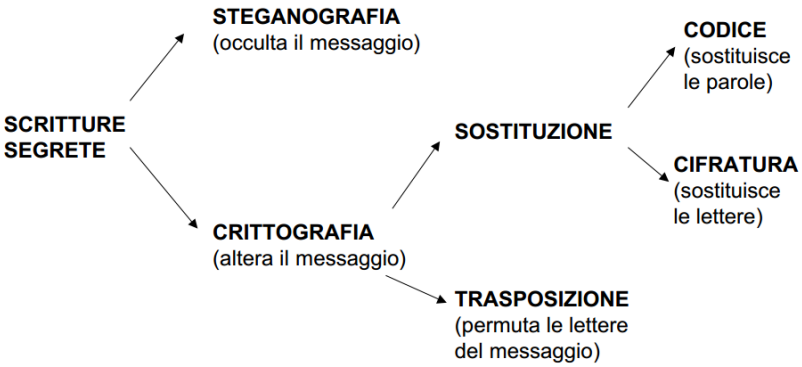
Schema lezione

- Presentazione e definizioni

A) steganografia (inchiostro simpatico, microdot…)
B) crittografia-crittoanalisi → trasposizione
→ sostituzione

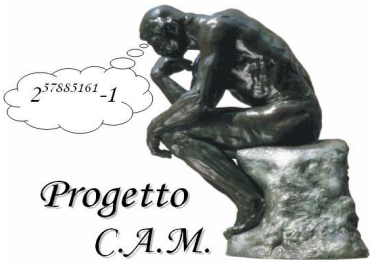
Che cos'è la crittografia



- Distinzione fra cifrare – decifrare e codificare -decodificare
- Utilizzo: tradizionale (militare: guerre, complotti) e moderno (comunicazioni in rete, acquisti online)
- Crittografia nella storia:
  - Antichità (scitale, Erodoto)
  - Cifratura di Cesare
  - Rinascimento: Leon Battista Alberti – Blaise de Vigenere
  - Sostituzione monoalfabetica e polialfabetica
  - Babbage
  - Sviluppo macchine: dai dischi rotanti alla macchina Enigma
- Passaggio dalla chiave unica alla chiave pubblica
- Matematica e crittografia

Esercizi – laboratorio

"Ciò che un uomo può inventare, un altro uomo lo può scoprire " (Sherlock Holmes)



Che cos'è la crittografia

La crittografia è la scienza che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggio.

Prima che una disciplina scientifica, la Crittografia era una pratica, un insieme di regole, di metodi, di strumenti. Era diventata quasi un'arte: l'arte di scambiarsi i messaggi senza farne capire il reale contenuto, anche se erano intercettati. Una disciplina dallo statuto ambiguo, al limite della magia e dell'esoterismo. Si ha a che fare con problemi di spionaggio, di nemici desiderosi di venire a conoscenza delle informazioni che scambiamo con i nostri alleati, per servirsene a nostro danno.
Si capisce che l'origine è antica, legata non solo ad esigenze commerciali, ma soprattutto diplomatiche e militari. È noto che in molti casi le sorti dei conflitti sono state decise da questa capacità di conoscere, con buon anticipo, le mosse dell'avversario. Poi, l'avvento delle reti di comunicazione digitale, utilizzate regolarmente nella vita quotidiana, ha richiesto nuove esigenze di sicurezza e di tutela della *privacy*. E la Matematica - in particolare la Teoria dei numeri - ha fatto cambiare natura alla Crittografia, liberandola dalla sua aura di mistero e trasformandola da un'arte in una scienza.

La crittografia nella storia

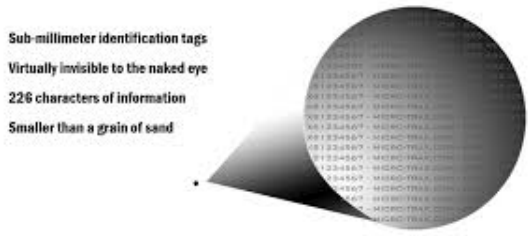
"steganografia" (è nascosto il messaggio e non il significato)
Tra i primi esempi di scrittura segreta vera e propria si citano alcuni geroglifici egiziani che potrebbero essere crittografati[1].
Possono essere trattati come esempi di crittografia anche le lingue morte (o, da un punto di vista personale, qualunque linguaggio o modalità di scrittura che non ci sia noto).

