MUSEO TECNICO NAVALE

CRYPTO

Parole (s)velate

….si può sostenere con forza che l'ingegno umano non possa architettare un codice che l'ingegno umano non possa risolvere. (E. A. Poe)

CRYPTO

Parole (s)velate

Catalogo a cura di:

C.V. Silvano Benedetti

Bruno Grassi

Presentazione

L'arte di cifrare i messaggi si chiama *Crittologia* e si divide in due branche: la *Crittografia,* cioè l'arte di scrivere messaggi segreti e quindi indecifrabili, e la *Crittanalisi,* cioè l'arte di decifrarli.

La crittografia è da sempre uno strumento importante per la salvaguardia delle informazioni non solo in campo militare, ma anche in campo diplomatico, politico, commerciale e legale.

Con uno sguardo al passato, fino al XX secolo la crittografia ha utilizzato lo stesso bagaglio culturale algoritmico: trasposizioni, sostituzioni, nomenclatori, repertori ecc..

Nel XX secolo, ricco di tensioni e guerre commerciali e territoriali tra i Paesi più avanzati, con l'impulso dato alle telecomunicazioni dall'invenzione della radio, la crittografia è diventata uno strumento indispensabile ed è progredita grazie all'impiego della tecnologia elettromeccanica, elettronica, digitale e dell'informatica. All'inizio del secolo nacque la più famosa delle macchine crittografiche della storia, Enigma, che durante la Seconda Guerra Mondiale rese a lungo indecifrabili le comunicazioni radio tedesche.

Oggi la crittografia, diventata scienza, è presente, spesso a nostra insaputa, in molti servizi cui accediamo giornalmente: dai cellulari ai bancomat, dalla pay TV alla posta certificata, al conto on line.

Il mondo è oggi fortemente condizionato dai computer e dalla fruibilità dei dati in rete ed è pertanto indispensabile che tali dati siano comprensibili solo dai legittimi proprietari; la crittografia svolge in questo un ruolo di primaria importanza mettendo insieme discipline quali matematica, informatica, fisica quantistica, ingegneria elettronica, statistica, meccanica.

La mostra odierna, realizzata grazie alla fattiva collaborazione tra il Museo Tecnico Navale, l'Associazione Rover Joe, i Centri di Telecomunicazioni ed Informatica della Marina Militare e la Scuola TLC delle FF.AA. di Chiavari, presenta numerose macchine cifranti del XX secolo, alcune delle quali segretate fino a pochi anni fa, e la riproduzione di alcuni cifrari della storia, costituendo un evento unico in Italia e tra i più rari nel mondo.

C.V. Silvano Benedetti

Steganografia e crittografia

Da sempre i potenti hanno avuto bisogno di comunicare in modo riservato per governare o comandare i loro eserciti. Essi temevano terribili conseguenze se i loro messaggi fossero caduti in mano ostili; informazioni preziose sarebbero state a disposizione dei rivali e dei nemici. Fu questo pericolo a promuovere lo sviluppo di tecniche di occultamento del messaggio destinato a renderlo comprensibile solo alle persone autorizzate.

Una delle prime tecniche usate per nascondere i messaggi si chiama *steganografia,* dalle parole greche *steganós*, che significa nascosto, e *gráphein*, che significa scrivere, che ha assunto forme diverse nelle varie regioni.

Erodoto racconta che uno dei metodi più bizzarri per trasmettere le informazioni segrete, utilizzato nell'antica Persia, consisteva nel rasare i capelli di uno schiavo e scrivergli il messaggio sulla testa. Lo schiavo si recava poi dal destinatario del messaggio dopo che gli erano ricresciuti i capelli e il messaggio era recuperato rasando nuovamente lo schiavo.

Nell'antica Cina era usanza dipingere il messaggio su striscioline di seta finissima che venivano appallottolate e ricoperte di cera. Le palline erano quindi inghiottite dal messaggero e recuperate dal destinatario.

Nel XVI secolo lo scienziato italiano Giambattista Della Porta dimostrò che era possibile comunicare tramite un uovo sodo preparando un inchiostro con 30 grammi di allume in mezzo litro d'aceto ed usandolo per scrivere sul guscio. La soluzione penetrava nel guscio, che è poroso, senza lasciar traccia all'esterno e tingeva l'albume dopo la bollitura. Il messaggio veniva letto semplicemente sbucciando l'uovo sodo.

Anche messaggi invisibili ottenuti con gli inchiostri simpatici hanno svolto un servizio attivo nel nascondere le informazioni. Il testo rimaneva invisibile sui fogli di carta e veniva rivelato solo con speciali procedimenti.

Durante la Seconda Guerra Mondiale venne utilizzata la tecnica dei "Microdot" o micropunti: tramite un procedimento fotografico gli agenti tedeschi in America Latina trasformavano una pagina scritta in una "macchia" del diametro inferiore al millimetro, che poteva essere nascosta nel puntino di una "i" in una banale comunicazione. Il microdot fu scoperto dall' FBI nel 1941 grazie ad una soffiata.

La steganografia moderna è invece basata sul metodo LSB (least significant bit, bit meno significativo) ed è strettamente legata all'informatica. La teoria che regola l'LSB è quella secondo la quale un'immagine ad alta definizione, così come un qualunque file multimediale audio/video, se modificato nei suoi bit meno significativi mantiene la propria integrità. In questo modo un qualsiasi file multimediale può essere modificato e solo chi conosce i bit modificati (che costituiscono la chiave di cifratura) può risalire al messaggio criptato.

In sintesi, la steganografia si compone di un messaggio "contenitore" pubblico, dentro il quale è celato il messaggio segreto in chiaro.

