Uso della crittografia durante la seconda guerra mondiale: la macchina cifrante Enigma

Stefano Buzzi, Daniela Saturnino
(Università di Cassino)

Fin dall'antichità, l'uomo ha avvertito l'esigenza di usare dei metodi di alterazione dei messaggi per nasconderne il contenuto a occhi indiscreti e riuscire a rivelarlo soltanto al destinatario. Da qui nasce la crittografia, la scienza che studia tecniche che permettano la manipolazione dei messaggi in modo da renderli incomprensibili alle persone non autorizzate. Il principale ambito di applicazione della crittografia è storicamente quello militare, anche se, nell'odierna società dell'informazione, la crittografia è ampiamente utilizzata per proteggere le transazioni bancarie e commerciali che avvengono per via telematica, e per garantire riservatezza alle informazioni che viaggiano attraverso la rete Internet o che sono stipate su supporti di memorizzazione quali ad esempio dischi rigidi.

La crittografia simmetrica si basa sull'uso di una chiave segreta, nota soltanto al mittente e al destinatario, e di un algoritmo, ovvero di un procedimento che permette di modificare il messaggio originario in un messaggio cifrato. Solo conoscendo la chiave è possibile risalire all' informazione originale. La storia è caratterizzata dallo sviluppo di tecniche di crittografia sempre più efficaci, soprattutto in ambito militare. La necessità di cifrare le comunicazioni militari risale, infatti, fino ai tempi di Cesare. Fino all'inizio del secolo scorso, le tecniche adottate facevano però uso di carta e penna, ma gli addetti alla sicurezza sentirono presto l'esigenza di un maggiore livello di segretezza. È in questo contesto che sono nate le macchine cifratici elettro-meccaniche, la più famosa delle quali è Enigma, usata dalle forze armate tedesche durante la Seconda Guerra Mondiale.

Nascita e funzionamento di Enigma

La macchina Enigma nasce molto prima della Seconda Guerra Mondiale e, a dispetto di quanto si potrebbe credere, non è stata creata per scopi militari. Realizzata nel 1918 dall'ingegnere berlinese Scherbius, era stata ideata con lo scopo di soddisfare le esigenze dei grandi industriali dell'epoca, che subito dopo la fine della Prima guerra mondiale, si videro costretti a fronteggiare il nuovo fenomeno dello spionaggio industriale. La prima macchina Enigma fu esposta nel 1923 al Congresso Internazionale dell'Unione Postale, per essere poi messa in commercio

suscitando l'interesse di acquirenti inaspettati, come gli stati maggiori degli eserciti di Germania, Giappone, Polonia e Stati Uniti. Diversi esemplari furono acquistati dalla Marina Militare tedesca nel 1926, poi nel 1929 il dispositivo venne acquisito dall'Esercito, e da allora in poi praticamente da ogni organizzazione militare tedesca e dalla maggior parte della gerarchia nazista. Versioni di Enigma furono usate per quasi tutte le comunicazioni radio tedesche, spesso anche per quelle telegrafiche, durante la guerra (perfino i bollettini meteorologici vennero cifrati dall'Enigma!).

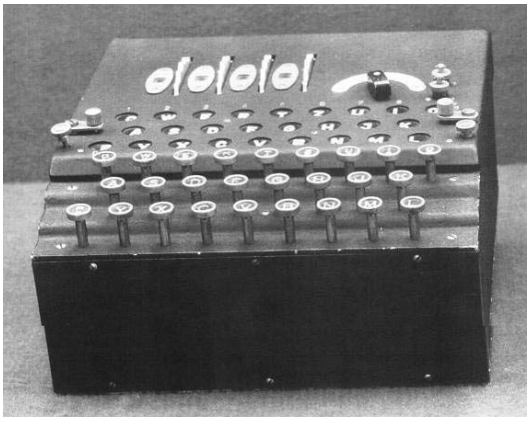


Figura 1 (Collezione Cremona)

La macchina Enigma aveva l'aspetto di una macchina per scrivere con due tastiere (fig. 1): una vera inferiore ((1) in fig. 2), e la seconda superiore ((2) in fig. 2) costituita da lettere luminose che si accendevano ad ogni tasto premuto sulla tastiera. La sequenza delle lettere che si illuminavano dava il messaggio cifrato (o quello in chiaro, se si digitava il testo cifrato).