[1] Si hanno prove di geroglifici " non standard" e di una tavoletta babilonese del 2500 a.C. che contiene termini crittografati

I) Erodoto (*libro VII delle Storie*)
Demarato per avvisare gli Spartani del prossimo attacco del re persiano Serse alla Grecia prese una tavoletta doppia, ne raschiò la cera e poi sul legno della tavoletta scrisse il piano del re. Fatto ciò versò di nuovo cera liquefatta sullo scritto, in modo che, venendo portata vuota, la tavoletta non procurasse nessun fastidio da parte dei custodi delle strade (prima della battaglia di Salamina,
480 a.C.)

II) Erodoto (*libro V delle Storie*)
"Istieo voleva dare ad Aristagora l'ordine di ribellarsi, non aveva alcun altro modo per annunziarglielo con sicurezza, essendo le strade sorvegliate, fatta rasare la testa al più fido degli schiavi, vi impresse dei segni, e aspettò che ricrescessero i capelli. Non appena ricrebbero, lo spedì a Mileto, non comandandogli null'altro se non che, quando giungesse a Mileto, dicesse ad Aristagora di fargli radere i capelli e di guardare la sua testa: i segni impressi ordinavano, come già prima ho detto, la rivolta."

E' una forma di steganografia anche la scrittura con inchiostri cosiddetti simpatici. Nel I secolo d. C. Plinio il Vecchio insegnava che dal lattice di titimabo si può ricavare un inchiostro invisibile. Trasparente una volta asciutto, il lattice vira al marrone se esposto a un calore moderato (questo comportamento è legato alla presenza del carbonio).
Nel XVI secolo lo scienziato Gianbattista Della Porta spiegò come comunicare tramite un uovo sodo, preparando un inchiostro con 30 g di allume in mezzo litro di aceto, e usandolo per scrivere sul guscio. La soluzione penetra nel guscio, che è poroso, senza lasciare tracce, e tinge l'albume solidificato; quest'ultimo potrà essere letto sbucciando l'uovo.
Il "microdot", cioè la riduzione di uno scritto alle dimensioni di un punto, è una forma di steganografia che ebbe largo impiego durante la seconda guerra mondiale.



Tramite un procedimento fotografico, gli agenti tedeschi in America latina trasformavano una pagina scritta in una macchia con un diametro inferiore al millimetro che poteva essere nascosta nel puntino di una i. Il primo microdot fu scoperto dall'FBI nel 1941 grazie a una soffiata. Fu consigliato agli americani di cercare, sulla superficie di una lettera, un luccichio che tradiva la presenza di un messaggio.

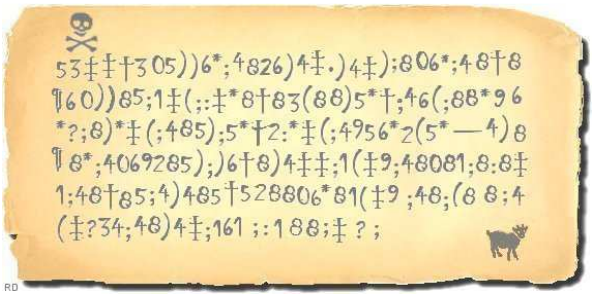
La longevità della steganografia dimostra che essa garantisce una certa sicurezza, ma il suo punto debole è evidente: la segretezza è perduta nel momento dell'intercettazione perché il testo è in chiaro.

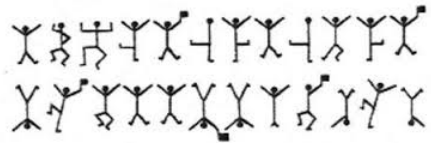
CURIOSITA '

Steganografia digitale: la steganografia al digitale ed è utilizzata per la trasmissione invisibile di messaggi. La forma di steganografia più comune consiste nel nascondere informazioni all'interno di file immagine o audio. Questa tecnica si basa sulla teoria che modifiche ai bit meno significativi delle immagini o dei file audio sono impercettibili per l'uomo e difficilmente individuabili tramite analisi statistiche a causa del rumore di fondo intrinseco dei tipi di file usati come contenitori. Micropunti fotografici: fotografie della dimensione di un punto dattiloscritto che, una volta sviluppate e ingrandite, possono diventare pagine stampate di buona qualità.