Per molto tempo la steganografia ha garantito una elevata sicurezza ma con i sistemi attuali, se il messaggio viene attentamente analizzato, vi sono buone probabilità di scoprirlo e leggerlo.

Contemporaneamente allo sviluppo della steganografia si sviluppò anche la *crittografia*, dal greco *kryptós*, che significa nascosto, la quale non nasconde il messaggio, ma il suo significato. Il messaggio viene reso incomprensibile alterandolo con un procedimento concordato tra mittente e destinatario; invertendo il procedimento si ricava il messaggio originale. Il vantaggio della crittografia è che, anche se cade in mano al nemico, il messaggio risulta incomprensibile e quindi inutilizzabile.

Oggi la crittografia è strettamente connessa all'informatica e invece che di "verme" e "codice", usa parole come "computer quantistici, chiavi pubbliche e private, firma digitale", sconosciute ai più, ma che hanno un'influenza diretta sulla vita e sulla sicurezza di ciascuno di noi.

In questo opuscolo esamineremo brevemente i cifrari storici e le macchine cifranti presenti in mostra, raccontandone le caratteristiche peculiari e alcune curiosità.

LA MOSTRA

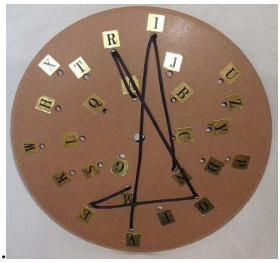
Crittografia classica

Scitala spartana - 486 a.C.

La Scitala Lacedemonica, spartana, consisteva in un bastone su cui si avvolgeva un nastro di pelle o pergamena su cui si scriveva il testo lungo l'asse del bastone su righe parallele. Svolto il nastro, il testo assumeva una sequenza casuale e quindi indecifrabile. Plutarco racconta, in "*Vite parallele*", che nel 404 a.C. lo spartano Lisandro venne raggiunto al suo accampamento da un corriere che gli consegnò un nastro che aveva con sè. Lisandro lo avvolse attorno ad un cilindretto di legno e così venne a sapere che i persiani intendevano attaccarlo. Il diametro del cilindretto era uguale a quello utilizzato dal mittente per scrivere il messaggio ed era la chiave di lettura.

Disco di Enea (390-360 a.C.)

Il generale ed inventore greco Enea il Tattico, in un suo trattato, descrive un disco in cui nella zona erano contenuti 24 fori, ciascuno dei quali era contrassegnato da una lettera. Un filo, partendo da un foro centrale, si avvolgeva passando per i fori delle successive lettere del testo. Il destinatario del messaggio svolgeva il filo dal disco segnando le lettere da esso indicate.



Scacchiera di Polibio - (200-118 a.C.)

E' il più antico codice poligrafico della storia, associava ad ogni lettera una coppia di numeri tra 1 e 5 in base ad una scacchiera.

Telegrafi a torce esistevano già da molti secoli ma potevano trasmettere solamente pochi messaggi; grazie a Polibio, qualsiasi tipo di messaggio poteva finalmente essere trasmesso a distanza rappresentando ogni lettera con due numeri in base alla riga e alla colonna corrispondenti alla sua posizione: ad es. A = 11, P = 42.

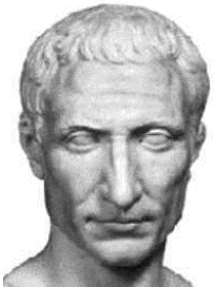
La sua importanza nella storia della crittografia sta nell'essere alla base di altri codici di cifratura usati ancora oggi.

#	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Υ
5	Φ	X	Ψ	Ω	‡

Cifrario di Cesare - 50-60 a.C.

Dell'epoca Romana è noto solo il cifrario di Cesare, prima forma di crittografia monoalfabetica a sostituzione, metodo semplice e molto diffuso, usato per la corrispondenza personale e militare.

Ogni lettera del testo veniva sostituita dalla lettera che la segue spostata di un numero fisso di posti nell'alfabeto. Svetonio ci dà testimonianza di questo nel testo *Vita di Cesare*.



Crittografia medioevale

In questo periodo fu scarso l'interesse per la crittografia, spesso usata solo per celare i nomi sostituendo ogni lettera con quella che la seguiva nell'alfabeto (per esempio A con B, B con C ecc.).

Verso l'anno mille comparvero i primi alfabeti cifranti, usati soprattutto nelle missioni diplomatiche e, a partire dal XIV secolo, dalle repubbliche marinare e dalla corte papale.

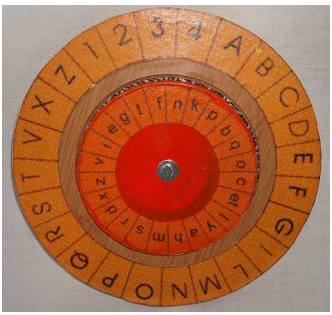
Un sistema usato dall'Arcivescovo di Napoli, Pietro di Grazia, tra il 1363 e il 1365 sostituiva le lettere con numeri o simboli speciali, la cui corrispondenza era fissata da una tabella.

Agli inizi del XIV secolo, per superare i tentativi di analisi statistica delle frequenze di ripetizione, si iniziano ad usare più simboli per cifrare la stessa vocale.

Disco di Leon Battista Alberti - 1466

Leon Battista Alberti, nel suo Trattato "De Cifris", introdusse il primo codice polialfabetico: un disco composto di due cerchi concentrici di rame. Uno esterno fisso, di diametro maggiore, sul quale sono riportate le lettere dell'alfabeto in chiaro ed uno interno mobile per le lettere dell'alfabeto cifrante. Il disco esterno è composto di 24 caselle contenenti 20 lettere maiuscole in ordine lessicografico, escluse H, J, K, W, Y, al posto delle quali ci sono i numeri 1, 2, 3, 4. Il disco interno riporta le 24 lettere minuscole in maniera disordinata (la u e la v sono nella stessa casella) ed un simbolo speciale "et".

