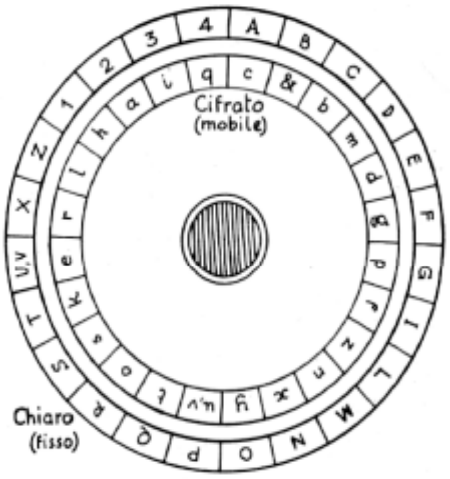


Liceo ginnasio Terenzio Mamiani
Viale delle Milizie, 30 - Roma

La matematica dei segreti

Percorso di crittografia dalla Scitala ad Enigma

di
Patrizia Cassieri

a. sc. 2012/2013

INDICE

BIBLIOGRAFIA

Simon Singh, *Codici & segreti*, saggi BUR, Milano 2011

W. Di Palma, K. Richter, S. Schoeneburg, *Bugie e segreti*, articolo

W. Di Palma, M. de Resmini, *Il crittografo di Leon Battista Alberti*, Kit interattivo , Museo della Matematica del comune di Roma

SITOGRAFIA

http://www.lnf.infn.it/media/cerruti/

http://www.cryptomuseum.com/crypto/vigenere/index.htm

http://www.bletchleypark.org.uk

INTRODUZIONE

Decine di milioni di messaggi sono inviati ogni giorno sotto forma di e-mail; il commercio elettronico è in continua espansione; il denaro si sposta nel cyberspazio; l'inoltro della dichiarazione dei redditi avviene per via telematica …….
Nell'Era dell'informazione è fondamentale proteggere i dati durante i loro spostamenti planetari.

Fornire questa protezione è compito della **CRITTOGRAFIA**.

La crittografia è, attualmente, una branca della matematica: questa concezione applicativa del pensiero astratto fu una vera e propria rivoluzione.

Per duemila anni la crittografia è stata importante solo per uomini di Stato e militari. Oggi tutti, più o meno consapevolmente, attingono alle sue risorse per salvaguardare la loro privacy.

L'evoluzione delle scritture segrete vede la dura battaglia tra **crittografi** e **crittoanalisti**. Nello sforzo di tutelare e, rispettivamente, violare la segretezza; gli opposti schieramenti hanno attinto a un'ampia gamma di scienze e specializzazioni dalla linguistica alla **matematica**, dalla teoria dell'informazione alla fisica quantistica. A loro volta, inventori e solutori di codici hanno arricchito questa disciplina e il loro lavoro ha accelerato il progresso scientifico e tecnologico.

L'analisi dei vari sistemi crittografici offre lo spunto per introdurre teorie matematiche che spesso non si incontrano nel curriculum scolastico e *sviluppare teorie matematiche non è un vezzo fine a se stesso ma trova applicazioni concrete*.

1. LE SCRITTURE SEGRETE

La scienza delle scritture segrete ha due metodi principali: la **steganografia** e la **crittografia**.

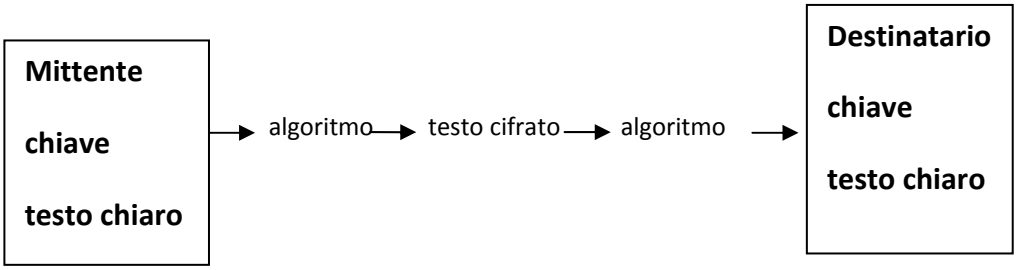
- La **steganografia** è la comunicazione segreta basata sull'occultamento del messaggio; deriva dalle parole greche *steganós* (coperto) e *gráphein* (scrivere).