Una scitala (dal greco σκυτάλη = bastone) era una piccola bacchetta utilizzata dagli Spartani per trasmettere messaggi segreti. (Plutarco, *Vite parallele*)
• Il messaggio era scritto su di una striscia di pelle arrotolata attorno alla scitala, come se fosse stata una superficie continua.
• Una volta srotolata e tolta dalla scitala la striscia di pelle, era impossibile capire il messaggio.
• La decifrazione era invece possibile se si aveva una bacchetta identica alla scitala del mittente: vi si arrotolava nuovamente la striscia di pelle ricostruendo la primitiva posizione.

Nel 1843 uscì *Lo scarabeo d'oro* di Edgar Allan Poe, che contiene un messaggio cifrato scritto con l'inchiostro simpatico (figura a fianco)





A fianco una parte del crittogramma da "*L'avventura dei danzatori*" di Arthur Conan Doyle

NOTA: l'intercettazione e la decifrazione di messaggi sono soggette a serie restrizioni di tempo perché l'informazione deve essere ottenuta presto per poter intervenire.

RICHIESTE

- **Segretezza**: il messaggio non deve essere leggibile a terzi.
- **Autenticazione**: il destinatario deve poter essere sicuro del mittente.
- **Integrità**: il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.
- **Attendibilità**: il mittente non deve poter negare di aver inviato il messaggio.

Utilizzo tradizionale della crittografia

- Gli usi tradizionali riguardavano quasi esclusivamente gli ambiti militari e di spionaggio (sono riportati numerosissimi esempi di uso di sistemi crittografici nel corso di guerre, battaglie, rivoluzioni, cospirazioni, complotti, ...)

Utilizzi moderni della crittografia

- L'uso più importante della crittografia in ambito "civile" è quella della sicurezza delle comunicazioni in rete
- Più in particolare le applicazioni di commercio elettronico sono quelle in cui maggiormente è sentita la necessità della sicurezza e della segretezza (scambio di dati sensibili, quali il numero di carta di credito, numero di conti bancari, ecc.)

Il crittosistema di Cesare

Svetonio, nella Vita dei dodici Cesari, racconta che Giulio Cesare utilizzava un sistema di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo

·a	·b	·c	·d	·e	·f	·g	·h	·i	·l	·m	·n	·o	·p	·q	·r	·s	·t	·u	·v	·z
·D	·E	·F	·G	·H	·I	·L	·M	·N	·O	·P	·Q	·R	·S	·T	·U	·V	·Z	·A	·B	·C

Ad esempio la frase
domani attaccheremo (testo in chiaro),
diventerà
GRPDQN DZZDFFMHUHPR (testo cifrato).

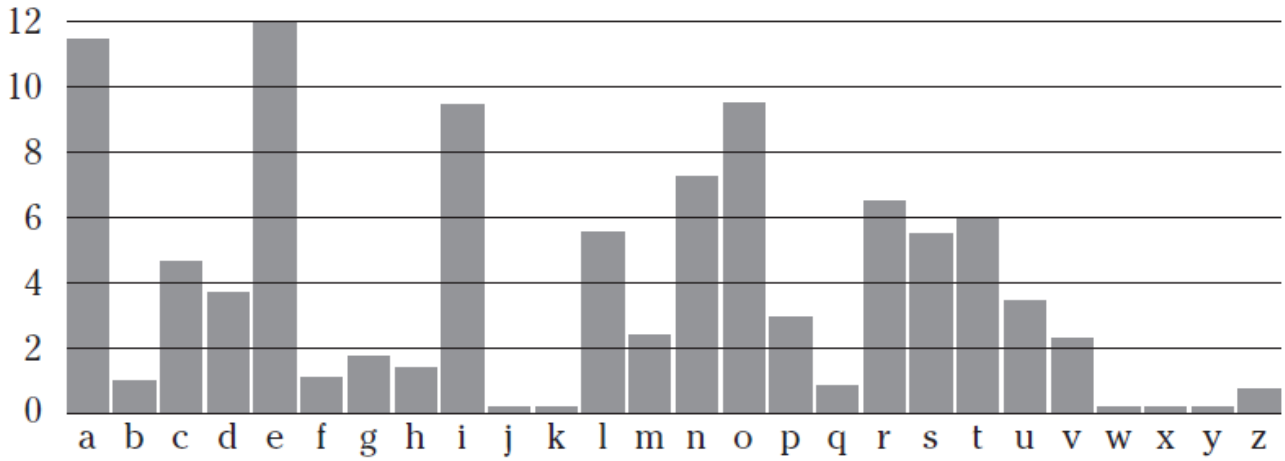
La decifrazione è altrettanto semplice, basta sostituire ogni lettera con quella che si trova tre posti prima