I numeri presenti nel disco venivano inseriti all'interno delle parole del testo in chiaro in maniera casuale e servivano come riferimento il cambio dell'alfabeto cifrante. Questo sistema cifrante fu una vera rivoluzione e per tre secoli fu il riferimento per i vari sistemi crittografici. Rappresenta l'inizio della crittografia moderna.

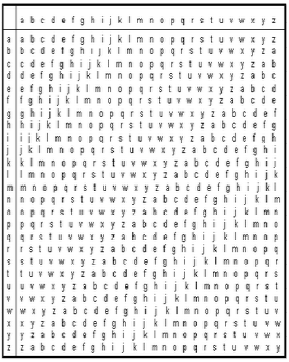


Crittografia moderna

Codice di Vigenère - 1586

Cifrario polialfabetico molto simile al cifrario di Cesare, che sposta di un carattere l'alfabeto successivo; la chiave, chiamata "verme", è concordata tra mittente e destinatario e ripetuta per tutta la lunghezza del testo in chiaro.

L'utilizzo è semplice: si entra sulle ascisse con la prima lettera del testo in chiaro, si scende sulla sua colonna e si sceglie la lettera sulla riga corrispondente alla prima lettera del verme trovata sulle ordinate. Si ripete la procedura per tutto il testo.

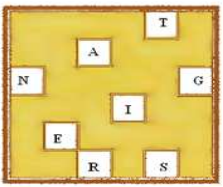


Griglie di Girolamo Cardano – XVI secolo

A Girolamo Cardano (Pavia 1501 – Roma 1576) si deve l'invenzione delle griglie forate che sono u esempio di steganografia: nasconde il testo segreto all'interno di un testo apparentemente innocuo.

Si tratta di un cartoncino o di una piastra metallica di forma rettangolare con una quadrettatura forata in maniera irregolare, attraverso la quale si scriveva il messaggio su un sottostante foglio quadrettato. Gli spazi liberi rimasti sul foglio venivano riempiti con lettere prive di significato o con frasi che confondessero il significato del testo segreto.

La griglia forata è la chiave di cifratura.



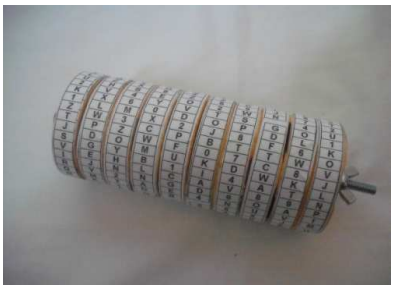
B	1	H	J	T	K
D	P	A	Q	U	2
N	3	U	N	9	G
F	E	O	I	I	8
V	E	A	O	7	T
O	M	R	6	S	L

Disco di Jefferson - 1795

Cifrario polialfabetico realizzato con un dispositivo meccanico composto da ruote di legno libere di ruotare indipendentemente su un asse metallico. Su ciascuna ruota sono scritte le 26 lettere dell'alfabeto in ordine casuale e diverso da ruota a ruota. Le ruote vengono allineate facendo corrispondere il testo in chiaro su una riga, quindi si trasmette il testo riprodotto su una qualunque delle altre righe. L'ordine di successione dei dischi era la chiave di cifratura concordata.

Thomas Jefferson, quando era segretario di stato del primo Presidente USA, propose questo strumento con il nome di *wheel cipher* (cifrario a ruote) per le comunicazioni diplomatiche riservate, ma il cifrario non ebbe il successo sperato.

Nel 1917 il Magg. Joseph O. Mauborgne ripropose il *wheel cipher* che, con il nome di M-94, rimase in uso nell'esercito USA fino al 1943.



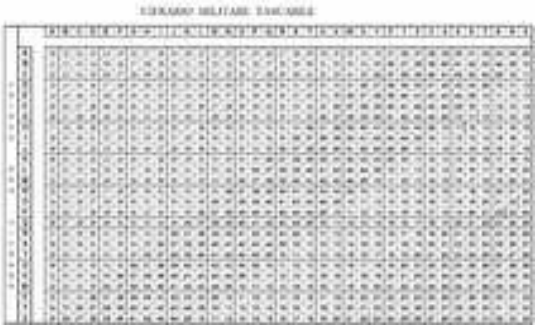
Codice Morse - 1835

Come qualunque alfabeto, anche il codice Morse può essere considerato un codice crittografico per sostituzione, in quanto ad ogni lettera e numero è sostituita una sequenza di punti e linee intellegibile solo per chi conosce il codice; sviluppato da Samuel Morse per la telegrafia, fu realizzato dal suo collaboratore Alfred Vail e diffusamente utilizzato per le comunicazini civili e militari per tutto il XX secolo.

A: ·–	B: –···	C: –·–·
D: –··	E: ·	F: ··–·
G: ––·	H: ····	I: ··
J: ·–––	K: –·–	L: ·–··
M: ––	N: –·	O: –––
P: ·––·	Q: ––·–	R: ·–·
S: ···	T: –	U: ··–
V: ···–	W: ·––	X: –··–
Y: –·––	Z: ––··	

Cifrario militare tascabile

Variante della tavola di Vigénère, era composto dalle 26 lettere e 10 numeri sull'asse orizzontale e l'alfabeto sull'asse verticale; all'interno si trovavano coppie di numeri da 10 a 45. La procedura di impiego era quella del Codice di Vigénère e il testo cifrato veniva trasmesso a gruppi di 5 cifre. Il sistema fu in uso all'Esercito italiano durante la Prima Guerra Mondiale e quindi abbandonato perché non dava sufficienti garanzie di sicurezza.