L'impiego della steganografia è raccontato in vari contesti da Erodoto, ad esempio narrando la storia di Istièo che voleva incoraggiare Aristagora di Mileto a ribellarsi al re persiano. Per far giungere le relative istruzioni in modo sicuro, Istièo fece rasare il capo ad un corriere, gli scrisse il messaggio sulla cute e aspettò che i capelli ricrescessero. Il corriere attraversò indisturbato il territorio persiano. Giunto a destinazione si rasò di nuovo il capo e mostrò il messaggio al destinatario.
Nei duemila anni trascorsi dal tempo di Erodoto, varie e fantasiose forme di steganografia sono state impiegate in tutto il mondo, ma inevitabilmente molti messaggi sono stati intercettati.

Parallelamente alla steganografia si sviluppò la crittografia.

- La **crittografia** è la comunicazione segreta che non mira a nascondere il messaggio in sé, ma il suo significato; deriva dalle parole greche *kriptós* (nascosto) e *gráphein* (scrivere).

Per rendere incomprensibile un messaggio, lo si altera per mezzo di un procedimento concordato dal mittente A (da cui ALICE) e dal destinatario B (da cui BOB).
Qualunque scrittura segreta può essere analizzata in termini di metodo crittografico generale, o **algoritmo**, e di **chiave**, che definisce i particolari di una cifratura efficace.



Per cifrare il testo di un messaggio, il mittente lo introduce in un algoritmo crittografico. L'algoritmo è un procedimento generale di scrittura segreta, i cui dettagli vanno precisati scegliendo una chiave. Applicando insieme chiave e sistema cifrato a un testo chiaro, questo è trasformato in un testo cifrato, o crittogramma. Il crittogramma può essere intercettato dal nemico (EVA) durante la trasmissione, ma il nemico non dovrebbe essere in grado di decifrarlo, mentre il destinatario, conoscendo algoritmo e chiave, può ripristinare il testo chiaro.
Un cripto sistema – o sistema cifrato – è quindi un modo per render le comunicazioni più sicure. I cripto sistemi più antichi sono tutti a **chiave privata**. Chi invia il messaggio e chi lo riceve conoscono l'algoritmo che tramuta il messaggio da linguaggio naturale (in chiaro) in quello criptato e viceversa (crittografia simmetrica) e la chiave è un **segreto** tra mittente e destinatario.
La struttura generale di un cripto sistema è la seguente:

Un sistema **E** per cifrare
Il messaggio **M** in chiaro
Un sistema **D** di decifrazione
Il messaggio **C** cifrato

Dati la chiave K e il messaggio M, lo schema E produce il testo cifrato
$C = E_K(M)$, che è il messaggio cifrato.
Lo schema di decifrazione D recupera $M = D_K(C)$.
L'ipotesi fondamentale è che E_K sia una applicazione iniettiva, da cui l'impiego di permutazioni.

2. LA CRITTOGRAFIA

La crittografia si può suddividere in due tipologie, note come ***trasposizione*** e ***sostituzione***.

2.1 Cifratura per trasposizione

Nella **trasposizione** le lettere del testo in chiaro vengono mutate di posto, generando un anagramma. Ogni carattere alfabetico mantiene la sua identità.
Se la parola in chiaro è **oca** di tre lettere , le permutazioni possibili sono 6, ma si ottengono 5 anagrammi (uno è il testo in chiaro!!):
oca, OAC, CAO, COA, OAC, OCA.

Dunque una parola di **n** lettere si può permutare in **n!** (n fattoriale) modi.
Se la parola è molto lunga, ad esempio n=20 si ha n!= 2432902008176640000 che è un numero enorme e in questa circostanza la trasposizione casuale garantisce una certa inviolabilità da parte dei crittoanalisi, nel senso che questi devono lavorare su 2432902008176640000 casi possibili!!! E, naturalmente, B deve conoscere il criterio fissato per decodificare il messaggio di A.

