COMUNICAZIONE CRIPTATE: LA CIFRATRICE "ENIGMA"

Un breve resoconto tra spionaggio e "controspionaggio radio" durante la seconda guerra mondiale,con la preistoria dell'informatica moderna attraverso aneddoti e personaggi storici e mitici: Turing padre dell'informatica e Fleming futuro scrittore di James Bond!

la Bomba

BREVE STORIA.

La crittografia ha origini che si perdono nella notte dei tempi, pensate messaggi segreti cifrati "semplici" furono costruiti per primi da assiri, ebrei, egiziani e indiani. Il primo a usare "in pratica" un sistema di sostituzione alfabetica semplice e rozzo fu addirittura Giulio Cesare,che scriveva invece di ogni lettera quella situata tre posti piu' in la nell'alfabeto:semplice ma geniale vista epoca. Nel 1466 Leon Battista Alberti (musicista,pittore e scrittore) inventa il sistema POLIALFA

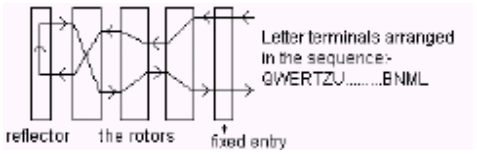
BETICO, mentre 100 anni dopo il bresciano Giovan Batista Belaso pubblico' una raccolta di cifrari e invento' la **CHIAVE**, costituita da una parola o frase che serviva appunto per codificare o decifrare un testo.
Peccato che per lunghi messaggi specie in uso militare era un sistema complicato e ingestibile bisognera' quindi attendere l'applicazione della CHIAVE alle macchine meccaniche.I sistemi migliori forse in assoluto, probabilmente anche forse per la loro estrema ingenuita',furono quelli adottati dai vari eserciti nella seconda guerra mondiale, vedi i soldati americani che usarono per le loro comunicazioni "criptate" gli indiani navajo (con ordine di ucciderli in caso di cattura) o il nostro esercito che usava i telefonisti sardi! Ma tornando alla nostra breve storia arriviamo alle macchine meccaniche. Il concetto del 1466 del Alberti fu ripreso nel XX secolo (tutto ritorna!) da vari inventori, che realizzarono telescriventi equipaggiate con una sequenza di **ROTORI** mobili. Questi ruotavano di uno o piu' passi, seguendo varie regole, a ogni carattere battuto sulla tastiera. La codificazione derivante era la **POLIALFABETICA**. Il primo brevetto fu conseguito nel 1919 dall'olandese Alexander Koch, e poi lo cedette al tedesco Arthur Scherbius. Nel 1917 invece antisegnano delle future comunicazioni criptate fu un ingegnere della AT&T americana Gilbert S.Vernam che collego' insieme due telescriventi, il segnale poi dalle due macchine veniva inviato a un circuito elettromeccanico che provvedeva alla codifica e trasmissione.

ENIGMA

E arriviamo al fulcro di questo articolo. Fu proprio il tedesco Scherbius che costrui' la macchina criptatrice ENIGMA che fu alla base della famiglia di macchine usate sia dai nazisti che dai giapponesi nella seconda guerra mondiale. Predecessore di enigma fu la "ruota di Jefferson" considerata il piu' antico esemplare di apparecchiatura crittografica "meccanica". Ma cosa che forse sconcertera' i piu', e' che gli alleati abbiano ricevuto aiuti "decisivi" per il loro lavoro di decriptazione dei vari messaggi Enigma dalle spie, che rivelavano loro i codici e le chiavi segrete,da incursori o da pure azioni militari (ma a volte per puro caso!), in cui si sottraevano i manuali con i codici e chiavi o addirittura le macchine criptatrici complete. Insomma non per deludere il pensiero romantico e di poesia della criptoanalisi "pura", ma molte volte e' stata la fortuna, il caso o la forza bruta che ha permesso ai suddetti di risolvere casi altrimenti impossibili! Queste affascinanti vicende furono narrate anche sul grande schermo vedi il film del 2000 "U-751" che trattava della cattura di un enigma su un u-boot e da "Enigma" del 2001 che trattava invece delle bombe (vedi piu' avanti) e della decifratura.