ESEMPIO:
Testo: TRASMETTERE IN GIORNATA
Chiave: F E R T

- Chiaro T R A S M E T T E R E I N G I O R N A T A

- Chiave F E R T F E R T F E R T F E R T F E R T F

- Cifra 34 31 27 11 27 18 10 12 19 31 31 37 29 20 35 43 32 27 27 12 15

- crittogramma: 34312 71127 18101 21931 31372 92035 43322
72712 15000

Crittografia in Italia all'inizio del XX secolo.

All'inizio del XX secolo la crittografia in Italia, che pur vantava tradizioni di tutto rispetto, aveva toccato uno dei suoi livelli più bassi ed era ancora in uso il cifrario militare tascabile di cui da tempo era noto un metodo di decrittazione. Con l'invenzione della radio i messaggi venivano sempre più trasmessi via etere e quindi maggiormente esposti all'intercettazione; il ricorso alla crittografia divenne indispensabile.

All'inizio della Grande Guerra la stazione radiotelegrafica italiana di Codroipo era in grado di intercettare i messaggi austriaci ma non di decrittarli. Per rimediare il Comando Supremo inviò il Cap. Sacco in Francia, ma i francesi si rifiutarono di istruire gli italiani sui metodi utilizzati.

Luigi Sacco

Crittanalista e ufficiale dell'Esercito, nella primavera del 1916 propose e ottenne di istituire un Ufficio Cifra italiano tramite il quale riuscì a decrittare i cifrari campale, diplomatico e navale austriaci e alcuni cifrari tedeschi in uso nei Balcani.

Pubblicò il *Manuale di Crittografia,* nato come manuale per crittografi e crittanalisti, ma che è una vera e propria storia della crittografia fatta di procedure definite in dettaglio e con matematica precisione.

Seconda Guerra Mondiale

Enigma e Ultra

La presentazione in ambito civile/commerciale della prima versione di macchina Enigma attirò l'attenzione dei servizi crittografici militari di varie nazioni che si convinsero che garantisse assoluta sicurezza nelle comunicazioni radiotelegrafiche criptate.

Un gruppo di criptoanalisti polacchi, adottando tecniche di analisi di vario tipo (statistica, matematica e ottico/meccanica) riuscirono a decodificare parte delle radiocomunicazioni tedesche in onde corte e nella tarda primavera del '39 decisero di condividere il loro segreto con colleghi stranieri, avendo percepito dalle intercettazioni l'intenzione tedesca di invadere la Polonia.

Il governo britannico acquisì queste informazioni e creò un centro, presso Bletchley Park, per cercare di forzare il sistema di cifratura tedesco e quindi la cifrante Enigma. Le operazioni di decodifica utilizzarono dapprima macchine elettromeccaniche, derivate dai prototipi realizzati dai polacchi, le "bombe", successivamente vennero realizzati rudimentali calcolatori elettronici utilizzanti tubi a vuoto o valvole.

I programmi di gestione del calcolatore furono elaborati grazie al contributo di Alan Turing, creatore della omonima macchina virtuale.

Al termine del conflitto Ultra fu sciolta e le migliaia di persone che avevano collaborato furono vincolate al segreto, mantenuto addirittura sino agli anni '90.

Cifrario SOE (Special Operations Executive)

Derivazione del cifrario di Vigénère, utilizzava alfabeti in ordine casuale concordato, rendendo più difficile la crittanalisi statistica. La segretezza si basava non solo sulla chiave, ma anche sulla tavola polialfabetica, che andava custodita con la massima attenzione.

Il cifrario fu usato durante la Seconda Guerra Mondiale dagli agenti dello *Special Operations Executive (SOE)* britannico; la tavola era scritta su fazzoletti di seta, mentre le frequenze radio ed eventuali chiavi e disposizioni transitorie erano scritte su carta di riso. L'agente che fosse stato catturato dal nemico, doveva immediatamente incendiare il fazzoletto (la seta brucia molto rapidamente) o ingoiare la carta di riso.

Alan Turing (1912-1954)

Operò presso Bletchley Park dal 4 settembre 1939 all'estate 1944 ed è uno dei più grandi matematici del XX secolo, fra i fondatori dell'informatica teorica.

Il lavoro eseguito da Alan Turing e dai suoi colleghi poté essere pubblicamente apprezzato solo molti anni dopo, quando cadde il segreto militare sulle tecniche di crittoanalisi eseguite. A lui si deve gran parte del merito del forzamento del codice della macchina Enigma, per il quale si servì di gigantesche macchine calcolatrici, che possono considerarsi i precursori dei moderni computers.

Genio indiscusso, personalità singolare, vagamente fobica, affascinato dalla favola di Biancaneve raccontata in quegli stessi anni da Walt Disney, morì misteriosamente avvelenato nel 1954 proprio mangiando una mela.

APPARATI IN MOSTRA

SCHEDE TECNICHE

ENIGMA

Concepita in Germania al termine delle Prima Guerra Mondiale, venne realizzata e prodotta nel 1923 in una versione primitiva proposta in ambito commerciale, successivamente adottata dalle Forze Armate tedesche in varie versioni civili e militari.

Le ridotte dimensioni ne consentirono la distribuzione anche a piccoli reparti, il facile impiego ne favorì la produzione in decine di migliaia di esemplari ed è oggi conservata come prezioso cimelio presso musei e collezionisti privati.