- La prima tecnica nota di crittografia militare è la ***scitàla*** o scitale (dal greco σκυτάλη, bastone) del V secolo a.C. Si trattava di una bacchetta utilizzata dagli Spartani per trasmettere messaggi segreti. Il messaggio veniva scritto su di una striscia di pelle arrotolata attorno alla scitala. Una volta srotolata la striscia di pelle dalla scitala, era impossibile capire il messaggio. La decifrazione era possibile solo se il ricevente aveva una scitala identica a quella del mittente.

- Un altro esempio di crittografia per trasposizione è quella detta a ***inferriate***. Il messaggio in chiaro viene scritto su due o tre linee.

Se il messaggio in chiaro M è "**codici e segreti"**, questo si scrive

Prima linea	C	D	C	E	E	R	T
Seconda linea	O	I	I	S	G	E	I

Il testo cifrato C risulta **CDCEERTOIISGEI.**

2.2 Cifratura per sostituzione

Nella cifratura per **sostituzione** ogni carattere alfabetico cambia identità, ma conserva il suo posto.

- **Sostituzione monoalfabetica**

Nella V*ita dei Cesari* di Svetonio, opera del II secolo d. C., si descrive la cosiddetta **Cifratura di Cesare**, usata dal famoso generale.
Si tratta di una cifratura a sostituzione monoalfabetica. Svetonio menziona il caso dello spostamento di tre lettere.

Si tratta di un alfabeto cifrante traslato di 3 posti rispetto all'alfabeto chiaro e quindi al posto di **a** si deve scrivere **D** etc…
Considerando l'alfabeto a 26 lettere

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
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

Testo chiaro M: **codici e segreti** Testo cifrato C: FRGNFNHVHLUHZN

Si può disporre anche di una **chiave.** Scegliamo una parola chiave o una frase chiave, ad esempio JULIUS CESAR. Occorre eliminare gli spazi e le ripetizioni, la sequenza ottenuta JULISCESAR sarà l'inizio dell'alfabeto cifrante, mentre le lettere che non fanno parte della sequenza vengono aggiunte in ordine alfabetico

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

Generalizziamo e …..modernizziamo

Chiamiamo Alfabeto l'insieme dei simboli che intendiamo utilizzare.
Sia la nostra versione a 73 simboli (l'ultimo è lo spazio)
.:;?!0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzòàùèé
Ad ogni simbolo si associa un numero, nel nostro caso da 0 a 72, dove 0 è il punto e 72 lo spazio. Identifichiamo un messaggio **M** con una **successione** finita di numeri compresi tra 0 e 72 : $M= x_1\, x_2\, x_3\, x_4 \,..\, x_n$.
Lo spazio delle chiavi K contiene 72 elementi, gli interi da 1 a 72. Per ogni chiave k c'è una funzione di cifratura Φ_k così definita

$$\Phi_k(M) = \mathrm{mod}(M + k; 73).$$

Per ogni chiave k c'è anche la funzione **inversa** che decodifica

$$D(\Phi_k(M)) = \mathrm{mod}(\Phi_k(M) - k; 73).$$

Ad esempio, il codice di Cesare spostava di tre posti, dunque la sua interpretazione algebrica è: **sommare 3 ai numeri corrispondenti alle cifre e ridurre modulo 73.**

Lo spazio delle chiavi

Quando le chiavi sono poche, per scoprire il messaggio è sufficiente provarle tutte. Nell' esempio abbiamo usato 72 permutazioni cicliche dei numeri da 0 a 72.

Si può utilizzare una generica permutazione σ di questi numeri. Avremo allora $\Phi_\sigma(\mathrm{M}) = \sigma(\mathrm{x}_1)\sigma(\mathrm{x}_2) \ldots . \sigma(\mathrm{x}_\mathrm{n})$. Ci sono 73! permutazioni su 73 simboli.

L'ordine dello spazio delle chiavi è allora circa $4{,}47 \cdot 10^{105}$.