·A	·B	·C	·D	·E	·F	·G	·H	·I	·L	·M	·N	·O	·P	·Q	·R	·S	·T	·U	·V	·Z
·u	·v	·z	·a	·b	·c	·d	·e	·f	·g	·h	·i	·l	·m	·n	·o	·p	·q	·r	·s	·t

Come decifrare un codice monoalfabetico?
Chi intercetta un messaggio cifrato con il metodo di Cesare può limitarsi a provare successivamente tutte le possibili chiavi di cifratura e trovare il testo in chiaro in un tempo ragionevolmente breve (attacco a forza bruta). La chiave consiste nella permutazione usata come alfabeto cifrante; con 26 lettere si ottengono 26! permutazioni (circa $4 \cdot 10^{26}$). Pensando di riuscire a valutare un milione di permutazioni al secondo servirebbero circa 10^{13} anni per completare la ricerca !! Questo NON significa che la cifratura sia sicura.
Ancora oggi si utilizza la tecnica che è stata descritta dallo studioso arabo Abu Yusuf Ibn Ishaq Al-Kindi nel IX secolo che si basa sull'analisi delle frequenze. E' necessario considerare che, in ciascuna lingua, la frequenza con cui compaiono le singole lettere dell'alfabeto segue leggi statistiche abbastanza precise e lo stesso vale per le coppie e le terne di lettere Disponendo di un testo abbastanza lungo l'analisi di frequenza è molto utile. Quindi:

- sapendo che il testo è in italiano, è facile che l'ultima lettera di ciascuna parola sia una vocale (questa osservazione non è essenziale per il metodo, ma lo rende più breve)
- si cercano i simboli più frequenti nel testo cifrato
- si provano a sostituire con le lettere più frequenti in italiano
- si cerca di vedere se si riesce a "intravedere" una parte di parole
- qualche tentativo può portare a parole improbabili

Per esempio nella lingua italiana le lettere più frequenti sono nell'ordine e, a, o, i, n, r, t, l, s, ... L'istogramma mostra ciò in modo sintetico.



Il cifrario di Vigenère

• E' il più semplice dei cifrari polialfabetici.
• Pubblicato nel 1586, il cifrario di Blaise de Vigenère fu **ritenuto per secoli inattaccabile**.
• Si può considerare una generalizzazione del cifrario di Cesare: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa è spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave da scrivere ripetutamente sotto il messaggio, carattere per carattere.

<u>Sostituzione polialfabetica</u>

- Un crittosistema per sostituzione polialfabetica non usa sempre lo stesso simbolo per la stessa lettera
- Per ogni posizione del messaggio in chiaro è usato un alfabeto diverso
- Così si supera (parzialmente…) il problema della debolezza visto per i crittosistemi monoalfabetici (infatti ha "meno" senso contare le frequenze di simboli, non essendoci più corrispondenza tra lettere in chiaro e simboli cifrati).

Leon Battista Alberti aveva già proposto intorno al 1460 l'utilizzo di più di un alfabeto, ma non trasformò l'idea appena abbozzata in una tecnica ben definita. A completare l'opera provvide un gruppo di intellettuali di varia provenienza che dell'invenzione della cifratura polialfabetica realizzò anche un dispositivo meccanico, il disco cifrante, per facilitare in modo significativo la produzione di scritture segrete.