Il principio di funzionamento risiedeva in una crittografia polialfabetica attuata a mezzo di un sistema elettromeccanico a rotori, cablati in modo unico e segreto; fu imitata prima e dopo il Secondo Conflitto Mondiale con esiti non altrettanto brillanti e fu altresì "protagonista" di pellicole di successo, romanzi, pieces teatrali, nonchè descritta in numerosi libri a carattere tecnico.

L'alimentazione a batteria o esterna di emergenza, eventualmente derivabile da un automezzo, serviva unicamente ad illuminare gli indicatori luminosi durante la digitazione dei testi. Per l'impiego servivano un operatore per la digitazione e uno per la lettura.

Collezione Rover Joe

SCHLUESSELGERAET SG 41

"Hitlermuhle" ovvero il mulino di Hitler

Progettata in piena Seconda Guerra Mondiale, entrò in servizio nel 1944 con la prospettiva di sostituire la macchina Enigma presso le Forze Armate tedesche, benché la stessa fosse considerata comunque sicura.

Adotta un meccanismo tipo Hagelin con rotori non cablati e differisce dalla M209 americana per la tastiera molto più pratica di tipo alfabetico (forze terrestri e navali) o numerica (forze aeronautiche), quest'ultima destinata principalmente alla trasmissione di messaggi codificati per le previsioni meteorologiche.

Gli eventi bellici ne impedirono la diffusione in servizio, che fu limitata a poche centinaia di esemplari; la maggior sicurezza intrinseca rispetto ad Enigma, che era stata forzata, avrebbe potuto influire efficacemente sulle sorti del conflitto.

Il nomignolo "mulino di Hitler" è suggerito dalla presenza della manovella sulla destra, necessaria per il funzionamento completamente meccanico. Il testo veniva stampato su nastro di carta che fuoriusciva dalla parte posteriore sinistra.

Collezione Rover Joe

HAGELIN M209

Macchina di ridotte dimensioni, progettata e prodotta dalla ditta svedese Hagelin in più di centomila esemplari per l'uso da parte delle Forze Armate USA durante il Secondo Conflitto Mondiale, rimase in servizio sino a tutta la guerra coreana, intorno alla metà degli anni '50.

Completamente meccanica, non necessitava di alimentazione elettrica; dotata di sei rotori, prevedeva l'introduzione del testo impostando una lettera alla volta mediante la manopola sulla sinistra.

Essendo non particolarmente complessa, era possibile per il nemico violare il segreto dei messaggi piuttosto rapidamente ma, essendo impiegata esclusivamente per uso tattico, la decodifica da parte del nemico era ottenuta dopo che l'azione si era già conclusa.

Il testo era prodotto in forma scritta su nastro di carta del tipo impiegato sulle telescriventi.

Collezione Rover Joe

NEMA (NEue MAchine)

Progettata e realizzata nel corso del Secondo Conflitto Mondiale da un'azienda Svizzera, derivava dalla versione commerciale di Enigma acquisita dall'esercito elvetico fin dagli anni '30 con il nome di K Swiss; di essa conservava il caratteristico indicatore alfabetico ausiliario rimovibile il cui uso avrebbe impedito all'operatore di vedere l'esito della cifratura. E' rimasta in servizio per alcuni decenni sia in ambito militare che diplomatico.

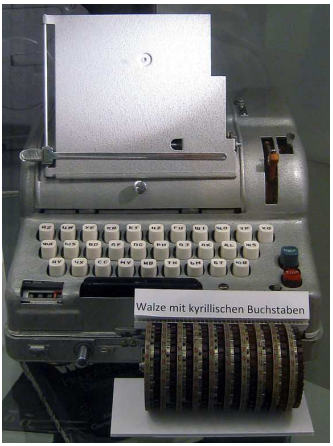
Utilizza dieci rotori il cui movimento risulta complesso e mutevole durante le operazioni di codifica/decodifica. Sebbene dismessa dal servizio, ancora oggi presenterebbe notevoli difficoltà di violazione anche con l'ausilio delle tecniche informatiche attualmente disponibili.

Alimentata da batteria o da rete, poteva essere collegata ad una telescrivente esterna e ad un indicatore del numero di lettere digitate.

Collezione Rover Joe

FIALKA (M125)

Imitazione post-bellica di Enigma realizzata negli anni ‘50 dall’Unione Sovietica in numerose versioni fornite anche ai Paesi aderenti al Patto di Varsavia o alleati, ne esistono quindi versioni con tastiere in caratteri latini o in caratteri cirillici. Rimase in servizio sino ai primi anni ‘90, al dissolvimento dell’Impero Sovietico.



E’ dotata di dieci rotori il cui senso di rotazione muta in modo pseudo-casuale e, diversamente da Enigma, non presenta indicatori luminosi alfabetici ma produce direttamente un testo scritto su nastro cartaceo.

Permette anche la trasmissione radiotelegrafica dei testi, potendo produrre anche un nastro nel codice Baudot tipico delle macchine telescriventi. La tecnologia impiegata sfrutta dispositivi elettronici a stato solido introdotti all'epoca: i transistori.

Con la cifrante KL7 – Adonis, in dotazione al Patto Atlantico, è stata protagonista della crittografia durante la Guerra Fredda.

Collezione Rover Joe

TSEC/KL-7 (Adonis, Polluce)

Macchina cifrante elettro-meccanica off line, derivata da Enigma, sviluppata dalla National Security Agency (NSA) USA, introdotta nel 1952 come principale dispositivo di cifratura della NATO con il nome di AFSAM-7, rimase in servizio fino al 1983. Anche conosciuta come Adonis (ad alto livello) e Polluce (a basso livello), era fondamentalmente una versione avanzata della macchina Enigma tedesca.