L'analisi delle frequenze

Gli **arabi** del Medioevo, non solo padroneggiavano la sostituzione monoalfabetica, ma inventarono la **crittoanalisi** . Furono i crittoanalisti arabi a trovare il punto debole della sostituzione monoalfabetica. La loro civiltà aveva raggiunto una sufficiente maturità in discipline come la matematica, la statistica e la linguistica. L'idea vincente fu quella di notare che in ogni linguaggio le lettere dell'alfabeto appaiono con una loro frequenza caratteristica e il metodo di sostituzione non altera la statistica del messaggio. Se in M una lettera compare con una frequenza del 46% allora in **C** la sua sostituta (con M non troppo breve) continua a comparire con una frequenza prossima al 46%. E questo permette una facile decodifica del messaggio da parte dell'avversario. Per secoli la cifratura per sostituzione monoalfabetica garantì la segretezza, ma lo sviluppo dell'analisi delle frequenze, nata prima in Arabia e poi in Europa, cancellò quella garanzia.

Nelle frasi in Italiano le varie lettere si trovano con le seguenti frequenze

Lettera	Frequenza %	**Lettera**	Frequenza %	**Lettera**	Frequenza %
A	11,74	**I**	11,28	**S**	4,98
B	0,92	**L**	6,51	**T**	5,62
C	4,50	**M**	2,51	**U**	3,01
D	3,73	**N**	6,88	**V**	2,10
E	11,79	**O**	9,83	**Z**	0,49
F	0,95	**P**	3,05		
G	1,64	**Q**	0,51		
H	1,54	**R**	6,37		

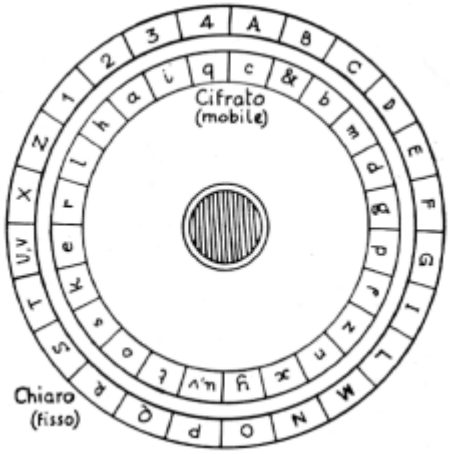
Un esempio molto bello di applicazione di questa tecnica si trova nel racconto di Edgar Allan Poe "Lo scarabeo d'oro"del 1843.

- **Sostituzione polialfabetica**

L'origine della cifratura per sostituzione polialfabetica si può far risalire ad un fiorentino del XV secolo: **Leon Battista Alberti**. Nato nel 1404, è uno dei principali esponenti del Rinascimento, di cui seppe interpretare le ambiguità e gli splendori, contribuendo a tracciare una nuova mappa di valori critici ed un diverso modo di interpretare il mondo. Alberti fu un grande architetto, un matematico, un fine letterato, un latinista, un musicista, un uomo di Chiesa ed un astuto diplomatico.
E proprio rivestendo i panni di funzionario del Vaticano elaborò un sistema crittografico semplice, ma geniale. Il metodo di Alberti realizza **permutazioni** variabili delle lettere dell'alfabeto mediante un **dispositivo meccanico**:

IL DISCO CIFRANTE

Questo è costituito da due cerchi concentrici con diametro diverso e ciascuno diviso in caselle con le lettere dell'alfabeto. Naturalmente un disco cifrante è in uso al mittente e uno al destinatario.



Sul disco grande sono riportate nell'ordine naturale le lettere dell'alfabeto e anche i numeri 1, 2, 3 e 4.

Sul disco piccolo sono presenti, in ordine casuale, le lettere dell'alfabeto e il simbolo & (et).

Mittente e destinatario concordano una **chiave segreta**, ad esempio (A,c) .

Se il mittente vuole inviare il messaggio "CODICI E SEGRETI", per prima cosa inserisce nel messaggio anche i numeri ed elimina gli spazi. Il messaggio in chiaro sarà: CODI4CI3ESEGRET2I

Posiziona poi i dischi secondo la chiave e comincia la cifratura. Ogni lettera del testo chiaro viene letta sul disco grande e si cifra con la corrispondente sul disco piccolo. Quando si incontra un numero la chiave viene cambiata leggendo la lettera corrispondente al numero stesso. Nel nostro caso il numero 4 corrisponde alla q, quindi la nuova chiave è (A,q) e così via…

Al diplomatico francese **Blaise de Vigenère**, nato nel 1523, si deve poi la forma definita di questo metodo polialfabetico. Il lavoro del crittografo francese è presente nel suo libro *Traicté des Chiffres* del 1586. La forza della cifratura di Vigenère sta nell'utilizzare non uno ma ventisei alfabeti cifranti.