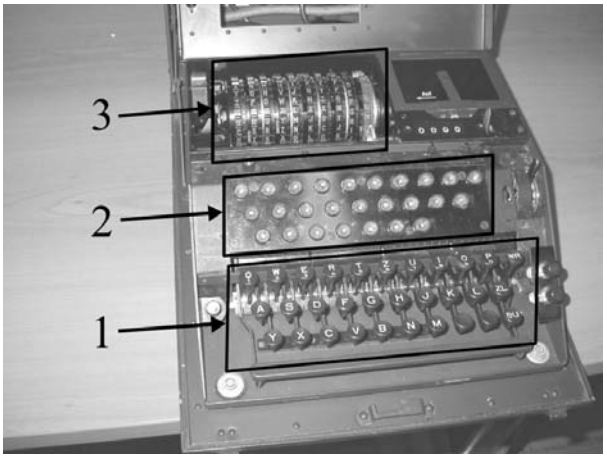


Figura 2 (Collezione Cremona)

(Paragrafo attuale)

Il suo funzionamento si basava su tre dischi cablati, detti **rotori** (fig. 3), che avevano 26 contatti per lato (uno per ogni lettera dell'alfabeto tedesco): i cablaggi dei dischi mettevano in comunicazione ciascuna lettera su un lato con una diversa lettera sull'altro lato. I dischi erano collegati insieme da un particolare meccanismo: il primo disco ruotava di una lettera ad ogni pressione di tasto, il secondo ruotava di una lettera ogni volta che il primo compiva un giro e il terzo ruotava di una lettera quando il secondo finiva un giro. I rotori erano imperniati su un medesimo asse ed era possibile cambiare l'ordine di disposizione dei tre dischi. Inoltre tali rotori erano scelti ogni giorno da un gruppo di cinque esemplari.

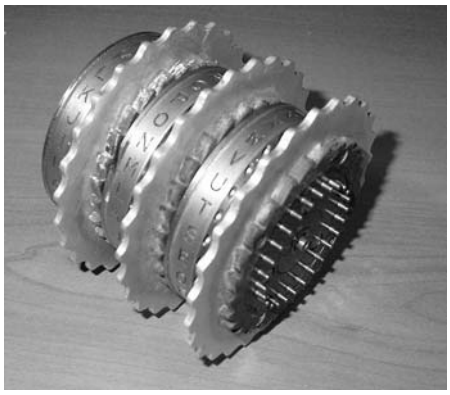


Figura 3 (Collezione Cremona)

Nella parte anteriore della macchina c'era un'altra sezione, denominata "pannello dei collegamenti" (fig. 4). Erano disponibili dieci cavi, con uno spinotto a entrambe le estremità, che servivano per scambiare tra loro coppie di lettere prima dell' immissione nel rotore, così da aumentare la sicurezza del codice.