Il disco cifrante è costituito da due dischi di rame, uno di diametro leggermente maggiore dell'altro. Lungo la circonferenza di ciascun disco è riportato l'alfabeto. I dischi sono liberi di ruotare l'uno rispetto all'altro, cosicché i due alfabeti vengono ad assumere differenti posizioni relative. Quindi il disco cifrante può essere usato per crittare un messaggio con il sistema di Cesare. Per esempio, per effettuare una cifratura di Cesare con spostamento pari a 1 basta collocare la *a* interna in corrispondenza della B esterna; il disco interno rappresenta l'alfabeto normale, quello esterno l'alfabeto cifrante. Poi senza spostare i dischi si cercano le lettere del testo chiaro sul disco interno, una per volta; in ciascun caso, la lettera corrispondente situata sul disco esterno è quella da inserire nel crittogramma. Il disco per cifrare può essere considerato uno "scambiatore", in cui una lettera del testo chiaro è immessa e rimpiazzata da un simbolo differente. L'Alberti suggeriva di cambiare l'assetto del disco durante la cifratura del messaggio, realizzando in sostanza una cifratura polialfabetica anziché monoalfabetica.

La forza della cifratura di Vigenère sta nell'utilizzare non uno ma 26 alfabeti cifranti per crittare un solo messaggio. Il primo passo sta nella stesura della tavola di Vigenère: si tratta di un alfabeto chiaro di 26 lettere seguito da 26 alfabeti cifranti,ciascuno spostato a sinistra di una lettera rispetto al precedente. Perciò, la riga numero 1 rappresenta un alfabeto cifrante con uno spostamento di Cesare pari a 1 che potrebbe essere utilizzato per realizzare una cifratura di Cesare in cui ogni lettera del testo chiaro è sostituita dalla lettera che, nell'alfabeto ordinario, viene subito dopo. In modo analogo, la riga 2 rappresenta un alfabeto cifrante con uno spostamento di Cesare pari a 2, e così via. La riga in cima al quadrato, in caratteri minuscoli, è un alfabeto ordinario di 26 lettere, che permette di cifrare qualunque lettera del testo chiaro tramite uno dei 26 alfabeti sottostanti. Per esempio usando l'alfabeto cifrante numero 2, *a* è cifrata come C, mentre usando l'alfabeto numero 12, è cifrata come M. Se per crittare l'intero messaggio il mittente adoperasse un solo alfabeto cifrante, saremmo di fronte a una normale cifratura di Cesare, cioè a una scrittura segreta che come abbiamo visto non è in grado di resistere all'analisi delle frequenze. Ma la cifratura di Vigenère comporta che per ciascuna lettera del messaggio si usi una diversa riga della tavola (cioè un diverso alfabeto cifrante). Perché il messaggio possa essere decifrato è indispensabile che il destinatario sappia quale riga della tavola è stata usata per ciascuna lettera; tale scelta si effettua tramite una parola (o una frase) "chiave".

Per illustrare in che modo la chiave e la tavola possono essere usate per crittare un breve messaggio, cifriamo *non vedo, non sento, non parlo* utilizzando *Sole* come parola chiave. In primo luogo, la chiave deve essere scritta sopra il messaggio più volte di seguito senza spazi liberi, in modo che a ogni lettera del messaggio corrisponda una lettera chiave.

Parola chiave	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L	E	S	O	L
Testo chiaro	n	o	n	v	e	d	o	n	o	n	s	e	n	t	o	n	o	n	p	a	r	l	o
Testo in citra	F	C	Y	Z	W	R	Z	R	G	B	D	I	F	H	Z	R	G	B	A	E	J	Z	Z

Per crittare la prima lettera del messaggio, *n,* controlliamo quale lettera della parola chiave le corrisponde nella riga superiore. Si tratta di S, che individua una specifica riga della tavola di Vigenère: quella che inizia per S. cioè la diciottesima.
L'alfabeto cifrante che forma questa riga sarà quindi quello che useremo per sostituire la prima lettera del testo chiaro. La sostituzione si effettua individuando la colonna *n,* cioè quella la cui prima lettera è n e cercando la sua intersezione con la riga S. L'intersezione corrisponde ad una casella, che contiene il carattere F. Per crittare la seconda lettera del testo chiaro, si procede allo stesso modo. La lettera sopra o è O, la quattordicesima della tavola. Per crittare o, cerchiamo sulla prima riga la colonna o, quindi la casella corrispondente all'intersezione di questa colonna con la riga O. La casella contiene la lettera C. Ogni lettera della parola chiave definisce un alfabeto cifrante della tavola di Vigenère; poiché la chiave è formata da quattro lettere diverse. Il mittente cifra il messaggio usando quattro righe della tavola, passando da una riga all'altra nello stesso ordine in cui le lettere si succedono nella chiave.