LA TAVOLA DI VIGENÈRE

	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

Si tratta di un normale alfabeto chiaro di 26 lettere seguito da 26 alfabeti cifranti ciascuno spostato a sinistra di una lettera rispetto al precedente.

Cifriamo il messaggio "**codici e segreti"** adoperando la parola chiave **MONTE**.

La chiave va scritta sopra il messaggio più volte di seguito senza spazi liberi, in modo che a ogni lettera del messaggio corrisponda una lettera della chiave. Il testo in cifra si genera leggendo la prima lettera del messaggio, **c**, e la lettera della chiave che le corrisponde, M. La riga della tavola che inizia per M è la 12° e su questa riga la lettera **c** va sostituita con la lettera O e così per ogni lettera in chiaro

Chiave	**M**	**O**	**N**	**T**	**E**	**M**	**O**	**N**	**T**	**E**	**M**	**O**	**N**	**T**
Testo chiaro	c	o	d	i	c	i	e	s	e	g	r	e	t	i
Testo cifrato	O	C	Q	B	G	V	S	F	X	K	D	S	G	B

La cifratura di Vigenère resiste all'analisi delle frequenze perché una lettera che compare più volte nel crittogramma può rappresentare di volta in volta lettere diverse del testo in chiaro. Inoltre ammette un numero infinito di chiavi segrete: mittente e destinatario possono scegliere qualsiasi parola o frase.
Questa cifratura **molto sicura** è anche molto complessa e quindi non ebbe successo e fu ignorata per quasi due secoli.
Le forme tradizionali di cifratura per sostituzione secondo la sostituzione monoalfabetica erano più che sufficienti per le necessità del XVII secolo ed erano rapide, comode e ormai collaudate.

Nel secolo successivo, tuttavia la crittoanalisi raggiunse un'efficienza degna dell'incipiente rivoluzione industriale. Ogni grande potenza europea aveva la sua "**camera nera**", centro nevralgico di decifrazione dei messaggi in codice e di raccolta di informazioni riservate. A questi specialisti stipendiati quasi nessuna cifratura monoalfabetica poteva resistere.

Vista la professionalità raggiunta dai loro avversari, i crittografi furono costretti ad adottare la cifratura di Vigenère, più macchinosa, ma ritenuta ***insolubile***!!!

Oltre all'efficacia della crittoanalisi, un altro evento spinse all'adozione di procedimenti crittografi più sicuri: l'invenzione del **telegrafo** e la conseguente necessità di proteggere i telegrammi dall'intercettazione e dalla decrittazione
Anno dopo anno il telegrafo e il **codice Morse** aumentavano la loro influenza a livello mondiale, aiutando la polizia ad arrestare i criminali, i giornali a pubblicare notizie sempre più fresche, il mondo degli affari a prendere decisioni sempre più documentate, le società a effettuare transazioni superando distanze di centinaia di chilometri. La protezione di questo nuovo tipo di comunicazioni, indispensabili ma vulnerabili, diventò un problema pressante perché il codice Morse non è una crittografia, ma un alfabeto alternativo. Si pensò allora di cifrare il messaggio prima di porgerlo al telegrafista e, tra i tanti sistemi disponibili, la cifratura polialfabetica di Vigenère, soprannominata ***le chiffre indèciffrable,*** fu considerata la più adatta.

I crittografi erano in vantaggio sui crittoanalisti

Ma Charles **Babbage** e, contemporaneamente Friedrich Wilhelm **Kasiski** scoprirono il punto debole di questa cifratura.
La fondamentale debolezza della cifratura di Vigenère è la sua **natura ciclica**: se la CHIAVE SEGRETA è di 5 lettere , ogni 5° lettera del testo chiaro viene crittata tramite lo stesso alfabeto cifrante. Una volta identificata la lunghezza della chiave, il crittoanalista può trattare il testo in codice come la somma di 5 cifrature monoalfabetiche, ognuna delle quali può essere risolta con l'analisi delle frequenze. Ma, anche se la chiave è lunga quanto il messaggio, la sicurezza non è garantita.