Nata come abbiamo visto per superare i cifrari manuali, Enigma come tutte le macchine cifranti inventate nei primi vent'anni del Novecento tento'di superare quei problemi e limitazioni utilizzando un sistema meccanico che generava "automaticamente"una chiave di lunghezza tale che consentiva di inviare centinaia e finanche migliaia di messaggi e cosa straordinaria senza MAI ripeterne la sequenza, punto debole di tutti i vecchi sistemi di criptazione! Inoltre, non era limitata a ventisei diversi alfabeti cifranti ,ma poteva attingere da milioni di diversi alfabeti;e il numero di sequenze di chiave possibili risultanti dal combinare meccanicamente questi milioni di alfabeti in varie combinazioni che potevano facilmente far raggiungere anche milioni di milioni. Per cambiare la cosi detta chiave bastava semplicemente riprogrammare un selettore o spostare una spina, il risultato equivaleva a inventare un cifrario completamente nuovo. Ma sopra tutto, cosi finalmente si eliminava la fatica di codificare e decodificare il messaggio: il testo veniva battuto sulla tastiera e il testo cifrato usciva immediatamente e viceversa.

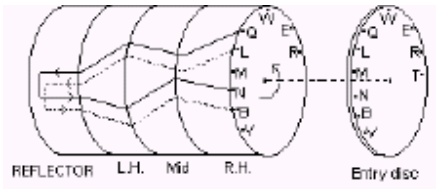
FUNZIONAMENTO
Invenzione di Scherbius,era come nelle altre macchine rotanti una serie di dischi rotanti (agli ini zi solo 3 poi si arrivo' fino a 8!) che modificavano l'alfabeto cifrante. Ciascuno di questi tre dischi, chiamati **ROTORI**, presentavano ventisei contatti elettrici (le 26 lettere del alfabeto) su ciascuna delle loro faccie. Una normale tastiera attivava i contatti elettrici che iniziava il processo di codifica, i contatti elettrici poi ovviamente erano collegati all'interno della stessa in modo "irregolare". In definitiva Enigma era cosi composta:



I 3 ROTORI schema di codifica.

Sequenza:

TASTIERA
E VISORE --------→ STATORE --- ROTORE -- ROTORE—ROTORE <---RIFLETTORE



la funzione del riflettore come dice il termine stesso chiudeva il percorso del segnale elettrico e lo faceva ritornare indietro verso i rotori allo statore e quindi finalmente al visore che visualizzava la lettera codificata. Chiaramente il tutto funzionava al contrario cioe' un messaggio da decrifrare veniva sempre digitato in tastiera e appariva poi sul visore decodificato: semplice e geniale. Per complicare ancor piu' il lavoro di intelligence dei servizi segreti inglesi e americani vennero poi apportate durante il conflitto mondiale varie modifiche:

- aggiunta di nuovi ROTORI, come abbiamo visto da 3 fino a 8 (la Kriegsmarine).
- cavallotti mobili nei contatti elettrici di ritorno del segnale nel RIFLETTORE.
- aggiunta di un pannello di commutazione con spinotti mobili tra TASTIERA e STATORE.