La natura polialfabetica della cifratura di Vigenère è la causa della maggiore resistenza all'analisi delle frequenze, essa era considerata così affidabile che fu chiamata la chiffre indéchiffrable. Ma proprio la sua maggiore complessità (fattore tempo) ne ritardò l'impiego fino a quando l'invenzione del telegrafo rese indispensabile una protezione sicura delle comunicazioni.

	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
a	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
b	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	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	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

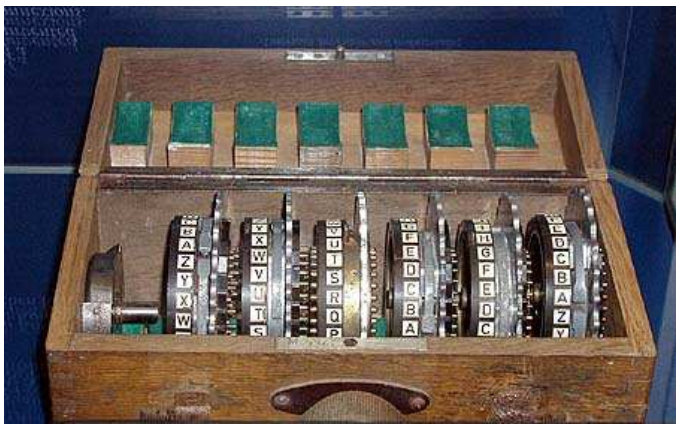
Babbage e Kasiski contro la cifratura di Vigenère

Il **metodo Kasiski** prende il nome dal maggiore prussiano Kasiski, che nel 1863 pubblicò un metodo di decifratura della tavola di Vigénère. Il maggiore Kasiski notò che spesso in un crittogramma di Vigénère si possono notare sequenze di caratteri identiche, poste ad una certa distanza fra di loro; questa distanza può, con una certa probabilità, corrispondere alla lunghezza della chiave, o ad un suo multiplo. In genere la stessa lettera con il cifrario di Vigénère è cifrata in modo diverso nelle sue varie occorrenze, ma se due

lettere del testo in chiaro sono poste ad una distanza pari alla lunghezza della chiave (od un suo multiplo), questo fa sì che siano cifrate nello stesso modo.Individuando tutte le sequenze ripetute (cosa che avviene frequentemente in un testo lungo), si può dedurre quasi certamente che la lunghezza della chiave è il massimo comun divisore tra le distanze tra sequenze ripetute, o al più un suo multiplo. Conoscere la lunghezza *n* della chiave permette di ricondurre il messaggio cifrato ad *n* messaggi intercalati cifrati con un cifrario di Cesare facilmente decifrabile. In realtà già nel 1854 lo scienziato inglese Babbage aveva individuato un criterio di decifrazione del tutto analogo a quello successivamente elaborato da Kasiski. Babbage non pubblicò mai questo lavoro[2], ma la sua scoperta emerge da un lungo epistolario ed il metodo di decrittazione è spesso chiamato Babbage-Kasiski.

NOTA: si è soliti assegnare un comportamento legittimo a chi cerca di comunicare, mentre l'intercettatore è visto sotto una luce negativa, come una persona che in maniera indebita vuole carpire i segreti altrui. Niente di più sbagliato, per quanto riguarda questa attività come vedremo con il prossimo esempio.