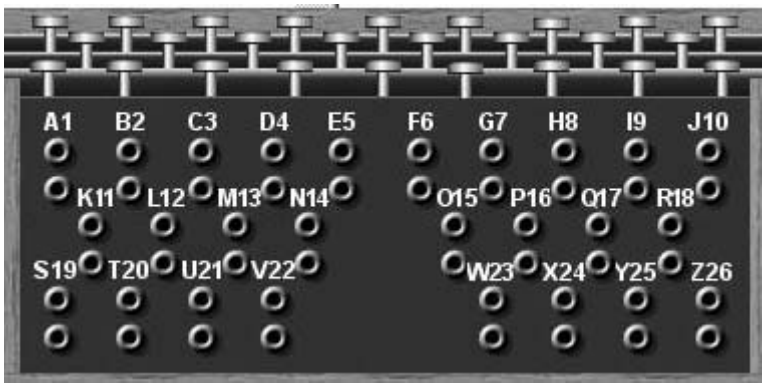
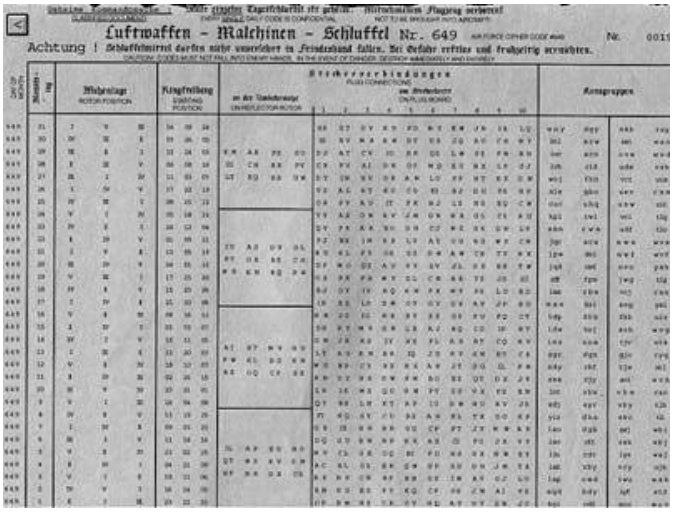


Figura 4

Le impostazioni della macchina costituivano la chiave per poter effettuare opportunamente la criptazione e la decriptazione del messaggio. Agli operatori addetti alla cifratura ogni mese veniva distribuito un foglio contenente le chiavi relative ad ogni giorno del mese (fig. 5). Tali fogli erano stampati con inchiostro solubile e custoditi con estrema attenzione. Quando si fosse presentato il rischio che uno di questi fogli potesse cadere in mani nemiche, l'ordine era di gettarlo in acqua per eliminare tutte le informazioni. I Tedeschi avevano molta fiducia nell' efficacia di Enigma ed erano convinti che soltanto procurandosi le chiavi gli Alleati avrebbero potuto decifrare le loro comunicazioni.

Per la marina tedesca venne messa a punto una versione particolare di Enigma, che impiegava quattro rotori cifranti presi da un insieme di otto, per aumentare ancora il numero di combinazioni disponibili.


Luftwaffen – Maschinen – Schlüssel Nr. 649

Achtung ! Schlüsselmittel dürfen nicht unverletzt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig zu vernichten.

Figura 5

La lotta contro Enigma

Il sistema di codifica della macchina Enigma era così sofisticato che nessuno riteneva possibile la decriptazione dei suoi messaggi: il modello base, costituito da soli tre rotori, permetteva già di arrivare a circa 150 milioni di milioni di milioni di combinazioni diverse. Tutto si sarebbe risolto per il meglio per i Tedeschi se non fosse stato per un curioso personaggio: Hans Thilo Schmidt. Spinto dal desiderio di un tenore di vita che il suo stipendio da funzionario dell'Ufficio Cifra dell'esercito tedesco non gli permetteva, nel 1931 questi cominciò a passare ai servizi segreti francesi i manuali operativi di Enigma usati dall'esercito tedesco, continuando a rivelare informazioni fino al 1943 quando, scoperto dalla polizia nazista, si suicidò in carcere per evitare le torture. I manuali di utilizzo, tuttavia, non consentivano da soli di capire la chiave utilizzata per codificare un testo, anche perché le chiavi di cifratura venivano cambiate costantemente, persino più volte al giorno. Consapevoli

di questo, i servizi segreti francesi decisero di rivolgersi alla Polonia.

I servizi segreti polacchi, infatti, a dispetto della riservatezza e del segreto, erano riusciti a intercettare una valigia diplomatica contenente un esemplare della macchina Enigma. A Varsavia operava un agguerrito gruppo di crittografi guidati dal matematico Marian Rejewski, che nell'agosto 1932 riuscì per la prima volta a violare Enigma. Una volta ricostruita la struttura logica di Enigma, Rejewski progettò e costruì la “bomba crittologica”, un rudimentale calcolatore composto da molti moduli; ciascun modulo consisteva di uno scaffale di ferro largo 2 metri e 10, alto 1 e 90, profondo sessanta centimetri, e pesante circa una tonnellata. Ogni modulo metteva in movimento 108 rotori (più tre di controllo) in gruppi di 12 per fila, che eseguivano gradualmente la decodifica dei messaggi.