Facciamo un semplice esempio (si fa' per dire!) sul funzionamento del Enigma:
Il contatto numero 1 sulla faccia destra poteva essere collegato al contatto numero 22 sulla fac cia sinistra; il 2 poteva essere collegato al 5; il 3 al 16 e cosi' via. Allorche' la corrente elettrica giungeva sulla faccia sinistra del primo rotore, attivava i contatti sulla faccia destra del rotore successivo,dove avveniva un'altro scambio di lettera e cosi' via. Ricordate che ciascuna faccia dei ROTORI aveva 26 contatti elettrici su ciascuna delle sue faccie. Ogni qual volta si premeva un tasto, il rotore di destra (il primo) avanzava di una tacca, cioe' compiva un ventiseiesimo di giro, spostando cosi' di una posizione tutti i suoi contatti elettrici. Una volta che il primo rotore aveva compiuto un giro completo, una ruota dentata faceva avanzare il rotore centrale di una tacca; allorche' anche questo completava un giro, il rotore di sinistra avanzava di una tacca.Og ni qual volta, uno o piu' rotori avanzavano, le interconessioni elettriche tra essi cambiavano e quindi i loro relativi percorsi del segnale elettrico, facendo si' che la corrente attraversasse i tre (poi cinque) rotori lungo un percorso diverso dal precedente. In tal modo, ciascuna lettera del messaggio veniva cifrata con un alfabeto completamente diverso; solo dopo che tutti i tre roto ri avevano compiuto un giro completo la "chiave" si sarebbe ripetuta.Cio' significa che era pos sibile digitare circa 17.000 lettere senza MAI riutilizzare la stessa sequenza di "chiave",veramen te ingegnoso! Non mi dilungo oltre essendo questo solo inizio della spiegazione del funziona- mento della macchina Enigma e non vorrei annoiare oltremodo il lettore, quindi passiamo alla descrizione storica dei passi salienti durante il secondo conflitto mondiale che l'ha vista assolo- ta protagonista.

La tabella di codifica dei 26 indicatori.

A TABLE OF TWENTY-SIX INDICATORS.																			
1	2	3	4		5	6	7	8			1	2	3	4		5	6	7	8
A	O	Q	S		T	R	T	N			D	Z	Y	P		G	B	I	R
T	R	X	N		Q	L	D	S			X	Q	O	W		Z	H	U	M
P	V	E	Q		A	W	Q	T			N	D	L	F		D	P	F	B
H	J	P	T		K	U	G	Q			M	C	K	O		X	G	O	H
R	S	C	Y		F	F	E	V			W	N	S	D		J	Y	H	X
U	U	I	V		N	C	L	Y			Q	X	A	A		C	M	R	I
O	I	N	G		W	Q	S	J			J	A	H	C		O	V	N	K
Y	E	B	J		S	D	Y	G			B	W	R	B		E	E	V	Z
C	M	V	R		L	K	C	F			K	H	G	X		I	I	J	D
F	T	W	U		Y	N	W	L			L	K	T	E		P	O	X	F
I	P	J	Z		V	A	M	S			S	F	F	M		B	Z	P	W
G	B	Z	H		U	S	Z	O			V	G	M	I		H	J	B	A
E	L	D	L		R	X	A	U			Z	Y	U	K		M	T	K	C

Esistevano vari codici (le varie "chiavi" di codifica per settare le diverse Enigma a seconda del le loro destinazioni) chiamati con vari colori e poi con nomi:

“CHIAVI”:

Codice Porpora = famoso codice Giapponese

Chiave Rossa / Marrone /azzurra = Luftwaffe (aviazione tedesca)

Chiave Gialla = Wermacht (forze armate tedesche)

Chiave Blu = Kriegsmarine (marina militare tedesca e sommergibili)

Chiave Arancione = S.S. (polizia criminale)

codici con nomi:

Luftwaffe = primula/calabrone/vespa/scarafaggio
scorpione (coordinamento con esercito)

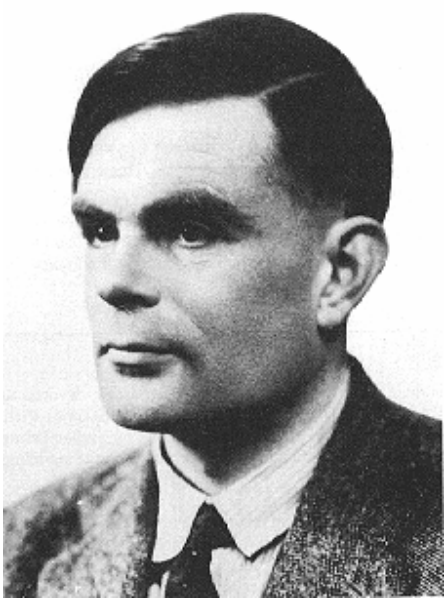
Wermacht = fringuello (panzer del Afrika Korps)
fenice (a livello armata)
avvoltoio (sul fronte russo)