Relativamente leggera (9.3 kg), simile ad una telescrivente, rappresentava il top della tecnologia degli anni '50; era dotata di otto rotori che alloggiavano in un cestello rapidamente sostituibile che facilitava le operazioni di impostazione giornaliera della chiave, normalmente sostituita alla mezzonatte GMT.

Presenta una tastiera intelligente, progettata con un bordo permutatore scorrevole, un interruttore complesso necessario per cambiare la direzione del segnale attraverso il gruppo rotore e tubi a vuoto per il controllo dei segnali di temporizzazione del sistema della stampante.

Alimentazione esterna a 24 Vcc, un motore principale che girava a 6600 RPM e spingeva le parti meccaniche, generatore di corrente alternata che forniva la 400V per pilotare le valvole. Il prodotto finale era una stampa su strisce strette di carta dove c'era la codifica del messaggio.

Collezione MARITELE Roma

HAGELIN BCX - 621/B

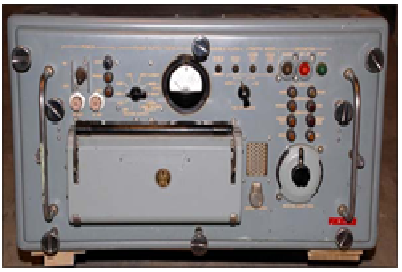
Derivata dalla Hagelin CX52 e simile a M 209, ne conservava il principio di funzionamento pur essendo dotata di motore elettrico e di tastiera alfabetica. La ditta costruttrice svedese, nel secondo dopoguerra si era spostata in Svizzera e produsse svariate versioni della macchina, che trovò largo uso anche presso gli organismi governativi italiani, rimanendo in servizio sino agli anni '80.

Queste macchine ebbero grande successo grazie codici di cifratura molto difficili da "forzare", anche con gli standard attuali, e ebbero larga diffusine sia in ambito militare che civile.

Collezione Scuola TLC delle FF.AA. di Chiavari

TSEC/KW-37 T e R

Nome in codice JASON, era un sistema di crittografia sviluppato nel 1950 dalla National Security Agency USA per proteggere le trasmissioni della US Navy e della NATO, consentendo alle navi di ricevere rapidamente messaggi e ordini, in sostituzione dei codici cartacei manuali; permetteva di mantenere il silenzio radio ed evitare quindi l'intercettazione e la determinazione della posizione in mare.



La catena di codifica e decodifica si basava su due componenti, la KWR-37 R (unità ricevente) e il KWT-37 T (unità trasmittente).

La 'chiave' di decodifica era una scheda perforata in modo casuale, che veniva sovrapposta ad un pannello con sensori posto sul frontale della macchina; la posizione dei fori sulla scheda abilitava il contatto elettrico dei sensori e stabiliva la chiave di cifratura giornaliera. Ogni scheda perforata aveva abbastanza combinazioni di chiavi da coprire 14 anni di utilizzo prima che la combinazione si potesse ripetere.

Ogni nave aveva almeno due KWR-37 R, che decrittavano i messaggi cifrati dai KW-37 T installati presso le strutture a terra, dove si trovavano i trasmettitori ad alta potenza.

Il KWT-37 T era composto da un intero rack con 5 unità sovrapposte:

- KW0-37, unità per le verifiche e gli allarmi, posizionata in alto;
- KWx-37, unità switch Timer e alimentazione, posizionata in basso.
- Tra i due si trovavano tre unità di trasmissione, denominate "Transmit Unit", le quali avevano il compito di produrre la stessa sequenza di codice e le cui uscite venivano combinate in un circuito di miscelazione che inviava il "verme di cifratura" ai ricevitori. Questa particolarità, oltre a garantire la cifratura dei messaggi, assicurava una maggiore protezione all'intera catena, essendo questa connessa ad apparati radio sempre in trasmissione. Il "verme di cifratura" veniva trasmesso costantemente anche in assenza di traffico per non dare punti di riferimento sulla partenza del KWT-37 ad un potenziale intercettatore.

Nel dopoguerra, con l'aumento vertiginoso del traffico radio, si rese necessario accoppiare alla cifrante una telescrivente. Nel 1968, dopo la cattura della USS Pueblo da parte della Corea del Nord, fu modificato il generatore di chiavi. Il sistema è rimasta in servizio fino ai primi anni '90.

Collezione Scuola TLC delle FF.AA. di Chiavari

TSEC/KW-7 (Oreste)

Macchina cifrante elettronica on-line sviluppata dalla National Security Agency USA intorno al 1960, divenuto il principale dispositivo di cifratura della NATO fino alla fine degli anni '80; nota come TSEC/KW-7 o Oreste.

E' una delle prime macchine cifranti completamente elettroniche, usata per inviare messaggi tramite una telescrivente su circuiti radio HF/UHF, fra nave - terra/terra-nave e nave - nave.

Alloggiata in un contenitore metallico a forma cubica, con tutte le connessioni sul retro e relativi controlli sul davanti, ospitava sul frontale il dispositivo di inserimento KYK-1 (cipolla) della chiave cifrante tramite dei penzoli.

I circuiti stampati erano dei moduli, differenziati dal colore a secondo del tipo di circuito, che avevano all'interno migliaia di transistor, tra i quali il 2N404, introdotto da RCA nel 1957, che è stato un transistor in lega di germanio PNP molto diffuso all'epoca.

Collezione Scuola TLC delle FF.AA. di Chiavari

TELSY TDS-2003

Dispositivo di cifratura telefono portatile della serie TDS-2000, introdotto da Telsy a Torino (Italia) intorno al 1980, fu acquisito dalle Forze Armate e dalla Polizia e restò operativo fino alla fine del 2000. Costruito all'interno di una valigetta standard di Delsey, molto comune negli anni '80, aveva alimentazione da rete nella parte frontale. Effettuava una cifratura bidimensionale tramite uno scrambler di divisione di tempo e di frequenza.