Quelle polacche erano però vittorie molto relative: il problema, infatti, non era solamente comprendere la chiave utilizzata per codificare un determinato testo, ma anche farlo velocemente. Conoscere in tempo reale il senso delle comunicazioni intercettate era di fondamentale importanza, mentre spesso questi stentavano a capire il senso di messaggi risalenti a mesi o a settimane prima. Inoltre la situazione si aggravò quando tra il 1938 e il 1939 i Tedeschi cambiarono le regole di cifratura, aumentando il numero dei rotori da tre a cinque e rendendo quasi inefficace il metodo polacco.

Figura 6

Con l'invasione della Polonia da parte dei nazisti, poi, la lotta per la violazione di Enigma si spostò in Gran Bretagna.

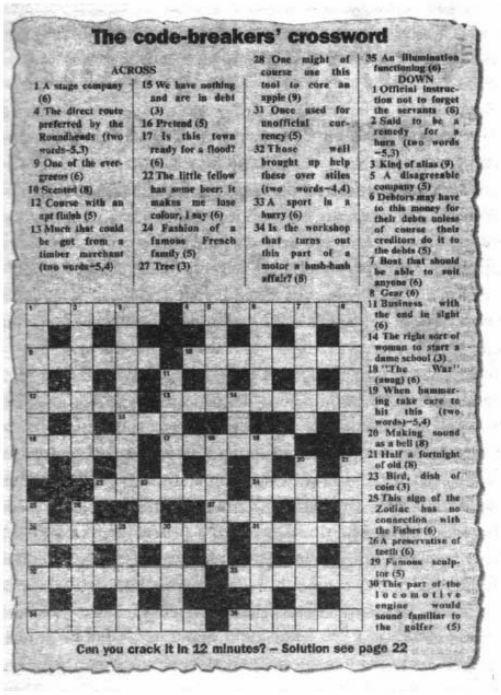
Nell’agosto del 1939 i Britannici costituirono, infatti, la scuola dei codici e dei cifrari (GC&CS) a **Bletchley Park** (fig. 6) nel Buckinghamshire, vicino Londra. Qui iniziò una guerra parallela, una vera e propria partita a scacchi, tra gli inglesi che

cercavano di decrittare i messaggi dei tedeschi il più velocemente possibile e questi ultimi che cambiavano costantemente le chiavi e perfezionavano le loro macchine.

Tra coloro che lavoravano a Bletchley Park c'erano esperti di ogni genere, ma soprattutto ingegneri e matematici, che venivano reclutati tramite un concorso (la risoluzione di un cruciverba (fig. 7)).

Inconsapevolmente gli stessi Tedeschi aiutarono gli Inglesi a decifrare Enigma, infatti i messaggi contenevano spesso le stesse espressioni: molti cominciavano con il medesimo testo di apertura oppure venivano riportate informazioni di routine e, soprattutto, tutti i messaggi si concludevano con l'espressione *Heil Hitler!*. Queste disattenzioni fornirono ai decifratori indizi, chiamati *cribs*, sul modo in cui era stata impostata Enigma in quel giorno ed erano, quindi, fondamentali per risalire all' informazione originale.

Nella squadra di ricercatori c'era un giovanissimo matematico di nome Alan Turing, che riprogettò la Bomba polacca dando origine a Colossus, il primo calcolatore elettronico, il cui prototipo *Colossus Mark I* (fig. 8), venne assemblato proprio a Bletchley Park nel febbraio del 1944.