Kriegsmarine = delfino (fronte atlantico e baltico)
focena (mediterraneo)
squalo (sottomarini U-Boot)

Gia' nel 1936 vennero "violati" i codici Rosso e Blu e uno dei maggiori successi prebellici fu la decrittazione nell'estate del '36 di una serie di messaggi della marina nipponica sui risultati del collaudo della corrazzata Natago. Ma i tedeschi non stava no con le mani in mano e cosi' nel 1939 sia gli americani che gli inglesi brancolavano nel buio. Nel marzo del '39 le truppe tedesche invadevano la Cecoslovacchia. Grazie al preziosissimo e fondamentale aiuto dei polacchi (Rejewski e altri) gli alleati riuscirono ad avere delle repliche quasi perfette delle Enigma tedesche. Avere le macchine non bastava bisognava farle funzionare, quindi si decise di reclutare uomini e donne nelle maggiori universita' inglesi quali Oxford e Cambridge ma anche a in quelle di Londra e Edinburgo. Vennero tutti portati nelle famose baracche poste a Bletchley, sito a meta' strada appunto tra Oxford e Cambridge, ove nacque il famoso "gruppo di Bletchley"(narrato anche in un film) fra i quali vi lavorava anche il mitico Alan Turing uno dei padri dell'informatica e dell'intelligenza artificiale (del 1936 la sua "macchina di turing"). Questo sito diviso in baracche di cui Turing era a capo della baracca 8, e ogni baracca aveva il compito di violare o decrittare messaggi specifici di una sola for za armata. Qui, nacquero le famose BOMBE, cioe' repliche della Enigma collegate fra loro, si incomincio' dalle 2 polacche poi con 4 fino alle 30 bombe del 1942. Pensate che solo per la manutenzione venivano impiegati alla fine del conflitto ben 256 meccanici della RAF e 1676 Wrens (ragazze) addette solo per farle funzionare. Nel 1944 gli inglesi contavano solo per la decrittazione di 3.722 persone ,mentre gli americani nel loro SIS Signal Security Service dell'esercito ben 10.371 addetti. Il problema principale e poi rilevatosi cruciale in molti casi, fu che i due servizi segreti lavoravano indipendentemente e si fidavano poco uno dell'altro, fomentati poi dalla vanagloria di arrivare per primi gli uni rispetto agli altri nella violazione di chiavi o codici nuovi. La parola collaborare era vista come un boccone amaro, da assaporare solo se costretti dai tristi e luttosi eventi che incalzavano sempre piu'. Ma per tutto il conflitto il cruccio principale fu che quando Turing e il suo gruppo riusciva a fare qualche piccolo passo avanti nel

la decrittazione dei messaggi i tedeschi arrivavano con macchine o codici nuovi, costringendoli a ripartire da capo. Uno dei tanti fu nel gennaio 1941 quando un documento catturato rivelo' che i famosi sottomarini U-Boot avrebbero da li' a poco usato una nuova macchina Enigma denominata in codice "M4", in cui il riflettore standard sarebbe stato sostituito con un riflettore sottile e ai 3 rotori si sarebbe aggiunto un quarto con la lettera greca beta.L'aggiunta di un quarto rotore avrebbe moltiplicato per ventisei il numero di possibili combinazioni dei rotori. Solo la verifica di tutti gli ordini nei rotori delle Bombe inglesi avrebbe richiesto 336x26 = 8736 tornate , nel peggiore dei casi cioe' ben 4000 ore od oltre 150 giorni di funzionamento! E, anche facendo funzionare le Bombe a pieno ritmo per violare la chiave di ciascuna giornata(e si perche' ogni giorno doveva venire cambiata la chiave di codifica dei messaggi!) occorrevano due settimane.Come si puo' ben intuire i problemi erano enormi, ma il personale e la buona volonta' fu molta, peccato che alla fine malgrado soprattutto gli inglesi ma anche gli americani riuscirono a decrittare molti messaggi segreti importanti (se non addirittura basilari in certi casi per la anticipata fine della guerra) ma "assolutamente" non recepiti dai capi di stato maggiore e generali e quindi sfortunatamente ignorati il piu' delle volte.La criptoanalisi in quel contesto storico era agli albori e non veniva neppure considerata scienza ma un gioco per enigmistici, e questo peso' molto sulla sua attendibilita' verso le strategie militari.