Collegabile direttamente ad una linea telefonica analogica (PSTN), nel caso in cui non fosse disponibile una linea diretta poteva essere utilizzato anche con l'accoppiatore acustico integrato e telefono esterno di interfaccia alla linea PTT.

Nascosto all'interno del accoppiatore acustico c'era un comune microfono di ricambio, da utilizzare nel caso in cui quello dell'ufficio/stanza fosse spiato, cosa molto frequente durante la Guerra Fredda.

Collezione Museo Tecnico Navale

TELSY TDS-2004

Dispositivo di crittografia vocale per l'uso su reti telefoniche analogiche (PSTN), introdotto da Telsy a Torino (Italia) attorno al 1981, rappresentava la versione da tavolo del 2004-M, del quale condivide l'elettronica; in produzione fino a metà degli anni '90.

Effettuava due modalità di cifratura: a divisione di tempo o divisione di tempo e di frequenza, in funzione della chiave in uso. Poteva immagazzinare fino a 9 chiavi di cifratura, impostabili tramite il selettore sul frontale.

L'immagine mostra il TDS-2004 con l'apparato telefonico D-2000, versione modificata del Krone FeTAp 752, dotato di tastiera che non supportava la selezione a toni DTMF. I pulsanti permettevano il passaggio della conversazione da "in chiaro" (CL) a "crypto" (CR) a "privata" (P). L'interruttore Push-to-Talk (PTT) era utilizzato solo in modalità half-duplex.

Una volta caricate le chiavi nell'unità principale, l'utente poteva controllare tutte le funzioni dal telefono. Una chiamata in chiaro veniva visualizzata tramite un LED rosso sul tasto CL (CLEAR). Una volta stabilita la connessione, una delle parti premeva il pulsante di CR (CRYPTO) per passare in cifrato e si accendeva il led verde corrispondente.

Il TDS-2004 conteneva due schede elettroniche principali e un alimentatore rimovibile (PSU); nella parte superiore si trovava la circuiteria analogica, mentre in quella inferiore i circuiti digitali. Queste due schede erano identiche alle schede utilizzate nel TDS-2004M e nel TDS-2003.

Collezione Museo Tecnico Navale

TELSY TDS-2004M

Dispositivo di crittografia vocale mobile, rappresenta la versione mobile del TDS-2004, montato in un cassetto metallico a standard militare anti urto, è rimasto in produzione fino a metà anni '90.

Effettuava due modalità di cifratura: a divisione di tempo o divisione di tempo e di frequenza, in funzione della chiave in uso. Poteva immagazzinare fino a 9 chiavi di cifratura, impostabili tramite il selettore sul frontale.

Per impostare una chiave, il selettore sulla destra del pannello frontale deve essere posizionato su "SET KEY (INS COD)", il selettore sul lato sinistro sul numero corrispondente alla memoria di immagazzinamento desiderata e il pomello centrale su "CLEAR(CHIARO)". Quindi si inserivano da 1 a 8 cifre, costituenti la chiave, ruotando il selettore sul numero desiderato e il pomello centrale su "CRYPTO" per memorizzarli.

L'immagine presenta un modello costruito nel 1991, verso la fine della vita operativa.

Collezione Museo Tecnico Navale

MACCHINE ECCEZIONALMENTE PRESENTI PER

L'INAUGURAZIONE DELLA MOSTRA

ENIGMA M4

Versione voluta dalla Marina tedesca, entrata in servizio nel 1942 principalmente a bordo degli U-boote impiegati in Atlantico nell'attacco dei rifornitori Alleati provenienti dagli USA. I sommergibili in emersione comunicavano utilizzando messaggi di durata brevissima per ridurre il rischio di intercettazione e individuazione radiogoniometrica.

L'utilizzo della cifrante unitamente al codice Shark impedì per mesi ad Ultra di decodificare le comunicazioni radiotelegrafiche tedesche.

Dotata di quattro rotori operativi con incise 26 lettere (invece che numeri), di cui il primo a sinistra non era mobile nelle fasi di codifica/decodifica e il suo posizionamento in "A" determinava la perfetta compatibilità di M4 con le macchine standard M3 o tipo I in uso presso le forze armate tedesche.

Collezione Mr John Alexander

TYPEX MK III

Cifrante portatile britannica, emanazione di Enigma, entrata in servizio nel 1937 per le Forze Armate britanniche e di alcuni membri del Commonwealth, basata su cinque rotori dotati di tacche multiple che, se inserite, ruotavano i rotori adiacenti, ed un riflettore rotante; i primi due rotori rimanevano fissi durante la cifratura.

Il testo veniva scritto con la mano sinistra mentre con la destra l'operatore ruotava una manopola; la velocità era solo di circa 60 lettere al minuto.

La cifrante riceveva in ingresso il messaggio in chiaro che veniva cifrato automaticamente, trasmesso in un'unica fase e, sempre in automatico, decifrato e stampato in ricezione.

Collezione Mr John Alexander

OMI Nistri

Derivata dalla Enigma tedesca, fu prodotta in pochi esemplari dalla O.M.I. di Roma ed impiegata dalle Forze Armate italiane a partire dagli anni '50.

Dotata di sette rotori, cinque nel modulo crypto, uno nel modulo scrittura e un riflettore, di una tastiera con 25 tasti alfabetici, un tasto speciale, che serviva da "spazio" in modo crypto e da lettera W in decodifica, e un pulsante per il movimento continuo.

Consentiva la stampa del testo su nastro di carta, velocizzando le operazioni di lettura e verifica,

Supportava l'alimentazione in corrente alternata a 120 – 160 – 220 – 260 Volt 42 – 50 Hz o in corrente continua a 12 Volt DC.