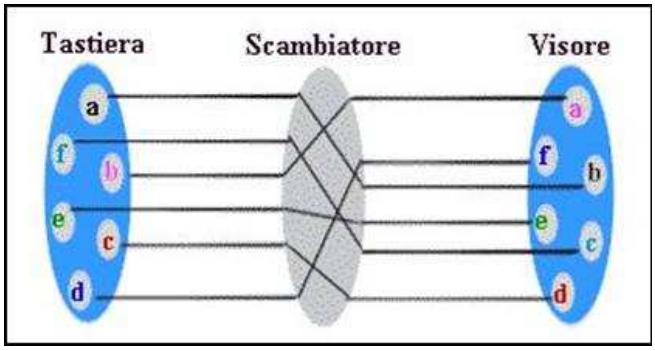
La macchina ENIGMA



I crittografi erano alla ricerca di un nuovo sistema che ripristinasse la sicurezza, soprattutto dopo l'invenzione del telegrafo senza fili. Ancora una volta il progresso delle comunicazioni acuiva la necessità di un sistema crittografico affidabile. Se non si poteva evitare che il nemico ascoltasse qualunque trasmissione via etere, si doveva almeno evitare che decifrasse quelle crittate.
Nel 1918 Arthur Scherbius e Richerd Ritter realizzarono un dispositivo crittografico che era una versione elettromeccanica più complessa e sofisticata del disco cifrante di Alberti. Questa macchina, chiamata ENIGMA, consisteva inizialmente di tre elementi collegati da fili elettrici:

- una tastiera sulla quale erano disposte le lettere dell'alfabeto ordinario per battere il testo
- uno scambiatore che era il marchingegno che permetteva la cifratura vera e propria
- un visore sul quale erano disposte tante lampadine quante le lettere dell'alfabeto, in modo che l'impulso elettrico, dopo essere stato elaborato andasse a illuminare la lampadina corrispondente alla lettera crittata.

[2] Forse Babbage non rese pubblica la sua scoperta per far mantenere il vantaggio britannico sui servizi segreti di altre nazioni.



In figura è rappresentato un alfabeto di sole sei lettere. Digitando a sulla tastiera a sinistra, la corrente entra nello scambiatore ed illumina B a destra. Ogni volta che una lettera è digitata e poi crittata lo scambiatore ruota di un posto, cambiando il modo in cui la lettera seguente sarà sostituita. L'aggiunta di un secondo scambiatore comporta il vantaggio che lo schema della cifratura non si ripete finché il secondo scambiatore non è tornato al punto di partenza, il che richiede 6 giri completi del primo scambiatore, cioè la cifratura di 6 x 6 lettere. In altre parole, due dischi con 6 posizioni ciascuno equivalgono a una sostituzione polialfabetica con 36 alfabeti cifranti. Se invece del nostro alfabeto semplificato fosse adoperato un alfabeto contenente 26 lettere, l'unità cifratrice commuterebbe in tutto 26 x 26 , cioè 676, alfabeti cifranti. Il modello base di Enigma utilizzava però 3 rotori, essa disponeva perciò di 26 x 26 x 26 = 17576 procedure di sostituzione diverse.

Supponiamo che un operatore volesse inviare una comunicazione cifrata. Prima di iniziare egli doveva regolare gli scambiatori, in modo che assumessero la posizione iniziale voluta. Le posizioni iniziali erano 17576; quella prescelta determinava il modo in cui un particolare messaggio sarebbe stato crittato. L'assetto iniziale di Enigma equivaleva alla chiave.

Grazie al "riflettore" la macchina poteva funzionare anche come decodificatrice, senza intervento specifico alcuno, cioè era necessario, prima di iniziare la decodifica, portare solo rotori e spinotti nella configurazione giornaliera prevista dai cifrari. Questa caratteristica comportava come conseguenza la "reciprocità" di codifica: se, in un determinato assetto dei rotori (e degli spinotti), la lettera B veniva, ad esempio, cifrata con una F, nel medesimo assetto, premendo il tasto F si codificava quest'ultima con B. Inoltre una lettera non poteva mai essere codificata in se stessa. La sua facilità d'uso e la sua presunta indecifrabilità furono le maggiori ragioni per il suo ampio utilizzo.

La macchina Enigma fu utilizzata dalle forze armate tedesche nel corso della seconda guerra mondiale per cifrare le comunicazioni radio tra le unità di combattimento e i quartieri generali.