La crittoanalisi aveva contrattaccato

Ci furono molti tentativi di escogitare nuove cifrature, ma niente di importante emerse nella seconda metà del ‘800.

Alla fine del secolo, il fisico **Guglielmo Marconi** inventò una forma di telecomunicazioni ancor più potente, e questo rese più urgente la necessità di un procedimento crittografico sicuro. Ben presto l’invenzione di Marconi ossessionò i militari che la osservavano con un misto di timore e avidità.

Con la **radio** i generali avrebbero potuto essere in continuo contatto coi reparti durante i loro spostamenti. Ma la natura ubiquitaria dei segnali radio è anche, in un contesto bellico, il loro più grande difetto.

Ancora una volta, il progresso delle comunicazioni acuiva il bisogno di un sistema crittografico affidabile.

Ma per la scienza delle scritture segrete gli anni compresi tra il 1914 e il 1918 non furono un periodo di brillanti scoperte. Gli inventori di codici escogitarono alcune nuove cifrature, ma si trattava di varianti o combinazioni di quelle del secolo precedente.

2.3 Enigma

La prima macchina cifrante è il disco di Alberti. Rimasto in uso per cinque secoli. può essere considerato uno <<scambiatore>>, in cui una lettera del testo chiaro è immessa e sostituita da un simbolo differente e il cambiamento di assetto realizza una cifratura polialfabetica. Lo strumento, quindi, cambia modo di funzionare durante la sostituzione. Cinquecento anni dopo Alberti una sofisticata rielaborazione del disco cifrante ha prodotto una nuova generazione di crittogrammi.

Nel 1918 l’inventore tedesco **Arthur Scerbius** mette a punto un dispositivo crittografico che è una versione elettromeccanica del disco di Alberti: ENIGMA.

La macchina per cifrare era contenuta in una scatola compatta di 34 x 28 x 15 cm e pesava ben 12 chilogrammi.

La versione base della macchina Enigma consiste di tre componenti collegati da fili elettrici:

- **una tastiera** per immettere le lettere del testo chiaro;
- **un’unità scambiatrice** (o rotore) che cifra la lettera trasformandola nel corrispondente elemento del crittogramma;
- **un visore** con varie lampadine che, accendendosi, indicano la lettera da inserire nel crittogramma.

L’operatore preme il tasto corrispondente alla lettera da crittare, l’impulso raggiunge l’unità scambiatrice e poi va a illuminare il visore in corrispondenza della lettera crittata. Il passo successivo consiste nel far ruotare automaticamente il disco scambiatore di un 1/26 di giro dopo la cifratura di ogni lettera. Il rotore definisce 26 diverse corrispondenze tra lettere in chiaro e cifrate, ed Enigma può essere usata

per effettuare una cifratura polialfabetica. Dopo **26** pressioni continue dello stesso tasto, il disco torna però alla posizione iniziale.

Per ridurre il numero di ripetizioni si può introdurre un **secondo rotore**. In questo modo, ogni volta che una lettera è cifrata, il primo rotore ruota di un carattere, mentre il secondo invece resta immobile fin quando il primo ha completato un giro; solo a questo punto il secondo scambiatore avanza di una posizione. L'aggiunta del secondo rotore comporta che lo schema della cifratura non si ripete finché il secondo scambiatore non è tornato al punto di partenza, il che richiede 26 giri completi del primo scambiatore, ovvero la cifratura di **26x26=676 lettere**.

Per una sicurezza ancora maggiore viene aggiunto un **terzo rotore**, per cui il numero di sostituzioni diverse è **26x25x26=16.900** (il secondo rotore effettua una rotazione in meno rispetto agli altri due, poiché dopo aver effettuato un giro completo rimane fermo una volta per far ruotare il terzo rotore).

Si può aggiungere un **riflessore,** che consiste in un disco di gomma con circuiti interni che non ruotano e i fili entrano ed escono dallo stesso lato. Col riflessore installato quando si digita una lettera il segnale elettrico attraversa i 3 rotori, raggiunge il riflessore ed è mandato indietro. Quindi il segnale elettrico passa di nuovo nei rotori, ma lungo un percorso diverso.