The code-breakers' crossword

ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words-5,3)
9 One of the ever-greens (6)
10 Scentest (8)
12 Course with an apt finish (5)
13 Muck that could be got from a timber merchant (two words-5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One night of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words-4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (6)
2 Said to be a remedy for a burn (two words-5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (sung) (6)
19 When hammering take care to hit this (two words-5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

Can you crack it in 12 minutes? – Solution see page 22

Figura 7

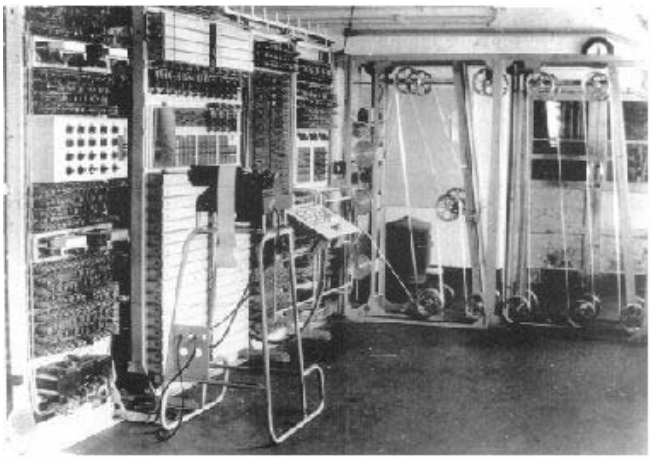


Figura 8

Turing svolse un ruolo fondamentale nel forzare il più complesso cifrario dell' Enigma navale, denominato *shark* – squalo, reso possibile anche da una fortunata operazione militare.

Nel 1941, infatti, la guerra aveva cominciato a svolgersi anche nell'Atlantico e il 9 maggio ci fu una battaglia tra il sottomarino tedesco U-Boot 110 e alcune navi inglesi. Quando il capitano di fregata John Baker Cresswell si rese conto che il sottomarino tedesco era in difficoltà sotto il bombardamento inglese, decise, anziché completare l'affondamento, di tentare un' abbordaggio. Fortunatamente la squadra inglese riuscì a recuperare intatta un esemplare della macchina Enigma, il suo manuale e le tavole per la disposizione dei rotori. Per mantenere la più grande riservatezza, l'equipaggio tedesco catturato fu mandato sotto coperta affinché non assistesse all'operazione. In seguito ai danni, però, il sottomarino finì comunque per affondare favorendo, così, il più assoluto segreto sulla vicenda.

Grazie a questo episodio e al lavoro degli uomini di Bletchley Park gli storici sostengono che la durata del conflitto è stata ridotta di almeno due anni.

Curiosità

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.

Soltanto negli ultimi anni molte informazioni sull'incredibile storia di Bletchley Park sono state rese note. Tragicamente tuttavia, per qualcuno i ringraziamenti sono arrivati troppo tardi.

Alan Turing è rimasto, infatti, a lungo un genio incompreso, solo un paio d'anni fa l'Inghilterra gli ha dedicato una statua. Turing entrò in depressione e morì, in circostanze non del tutto chiare, nel giugno 1954, a 42 anni. La statua che gli è stata dedicata, a Manchester, lo ritrae con una mela in mano (fig. 9), la versione ufficiale vuole, infatti, che abbia, più o meno volontariamente, ingerito del cianuro accompagnandolo ad una mela. Ma una biografia recente adombra l'ipotesi che Turing, detentore di importanti segreti ma ritenuto incontrollabile, fosse diventato un possibile pericolo per la sicurezza nazionale, e che i servizi segreti inglesi abbiano così inscenato un suicidio per liberarsi di questo scomodo personaggio. Anni dopo, nella Silicon Valley californiana, sorgerà una famosa compagnia costruttrice di computer, la "Apple", il cui simbolo sarà una mela morsicata proprio in onore di Alan Turing.

Figura 9

Ma la morte di Turing è solo uno dei tanti misteri legati alla storia di Enigma. A Londra, o meglio alcuni metri al di sotto di essa, esiste un particolarissimo Museo: il Cabinet of War. Era il quartier generale inglese durante la Seconda guerra mondiale, in cui si riuniva il Gabinetto di guerra presieduto da Winston Churchill. In esso confluivano tutte le informazioni ricavate a Bletchley Park e si decideva in quale modo sfruttarle.