La Polonia sapeva che se la Germania avesse iniziato una guerra, essa sarebbe stata la prima ad essere attaccata e chiese alla Francia i progetti e tutto ciò che era stato recuperato per la realizzazione di un prototipo per provare a violare il codice. Vista la natura tecnologica di Enigma,

Biuro Szyfrów (Ufficio Cifra) polacco decise di interpellare gli accademici della vicina Università Pozna, sottoponendoli ad un test per trovare le persone più adatte a decrittare Enigma.

I primi a decifrarla nel 1932 furono un gruppo di ingegneri polacchi.Il loro lavoro ha permesso ulteriori lavori su Enigma, sempre aggiornata dai tedeschi. La decriptazione dei messaggi cifrati con Enigma fornì per quasi tutta la seconda guerra mondiale importantissime informazioni alle forze alleate.

L'*intelligence* polacco, guidato dal matematico Marian Rejewskj, progettò una macchina apposita chiamata *BOMBA* per simulare il funzionamento di una macchina Enigma ed ottenere da un messaggio cifrato, con tentativi sistematicamente reiterati, le chiavi di regolazione della macchina che aveva eseguito la cifratura e quindi poterlo decifrare a sua volta. I tedeschi però cambiarono il funzionamento di Enigma introducendo un insieme di cinque rotori, dei quali erano usati sempre solo tre ma diversi ogni giorno: questo moltiplicava per sessanta le combinazioni possibili e

la *bomba* polacca non poteva affrontare un tale incremento di complessità. Alla vigilia dell'invasione della Polonia, nel 1939, il progetto fu trasferito agli inglesi, i quali organizzarono a Bletchley Park un'attività di intercettazione e decifrazione su vasta scala delle comunicazioni radio tedesche con un gruppo di filologi, enigmisti e con l'aiuto di grandi matematici, fra i quali il " genio" Alan Turing (1912-1954).

Ciò che è stato cifrato da una macchina può essere ancor più facilmente decifrato da un'altra macchina (Alan Turing)

I crittoanalisti partirono dall'ipotesi che in alcuni testi vi fossero delle parole note in posizioni specifiche. Ad esempio ogni giorno i tedeschi trasmettevano bollettini meteorologici che contenevano la parola Wetter (tempo atmosferico) in una determinata posizione.[3]
Nel maggio del 1941 la marina inglese riuscì a mettere le mani su un apparato Enigma intatto e sui documenti di cifratura, catturando un sommergibile tedesco durante un attacco da parte di quest'ultimo ad un convoglio alleato.

Fino a poco tempo fa si riteneva che tutti i sistemi crittografici dovessero avere chiavi simmetriche, cioè dovevano servire sia a criptare sia a decifrare. La chiave era un segreto condiviso fra mittente e ricevente.

Altre macchine ed altri sistemi fanno parte della storia della Crittografia del `900. Il sistema più noto, e che ha resistito per il maggior periodo agli assalti della decrittazione, è quello fissato in maniera ufficiale nel 1977 dall'amministrazione degli Stati Uniti, il DES (*Data Encryption Standard*), un cifrario monoalfabetico la cui sicurezza, che riposava su una chiave da 56 *bit* (di cui 8 di controllo), è stata infranta nel 1998. Questo è il primo sistema di Crittografia commerciale, che è stabilito come standard da un ente normativo, allo scopo di evitare il proliferare di sistemi cifranti incompatibili fra di loro.
Il DES esegue una serie di trasformazioni elementari ripetute più volte su pacchetti opportunamente strutturati del testo, in modo di sottoporre i *bit* che lo compongono ad una modifica globale, dipendente in maniera essenziale dalla chiave scelta: gli algoritmi sono resi pubblici; la chiave -nel rispetto più rigoroso del *principio di Kerckhoffs*- è l'unico dato fissato dall'utente.
L'aspetto importante è che la cifratura può avvenire in tempo reale con un calcolatore di media potenza. Inoltre il sistema è *simmetrico* nel senso che, come tutti i sistemi esemplificati fino a questo punto, la chiave è usata direttamente per la decrittazione.

[3] In generale, i crittografi temono ogni forma di ripetizione, perché ripetizione significa regolarità e struttura del crittogramma, sinonimo di cifratura debole.