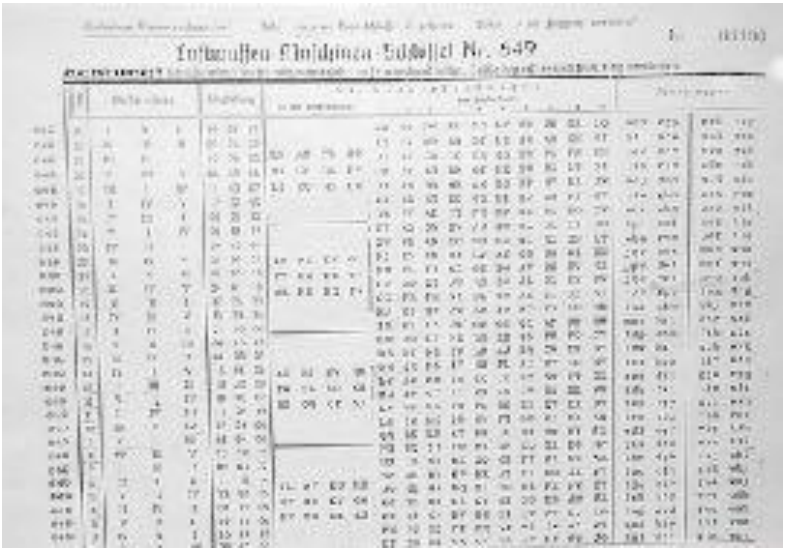
con i connettori per poi essere inviato al primo dei rotori che codificava l'alfabeto. Tramite il posizionamento dei rotori e delle connessioni sul pannello frontale l'operatore impostava la chiave di cifratura di Enigma, che permetteva già in questa modalità centocinquanta milioni di combinazioni ($150 \cdot 10^6$ combinazioni). All'apice della guerra i codici venivano cambiati anche ogni 8 ore, e anche la macchina fu migliorata, aggiungendo altri rotori: i rotori funzionanti erano tre, ma si passò prima a cinque, poi a sette rotori, aumentando le possibili combinazioni per la codifica approssimativamente dieci milioni di miliardi di combinazioni ($\sim 1 \cdot 10^{16}$ combinazioni).

Le piccole finestre mostravano le lettere sui rotori indicate secondo il loro ordine numerico nell'alfabeto e ogni volta che si premeva un tasto, il rotore si muoveva in avanti di una lettera. L'impulso passava da destra a sinistra attraverso ciascuno dei 3 rotori. All'interno di ogni rotore vi erano dei cavetti che trasmettevano gli impulsi seguendo un percorso che portava all'illuminazione della lettera codificata, per poi rientrare attraverso il percorso nel pannello (plugboard) e codificando l'informazione

Nel percorso di decodifica il segnale elettrico rientrava nel labirinto del plugboard e poi metteva in movimento i rotori. Alla fine una spia luminosa si accendeva sulla macchina, indicando nell'apposito quadro sinottico le lettere trasposte. La lettera che si accendeva dipendeva dalla codifica impostata per la macchina.

Per fare in modo che la macchina del mittente e quella del destinatario fossero coordinate perfettamente, coloro che usavano la macchina utilizzavano delle tavole con i codici di settaggio, che venivano cambiati ogni giorno; le tabelle (guide) riportavano quali erano i rotori e in quale ordine dovevano essere utilizzati, per la cifratura o la decodifica del messaggio.

Un esempio dei codici giornalieri usati come chiavi di codifica per "Enigma".



Il messaggio era trasmesso e ricevuto come una sequenza morse; nella decodifica poi, le lettere del messaggio morse erano decifrate con il codice luminoso della macchina, che veniva trascritto in modo da poter leggere il messaggio inviato.