Come abbiamo visto oltre al famoso Turing nel gruppo di Bletchely troviamo un altro personaggio a noi tutti noto per la famosa saga dell'agente 007, ebbene si arrivo' il capitano di corvetta Jan Fleming dei servizi segreti navali che invio' una nota geniale all'ammiraglio Godfrey,dimostrando gia'da allora il suo brillante talento che poi diede vita al personaggio di James Bond. Propose di ottenere dal ministero dell'aereonautica inglese un bombardiere tedesco in grado di volare, scegliere un equipaggio di 5 persone vestite in divisa tedesca in grado di parlare la lingua e di aggiungere sangue e bende in modo appropriato. A quel punto far schiantare aereo nella Manica dopo aver trasmesso un SOS ai servizi di salvataggio, e una volta a bordo della nave di soccorso tedesca, sparare all'equipaggio gettarlo in mare e condurre la nave tedesca con Enigma e relativi cifrari e codici in un porto inglese. Notare che, come pilota Fleming candido' esso stesso, per citare come fosse oltremodo pure corraggioso e temerario oltre che con un fervida fantasia. Fu perfino trovato l'equipaggio e la missione prese il nome di OPERAZIONE RUTHLESS (senza pieta') ,peccato che in zona non vi fossero navi nemiche e l'operazione fu cancellata il 16 ottobre 1940.


Turing

SPIONAGGIO VIA RADIO

Vediamo un proficuo connubio tra decifrazioni e triangolazioni radio: il caso della corazzata BISMARK. Il 18 maggio del 1941 la Bismark salpo',scatenando una caccia epica, pecca to pero'che la baracca 8 non fosse ancora in grado di leggere i codici dell'ENIGMA navale. Infatti, il 24 maggio la Bismark distrusse incrociatore inglese da battaglia Hood, la piu' famosa delle navi della flotta di Sua Maesta'. Non potendo leggerne i messaggi il gruppo di Bletchley Park avevano scoperto spiando i segnali radio che il controllo radio era passato da Willhelmshaven al centro radio a Parigi, segno evidente che la nave si stesse dirigendo verso i porti francesi. Il fato volle che il generale Jeschonnek,avesse a bordo della Bismark un figlio guardiamarina, il generale (cuore di padre!) invio un messaggio alla nave pero' fortunatamente per gli inglesi non con la chiave navale fino a quel momento inespugnata ma bensi' con la chiave Rossa dell'aereonautica, chiedendo dove stesse dirigendosi la Bismark e di conseguenza il figlio. I messaggi furono prontamente decrittati e scoperta la posizione della nave inviati due biplani dalla portaerei Ark Royal che la bombardarono e immobilizzarono. Il mattino dopo le corazzate King GeorgeV e la Rodney la finirono.

Nel 1943 la sfida tra criptoanalisti giunse a un punto morto e per di piu' neppure la triangolazione radio serviva molto; l'Atlantico infatti era talmente zeppo pieno di U-Boot che un cambio di rotta non rappresentava piu' un informazione utile come per il caso sopra della Bismark. Ammiraglio Doniz poi, aveva imposto il massimo silenzio radio ai suoi sottomarini comunicazioni radio brevi e solo per il tempo necessario. Ma l'avvento di nuove tecnologie stava cambiando il corso degli eventi. Gli alleati avevano cominciato a equipaggiare gli aerei di ricognizione con "nuovi" **RADAR con lunghezze d'onda di 10 cm** quindi molto piu' precisi,contro i quali i ricevitori di allarme tedeschi erano inefficaci. Allora Ammiraglio Doniz ordino'di pitturare gli u-boot con vernice anti-infrarossi che invece si rivelo' un gros so errore, infatti tale pittura non faceva altro che accrescere l'impronta radar .