Per inviare un messaggio cifrato, come prima cosa devono essere regolati i rotori in modo che assumano la posizione iniziale voluta.

Le posizioni possibili sono $\mathbf{26^3 = 17.576.}$

Per decifrare il crittogramma, il destinatario deve possedere un'altra macchina Enigma, un cifrario con l'assetto dei rotori da utilizzare.

Per accrescere l'affidabilità si possono utilizzare rotori removibili e sostituibili. Quindi dati tre elementi intercambiabili essi possono essere **permutati** in sei modi differenti; con questo accorgimento il numero di chiavi aumenta di un fattore pari a sei.

Nel 1925 Scherbius organizzò la produzione in larga scala della cifratrice, che fu in dotazione alle forze armate tedesche a partire dall'anno successivo. Allo scoppio della seconda guerra mondiale, l'invenzione di Scerbius aveva messo loro a disposizione il più sicuro sistema crittografico del mondo. Ci fu un momento in cui sembrò che Enigma dovesse avere un ruolo fondamentale nel trionfo delle armate di Hitler, invece, fu la causa della loro sconfitta grazie al lavoro dei crittoanalisi di **Bletchley Park**.

Alan Mathison Turing (1912 –1954) fu uno dei più brillanti crittoanalisti che operarono in Inghilterra durante la seconda guerra mondiale. Turing lavorò a Bletchley Park, il principale centro di crittoanalisi del Regno Unito, dove ideò una serie di tecniche per violare i cifrari tedeschi, incluso il metodo della **Bomba**, una macchina elettromeccanica in grado di decodificare codici creati mediante la macchina Enigma.

2.4 Crittografia moderna

Si comincia a parlare di crittografia moderna nel dopoguerra, quando molti codici fino ad allora ritenuti sicuri cominciarono a vacillare con l'avvento della **crittoanalisi computerizzata**. Si comprese allora che la sicurezza delle informazioni cifrate deve basarsi sulla segretezza della chiave.

La svolta decisiva ci fu negli anni '70, un decennio d'oro per la crittografia, quando si formarono due scuole di pensiero: quella dei sostenitori dei cifrari a **chiave segreta** e quella dei sostenitori dei cifrari a **chiave pubblica**.

In base a queste considerazioni gli algoritmi che fanno uso di chiavi si dividono in due categorie:

Algoritmi simmetrici (detti anche a chiave simmetrica o a chiave segreta);

Algoritmi asimmetrici (detti anche a chiave asimmetrica o a chiave pubblica).

Sistemi di cifratura, ancora oggi usati, sono il DES a chiave segreta e l'RSA a chiave pubblica.

Tutti i metodi utilizzano una chiave per l'operazione di cifratura e una per l'operazione di decifrazione. Il messaggio può essere letto solo se la chiave di decifratura si accoppia con quella di cifratura, e qui sta la differenza fra i due sistemi sopra citati, in un caso le chiavi sono uguali mentre nell'altro sono diverse.

Nella **crittografia a chiave simmetrica** mittente e destinatario devono condividere una chiave tramite la quale possono cifrare e decifrare le informazioni. La chiave, però, deve essere condivisa prima di spedire il messaggio. Il problema maggiore che si incontra con questa tecnica crittografica è proprio la **condivisione** della chiave.

Per risolvere questo inconveniente la soluzione migliore è quello di rendere la **chiave pubblica**.

Ogni utente possiede due chiavi, una pubblica ed una privata: la prima viene usata dagli altri utenti che vogliono comunicare con lui in segreto, mentre la seconda viene usata dall'utente per decodificare i messaggi cifrati.

Questo tipo di cifratura si basa su alcune assunzioni della **teoria dei numeri** relative alla difficoltà, anche per un computer veloce, di eseguire particolari operazioni .

RSA, per esempio, si basa sulla difficoltà di **fattorizzare** un numero intero molto grande al fine garantire che, pur conoscendo la chiave pubblica, non esista alcun modo efficiente per ottenere la chiave privata. Da qui l'interesse della crittografia moderna per la generazione di **numeri primi** molto grandi.