La ditta Nistri operava a Roma fin dalla Prima Guerra Mondiale per la produzione di apparecchi per la ricognizione aerea e il tiro; durante il Secondo Conflitto Mondiale si specializza in apparati strategici. Al termine del conflitto dovette riconvertirsi ad usi civili.

Collezione Mr John Alexander

Il Museo Tecnico Navale della Marina Militare

Ogni Museo è una storia e il Museo Tecnico Navale ne racconta una particolare che guarda all'uomo, alla sua capacità di confrontarsi con il mare, elemento da sempre amato e temuto, e con la tecnologia, che gli ha permesso di superare difficoltà un tempo insormontabili.

Scopo del Museo Tecnico Navale è celebrare l'ingegno umano, la tecnologia, frutto dell'ingegno, gli eroi i quali, grazie all'ingegno e alla tecnologia, hanno compiuto imprese memorabili.

Amedeo VII di Savoia realizzò la prima base navale sabauda a Villefranche sur mer sul finire del XVI secolo e progressivamente iniziò la raccolta di cimeli che nel 1775 fu organizzata a museo; allo scoppio della Rivoluzione Francese il museo fu trasferito a Cagliari, poi a Genova e nel 1870, con l'Unità d'Italia e la costruzione dell'Arsenale Militare, alla Spezia e ci rende oggi il museo navale più antico del mondo.

Le raccolte del Museo Tecnico Navale sono in continuo ampliamento e oggi spaziano su vari settori: polene, mezzi d'assalto, esplorazioni polari e subacquee, comunicazioni marconiane, modellismo e architettura navale, armi da fuoco, siluri e artiglierie navali, propulsione, fari e segnalamenti, navigazione e attrezzatura, bandiere di combattimento, uniformologia, medaglie, sigilli e fregi che offrono una vastissima panoramica sulla storia e sulle tradizioni della marineria in generale e della Marina Militare in particolare. Documenti e oggetti testimoniano le opere di personaggi leggendari come Millelire, Des Geneys, Cavour, Garibaldi, Chiodo, Saint Bon, Brin, Marconi, Duca degli Abruzzi, Calderara, D'Annunzio, Rizzo, Rossetti, Nobile, Cattaneo, Tesei, Faggioni, Arillo e ne garantiscono un immortale ricordo.

Una visita al Museo Tecnico Navale costituisce un approccio che realizza appieno lo scopo per il quale esso fu istituito: mantenere vivo il culto delle tradizioni della Marina Militare, raccogliere e degnamente custodire il suo passato di gloria, di ingegno, di onore e documentare l'evoluzione della tecnologia nel settore marittimo.

Direttore del Museo è il C.V. Silvano Benedetti.

L'Associazione Culturale Rover Joe

Rover Joe è un associazione storico culturale, fondata e supportata da Alberto Campanini, con lo scopo di collezionare, restaurare e mostrare al pubblico le tecnologie elettroniche ed i sistemi di radio comunicazione impiegati durante il Secondo Conflitto Mondiale; il suo impegno vuole essere un tributo alla memoria di quanti hanno contribuito, con le loro capacità e soprattutto col loro ingegno, alla realizzazione di veri e propri capolavori d'ingegneria.

All'attenzione dedicata agli oggetti si affianca la ricerca e lo studio della documentazione tecnica e storica degli apparati e delle attrezzature.

Presso la sede di Fidenza (PR) sono raccolti e conservati migliaia di apparati per telecomunicazioni originali, dei quali viene curato il restauro, la manutenzione e l'esposizione al pubbico in occasione di mostre e convegni; tra essi, alcune macchine "Enigma" in buone condizioni di funzionamento, per le quali l'Associazione è stata invitata a tenere conferenze e dimostrazioni in numerosi ambiti culturali e istituzionali.

Perché il nome Rover Joe?

Il nome trae origine da un sistema di comunicazione ideato dall'Esercito degli Stati Uniti nella Seconda Guerra Mondiale proprio per la campagna d'Italia: un sistema radio mobile istallato su jeep Willys equipaggiata di due apparati radio per la comunicazione con le truppe terrestri e l'aviazione. Il mezzo, denominato AN/VRC-1 o, più spesso, con il nickname di "Rover Joe", ha coordinato gli interventi dell'aviazione statunitense lungo le linee mobili del fronte, innovando significativamente le comunicazioni tra Forze Armate diverse che, fino ad allora, erano a comparti stagni.

Bibliografia

http://crittografia.altervista.org/crittografia/timelinecritto.html

http://www.cryptomuseum.com/crypto/telsy/tds2003/index.htm

http://www.radiomilitari.com

Fabrizio Palmieri: Crittografia – Le origini, il Medioevo, La Grande Guerra

http://en.wikipedia.org

Il Museo Tecnico Navale e l'Associazione Rover Joe ringraziano tutti coloro che hanno contribuito alla preparazione della mostra *Crypto – Parole (s)velate* e alla redazione di questo catalogo.

In particolare, preme sottolineare la competenza e la disponibilità del C.C. Antonio Pappaluca di MARITELE Roma, del 1° Mar. Antonio Di Benedetto di MARITELE La Spezia, del Sig. Fabrizio Palmieri dell'ARI La Spezia e della Scuola TLC delle FF.AA. di Chiavari, senza i quali la mostra non avrebbe visto la luce; inoltre, un ringraziamento a Mr. John Alexander, collaboratore del National Museum Of Computing (UK), per l'entusiasmo con cui ha aderito alla nostra iniziativa.

Non dimentichiamo i nostri fucilieri!

Support our marines!

MUSEO TECNICO NAVALE