"Enigma" nella letteratura e nel cinema

Le storie di spie, servizi segreti, messaggi dal contenuto importante destinato a pochi in scenari di guerra hanno da sempre costituito una fonte di curiosità per gli storici ma sono anche di ispirazione per romanzieri e sceneggiatori; "Enigma" è in questo caso un tema perfetto per questo scopo, ed ha inspirato testi storici ma anche biografie e storie fantasiose, non necessariamente vere.
Il romanzo "*Enigma*" di *Robert Harris* è costruito intorno al ruolo di Enigma e della sua forzatura, per il contrasto all'azione dei sommergibili tedeschi durante la seconda guerra mondiale. Il libro parla della storia di decodifica di Enigma avvenuta in poche settimane, con in primo piano l'aiuto tecnologico sfruttato prima dai polacchi, poi dagli inglesi e infine dagli americani.
Ma la letteratura non è la sola a raccontare storie con protagonista principale o "guest star" "Enigma": anche il cinema ha promosso diversi film, in un periodo di circa 36 anni. Qui sotto ne sono elencati alcuni e anche vincitori di un premio Oscar:

1. "*Secret of Enigma*", del 1979, è un film polacco di *Roman Wionczek*, e racconta la storia del Biuro Szyfrów (Ufficio Cifra) polacco e di Rejewski, che violò per primo il codice di Enigma;
2. "*U-571*" (anno 2000), è un film, una coproduzione franco-statunitense, di *Jonathan Mostow*. La storia, non vera, si basa su quanto accaduto nell'operazione "Primrose". Gli americani vengono a sapere che un U-Boot tedesco in difficoltà, l'U-571, attende soccorso da un altro U-Boot. Una squadra di incursori viene subito approntata e inviata con un sommergibile mascherato da U-Boot tedesco per abbordarlo e impadronirsi di Enigma e dei relativi documenti di cifratura; il vero soccorritore tedesco però arriva sullo scenario di guerra, affonda il sommergibile americano ed è a sua volta affondato dagli incursori americani con l'U-571. Quest'ultimo è nuovamente attaccato da un cacciatorpediniere tedesco (Torpedojäger), avvisato dell'accaduto da un aereo ricognitore della Luftwaffe. La battaglia fra il caccia tedesco e l'U571 in mano americana è fatale ad entrambe le unità: il cacciatorpediniere è affondato con l'ultimo siluro utile del sottomarino, che però è gravemente danneggiato dalle bombe di profondità e affonda. I superstiti attendono i soccorsi su un battellino di salvataggio: con loro i cifrai nazisti e "Enigma". Al film è stato assegnato un Premio Oscar nel 2001, per il miglior montaggio sonoro.
3. "*Enigma*" (anno 2001), film di *Michael Apted*, (una coproduzione inglese, statunitense, tedesca e olandese), è tratto dall'omonimo romanzo di Robert Harris. Nel marzo 1943 i decifratori di Bletchley Park scoprono con disappunto che i tedeschi hanno modificato il sistema "Enigma" usato dai loro U-Boot. Il brillante decriptatore Tom Jericho, facente parte del gruppo di Betchley Park e temporaneamente congedato per un esaurimento nervoso, è richiamato e incaricato di decifrare i nuovi codici nazisti. A Betchley Park però c'è una spia e Tom è fra i sospettati, anche perché aveva avuto una storia con Claire, una collega, che era misteriosamente scomparsa. Tom Jericho riprende il suo lavoro ma con una amica di Claire, Hester Wallace, indaga sulla scomparsa della donna. I due scoprono che il nuovo compagno di Claire, Puck, tradisce gli inglesi passando informazioni sul lavoro di Betchley Park ai tedeschi, come atto di vendetta verso i russi: infatti, nel massacro di Kathy, in Polonia, era morto il fratello di Puck. Puck è scoperto e ucciso poco prima di rivelare preziose informazioni ai tedeschi, mentre la scomparsa di Claire continua ad essere un mistero. La guerra fi-

nisce, e Tom ed Hester, che aspetta un figlio da Tom, si recano al cinema. Tom individua e riconosce Claire da lontano, ma ormai la sua vita continua felicemente con Hester.

4. "*The Imitation Game*" (anno 2014) è un film di produzione congiunta USA - Gran Bretagna sulla vita di Alan Turing, il grande matematico ed esperto di crittografia inglese ingaggiato dai servizi segreti britannici durante la seconda guerra mondiale per decifrare il sistema di messaggistica crittografato "Enigma" utilizzato dalle truppe tedesche: Il filma ha vinto un Premio Oscar nel 2015 per la miglior sceneggiatura non originale di Graham Moore, basata sul libro di Andrew Hodges.

Lavoro a cura di
Bruno Cappella, Francesco Greco (3ª CHB),
con il contributo di Cecconi Pietro, Cirri Simone,
Benini Gabriele (3ª CHA),
Revisione prof. Andrea Mazzei