Si racconta che nel 1941 fu intercettato e decodificato un messaggio radio che annunciava entro una certa data il bombardamento di Coventry, una città sulla costa inglese. Churchill si trovò di fronte a un delicato dilemma: dando l'ordine di evacuazione alla città, avrebbe fatto capire ai tedeschi che i loro messaggi

crittografati non erano più segreti per gli inglesi. Si decise allora di non dare l'ordine di evacuazione, determinando in questo modo la morte di duemila persone, pur di mantenere il segreto. L'apertura di alcuni archivi ha insinuato anche il dubbio che Churchill, venuto a conoscenza dell'attacco giapponese contro gli americani a Pearl Harbour (dicembre 1941), non abbia avvertito il governo Usa perché voleva fortemente che questi entrasse in guerra come suo alleato.

Churchill andò una sola volta a Bletchley Park e rimase molto sorpreso dal modo in cui si lavorava: trovò alcuni scienziati, tra cui Turing, seduti per terra mentre smistavano mucchi di carta. Tenne un breve discorso che cominciava con: "A guardarvi, non si direbbe che siate a conoscenza di un segreto…".

Le curiosità legate a Bletchley Park però non finiscono qui. Qualche anno fa, durante una mostra a Bletchley Park, una delle macchine Enigma in esposizione è stata trafugata da una teca. Qualche tempo dopo, alcune lettere di riscatto sono apparse sulla stampa inglese chiedendo denaro in cambio della restituzione della macchina. Alcune citavano persino problemi matematici legati al sistema crittografico di Enigma. L'anno successivo un famoso giornalista della BBC, ha ricevuto un pacco al cui interno si trovava proprio la macchina rubata. Mancava ancora un rotore, che fu rinvenuto solo qualche mese più tardi. Ancora oggi non è stato scoperto chi abbia commesso questo furto.

La cosa più sorprendente di tutta questa storia è però il possibile finale che si sarebbe avuto se la Germania avesse resistito maggiormente. Si è scoperto, infatti, che nel maggio del 1945 a Berlino avevano deciso di cambiare radicalmente le tabelle per definire le chiavi da usare nella cifratura dei messaggi in codice. Se ciò fosse avvenuto, i ricercatori di Bletchley Park avrebbero dovuto affrontare una nuova sfida e chissà se e in quanto tempo avrebbero avuto la meglio...

Per Approfondire

- Hugh Sebag Montefiore, *Il codice Enigma*, Il Saggiatore, 2003.

- Andrew Hodges, *Storia di un enigma. Vita di Alan Turing (1912-1954)*, Bollati Boringhieri, 2003.

- David Kahn, *The codebreakers: The comprehensive history of secret communications from ancient times to the Internet*, Scribner, 1996.

- Stephen Budiansky, *La Guerra dei codici. Spie e linguaggi cifrati nella seconda guerra mondiale*, Garzanti, 2006.

Gli Autori

Stefano Buzzi è Professore Associato di Telecomunicazioni presso la Facoltà di Ingegneria dell'Università degli Studi di Cassino. Laureatosi con lode in Ingegneria Elettronica presso l'Università Federico II di Napoli nel 1994, ha successivamente ivi conseguito anche il titolo di Dottore di Ricerca. E' autore/co-autore di oltre novanta articoli scientifici pubblicati su riviste internazionali o su atti di conferenze internazionali, ed è membro del comitato editoriale di riviste scientifiche internazionali; ha trascorso nella sua carriera numerosi soggiorni di ricerca presso la Princeton University (USA). La sua attività è incentrata sull'elaborazione statistica dei segnali, e sulle sue applicazioni alle telecomunicazioni

e ai sistemi radar. A Cassino tiene attualmente corsi di *Trasmissione Numerica*, *Sistemi di Telecomunicazioni*, *Sistemi Radiomobili* e *Crittografia e Sicurezza delle Reti*.

Daniela Saturnino ha conseguito con lode la Laurea Triennale e la Laurea Specialistica in Ingegneria delle Telecomunicazioni presso l'Università degli Studi di Cassino, rispettivamente nel 2004 e nel 2006. Attualmente frequenta il Corso di Dottorato di Ricerca in Ingegneria Elettrica e dell'Informazione presso l'Università di Cassino, ed è impegnata in attività di ricerca sui sistemi di comunicazione wireless di futura generazione.