Dopo lo smacco americano di Pear Harbor, i codici della versione enigma giapponese (chia matio codice viola) furono decrittati nell'atollo di Midway, dagli analisti diretti dal comanda

nte J.Rochefort. I giapponesi usavano anche un nomenclatore (una zona chiamata con un codice) per confondere ancora di piu'e indicarono il loro prossimo obiettivo con AF. Rochefo rt intui' che AF stava per Midway e furbescamente invio' un messaggio radio "in chiaro" in cui diceva che a Midway si era rotto impianto di dissalazione.I giapponesi ritrasmisero in co dice l'informazione: "manca acqua dolce in AF", confermando ipotesi di Rochefort. Cosi' lo ammiraglio Nimitz dispose le sue 4 portaerei in posizione e riporto' la piu' famosa vittora alle Midway affondando le 4 portaerei giapponesi dell'ammiraglio Yamamoto.

I tedeschi facevano comunque di tutto per complicare il piu' possibile le intercettazioni radio dei loro messaggi: cambiavano continuamente frequenze, modificavano quotidianamente i segnali di chiamata di ogni stazione radio, inviavano traffico fittizio, facevano usare la la stessa frequenza a reti diverse. Tutto cio' complicava ulteriormente la decrittazione dei messaggi e richiedeva una attenta ricerca della banda radio in uso.Tra altro gia' nel 1940 sia la marina che esercito americana avevano costruito proprie reti di stazioni radio di monitorag gio senza alcun coordinamento reciproco. Gia' dagli anni venti e trenta l'arma della marina aveva una piu' spiccata inclinazione tecnica rispetto all'esercito, anche perche' la loro linfa vitale erano le navi mentre esercito faceva ancora fatica ad abbandonare i cavalli! Il direttore delle comunicazioni navali nel 1930, il capitano Hooper, era un grande sostenitore della radio ed e' certamente grazie a queste persone umili ma illuminate che dobbiamo i fatti a cui poi siamo arrivati in questo scritto. Egli fece installare il primo posto di intercettazione nel consolato americano di Shangai nel **1924**, una stazione temporanea alle Hawaii e a est di Honolulu nel 1925 e nel 1927 stazioni permamenti a Guam e nelle filippine. Sperimento' anche stazioni radio di intercettazione a bordo di navi. Allorche' scoppio la guerra in Europa furono anche installate stazioni radio sul Canale di Panama, in Texas, in California e nel NewJer sey.In quel periodo infatti, buona parte del traffico transatlantico e transpacifico consegna to dalle societa' telegrafiche viaggiava via radio, anziche' cavi sottomarini: cosicche' era ovvio che se si aveva a disposizione una stazione radio in una posizione strategica si sarebbe potuto intercettare tutto questo traffico. Di norma nelle ambasciate non era consentito avere collegamenti radio diretti con le rispettive capitali, cosicche' i telegrammi diplomatici cifrati in entrata e in uscita dall'America venivano trasmessi da queste societa' commerciali. Inoltre, gli apparati militari delle nazioni straniere mantenevano le proprie reti di stazioni radio;tali canali utilizzati per comunicazioni a lunga distanza (tra le quali quelle tra Tokyo e e le Mandate Island nel Pacifico controllate dal Giappone) viaggiavano sulle **ONDE CORTE** che come ben sappiamo si propagano nella ionosfera e possono essere quindi captate anche a grandissime distanze dal loro punto di origine. Tutto consisteva nel identificarne le frequenze in uso per ogni determinato paese e decrittarne tutto il relativo traffico.

STAZIONI RADIO

Alla fine del 1943 il servizio decrittazioni della marina americana aveva in servizio attivo ben 445 stazioni riceventi a onda corta, che alla fine della guerra arriveranno a 775. Solo a Washi ngton ben 120 riceventi, 75 in California e 200 a Wahiawa nelle Hawaii. Il traffico degli U-Boot veniva interamente intercettato a Chatham, Cap Code e Massachusetts. Grande aiuto fu' fornito prima dall'NCR poi dai tecnici e ingegneri della IBM per la costruzione delle BOMBE americane.

Mentre la Royal Navy inglese disponeva di 172 stazioni radio, l'Esercito inglese di 169 stazio ni radio, la RAF di 265 stazioni radio, il Foreign office di 187 stazioni e il Post Office (le poste) di 17 stazioni radio di ascolto e intercettazione. A cio' si aggiungevano le stazioni in Canada a Malta,Gibilterra,Alessandria d'Egitto,Cairo,Baghdad, Egitto e in Sud Africa e India.

CURIOSITA' TECNOLOGICHE

Anche una famosa stella di Hollywood fu famosa nello spionaggio tecnologico: Hedy Lamarr. Morta nel 2000, divenne famosa per il primo nudo al cinema nel film ESTASI del 1932. Brevetto' infatti nel 1942 un sistema di controllo radio delle torpedini che e' alla base dello SPREAD SPECTRUM, la tecnologia delle comunicazioni su cui si basano oggi alcuni telefoni cellulari e satelliti militari . Lo fece per aiutare il suo paese contro il nazismo. La sua idea si basava sul principio di dotare le torpediniere americane di controllo radio indecifrabile dal nemico.Anziche' su un'unica frequenza, facile da intercettare e bloccare bisognava usare piu' frequenze e sempre diverse. Sfortunatamente per quei tempi, la tecnologia non permetteva i prodigi tecno logici e di miniaturizzazione attuali, quindi essendo troppo ingombrante non fu adottato dalla marina militare. Ma nel 1957 la Sylvania electronics (grazie al transistor) lo realizzo' e cosi' l'invenzione dell'attrice venne impiegata per la prima volta nel blocco navale di Cuba nel 1962.Per questo importante brevetto l'attrice non ricevette un soldo, ma non se ne rammarico' era con tenta di aver potuto aiutare il suo paese.

Fleming papa' di 007 !

AVVENIMENTI STORICI.

1940 GC&CS Nessun successo sull'Enigma marina tedesca.
1940 SIS nessun successo codice porpora giapponese.

1941 GC&CS: nessun successo sulla chiave Enigma esercito tedesco.
decrittate chiavi della Luftwaffe
Feb. : decrittate Enigma marina tedesca. Sugli U-Boot nuova Enigma M4.
Mag: catturato sottomarino U-110 e recuperata un Enigma della Marina
con i Bigrammi (codici).
Giu: Invasione russa - Operazione Barbarossa
Set: A Bletchley Park piu' di 1.000 dipendenti per la decritt.codici enigma.

Viene forzato il codice dell'esercito e cifrario manuale "Darsena".

Nov: Da stallo a troppo lavoro per decrittare tutti i messaggi dell'esercito, marina e aviazione tedeschi.
In uso 6 BOMBE, gli inglesi decodificavano "solo" loro tutto il traffico tedesco, mentre americani il traffico giapponese. Non accettano collaborazione degli americani perche' Enigma "e' affare solo loro!".
Gli americani usano macchine IBM per decrittare.

Dic: Attacco giapponese a Pearl Harbor.

1942 Giu: decrit. codici navali e traffico diplomatico giapponese dagli americani.

Lug: 169.000t. di navi tedesche affondate (rifornimenti per Rommel).
Ago: Decrit.chiave esercito cosi Montgomery sconfigge Rommel in africa.
Set: Inglesi hanno ora in uso 30 BOMBE.
Ott: Battaglia di El-Alamain.
Nov. Decrittata chiave Squalo (U-Boot nel atlantico).

1943 Americani decrittano codice "Floradora"usato dai diplomatici tedeschi.

MAR: Americani costruiscono 96 BOMBE.
LUG: Ecatombe di U-Boot nell'Atlantico grazie ai nuovi radar!
AGO: Tutto il traffico degli U-Boot sara' decodificato fino a fine guerra!
DIC: Americani hanno 144 BOMBE.

1944 Colpisce la prima bomba V-1 su Londra.

FEB: Americani la marina ordina altre 50 BOMBE.
GIU: D-Day
LUG Fallito attentato alla vita di Hitler
SET: Primo missile V-2 su Londra
DIC: Offensiva alle Ardenne

1945 A gennaio forzato l'inespugnabile blocchetto monouso tedesco.

APR: Roosvelt muore.
APR: Hitler si suicida nel bunker a Berlino.
MAG: La Germania si arrende.
AGO: Lancio bombe atomiche Yoroshima e Nagasaky
AGO: Il Giappone si arrende.

Si puo' notare come la decrittazione sia stata se non fondamentale, almeno essenziale per la fine del secondo conflitto mondiale con la vittoria degli alleati.

IL FUTURO

Il governo americano negli ultimi anni ha tentato di introdurre il DES (Data Encryption Standard), un sistema crittografico sviluppato alla NSA la sicurezza nazionale americana. Il governo pretendeva che "tutti" i messaggi scritti utilizzassero questo standard ma i privati ovviamente hanno resistito sostenendo che la NSA intendeva procurarsi un economico e facile sistema

per decifrare tutti i messaggi privati. Recentemente la stessa DES non certifichera' piu' questo sistema non ritenuto piu' sicuro, conclusione: i sistemi sicuri esistono ma sono complessi da capire ma sopra tutto da USARE! Ad esempio su internet viene da tempo usato il PGP (Pretty Good Privacy), basato su una "chiave" pubblica resa nota a tutti e una privata che abbiamo solo noi e il nostro corrispondente, ha un livello di sicurezza abbastanza buono. Mentre per le transazioni bancarie sempre su internet spesso si usano sistemi semplici come "RO13"che sostituisce ogni lettera con quella che la segue di 13 posizioni, ma anche con sistemi molto complessi e impenetrabili. Ma come ormai avrete capito la "battaglia crittografica" procede e uno studente ventenne di elettronica e' infatti riuscito a sfondare l'algoritmo del sopra citato PGP di Phil Zimmermann, (una crittografia a ben 128 bit)che si stimava assolutamente inespugnabile!
Ma i primi mesi del 2003, i ricercatori del laboratorio informatico del Politecnico di Losanna (LASEC) hanno violato il mitico **codice SSL**(indicato nel browser da un piccolo lucchetto giallo). , quello usato per impedire che durante i pagamenti via web, i numeri delle carte di credito possano essere intercettati . E non e' neppure la prima volta che il codice SSl viene violato, ma la vulnerabilita' scoperta ora mette seriamente in discussione l'affidabilita' del sistema.Inventato da Nestcape alla meta' degli anni '90, questo codice e' stato poi anche adottato da Microsoft e Opera nei rispettivi software per navigare in internet.

GLOSSARIO:

ABWHER Controspionaggio tedesco

BOMBA Piu' macchine Enigma collegate insieme: erano armadi di 2 metri di altezza con 3 file di 10 enigma collegate per un totale per bomba di 30 equivalenti enigma.

CHIAVE Parola o frase per codificare un messaggio.

C-38 HAGELIN Enigma italiana.

GC&CS Scuola intercettazione britannica, era a capo il mitico "C".

OSS Servizi Segreti poi diventati la CIA.

OP-20-G Servizi decrittazioni della marina americana.

MADAM-X Bomba americana dell'esercito (IBM).

SIS Genio Segnalatori americano

SIGABA macchina cifrante americana dal 1940.

TYPEX macchina cifrante inglese.

ULTRA messaggi cifrati segreti inglesi (i famosi messaggi ultra).

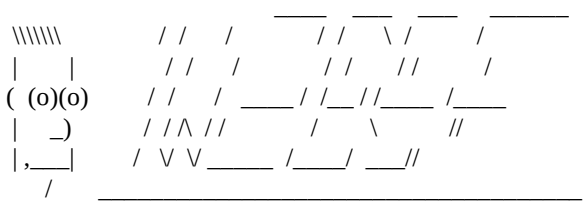
Bibliografia:

The Codebrakers -David Khan (oltre 1000 pagine!)
Crittologia - Berardi/Beutelspacher
Enigma – Budiansky

www.dxworld.com/cryptos.html sito di base !!!

www.eclipse.net/~dhamer/download.htm doc in PDF

http://frode.home.cern.ch/frode/crypto/simula/index.html simulatore in DOS



www.elio.org/iw2bsf e-mail: iw2bsf@amsat.org

"The space is my hobby"