



Crt

LA CRITTOGRAFIA. Dalle oscure origini al Rinascimento italiano

MICHELE ELIA

La storia della crittografia, dai tempi più antichi fino al Rinascimento italiano, è ricca d'intuizioni brillanti che formano l'attuale base scientifica della disciplina. In quest'articolo, sono ripercorse le fondamentali tappe nell'intento di descrivere i passaggi più significativi che hanno segnato l'evoluzione della crittografia da rudimentali o ingenue idee a una raffinata arte, patrimonio di élite. I due esempi, forse più indicativi, di questa evoluzione sono l'introduzione della steganografia, dove il messaggio segreto è abilmente nascosto all'interno di un testo in chiaro, e l'invenzione della chiave crittografica, un'espressione mnemonica da tenere riservata in sostituzione dell'intero algoritmo cifrante.

Non vi è nulla
che renda un uomo più sospettoso,
che il conoscere poco.
Francis Bacon



INTRODUZIONE

Le origini incerte e misteriose delle scritture segrete si perdono nei pochi secoli di storia su cui abbiamo attendibili informazioni. D'altronde, la storia delle comunicazioni segrete è sempre stata considerata tra agiografia e mito per la diffusa opinione, non del tutto infondata, che il successo della protezione di un messaggio risieda principalmente nella mancanza di conoscenza del sistema di protezione impiegato. In società travagliate da conflitti originati da colossali interessi economici, sfrenate ambizioni personali, implacabili odi e smanie di potere, le scritture segrete sono state un imprescindibile strumento sia per ordire intrighi, sia per difesa. Non a caso i geroglifici egizi furono a lungo considerati come messaggi dal recondito e insondabile significato. Interpretazione consolidatasi dopo che la loro chiave di lettura fu trovata dal matematico francese Jean-François Champollion, il quale formulò, quasi divinò, l'ipotesi rivelatasi corretta che molti di quei segni avessero un significato fonetico di lettere il cui suono è richiamato dal corrispondente simbolo. Va detto che il lavoro del Champollion fu orientato dalle

geniali intuizioni, anche se non conclusive, dell'inglese Thomas Young sull'interpretazione della stele di Rosetta. Ora gli ideogrammi appaiono come una scrittura cifrata del linguaggio parlato per mezzo di segni comprensibili solo a ristrette cerchie, forse per questioni religiose, ovvero per motivi di predominio culturale o di casta. Questa ipotesi è coerente coi geroglifici trovati in una tomba nella città egizia di Menet Khufu in cui, intorno al 1900 a.C., uno scriba tracciò, con segni differenti da quelli usuali, la vita del suo padrone Khnumhotep. L'interpretazione corrente di questi simboli è che fossero una scrittura cifrata, ma lo scopo dello scriba fu, forse, solo quello di limitare la lettura dell'iscrizione a una ristretta cerchia di persone. Certamente, la sostituzione di segni pittorici fu pratica corrente per comunicare segretamente lungo le sponde del Nilo dove, alla corte dei faraoni, tra piramidi e sfingi, si giocò per migliaia di anni il gioco del potere. Tuttavia, l'impiego della crittografia in Egitto è solo un'ipotesi, seppur molto plausibile, non confermata esplicitamente in nessuno dei documenti che si è riusciti a interpretare. Fu nella Grecia tormentata dai conflitti tra le città-stato che apparve un uso sistematico delle scritture segrete di cui si hanno notizie storicamente accertate. Il metodo crittografico utilizzato dagli spartani intorno al 500 a.C. era la scitola (dal greco: *skytàla*, ovvero bastone) per crittare e decrittare messaggi scritti su una striscia di pergamena, avvolta in modo elicoidale intorno alla scitola, e su cui il messaggio era scritto per lungo; quando la striscia era svolta, la scrittura appariva come una sequenza casuale di lettere. Il sistema degli spartani è il capostipite dei metodi crittografici, ossia di tecniche consistenti nella trasformazione dei messaggi in modo tale da renderli comprensibili solo a chi ne conosca la trasformazione inversa.

Un secondo insieme di metodi, detti steganografici, è costituito dal celare l'esistenza stessa del messaggio in base all'ovvia osservazione che non si può cercare ciò di cui non si conosce l'esistenza. È della steganografia che si hanno notizie accreditate più antiche. Erodoto (484-425 a.C.) nelle sue *Historíai* ne riporta esempi singolari, uno dei quali è legato al notissimo evento delle Termopili. Racconta, infatti, che Demarato, un greco in esilio presso la Corte persiana, avendo appreso di un imminente attacco alla Grecia e volendo avvisare gli spartani, utilizzò una tavoletta ricoperta di cera che serviva per la scrittura. Rimossa la cera, Demarato incise il messaggio sul legno della tavoletta e quindi tornò a ricoprirla con la cera celando così il testo. L'innocua tavoletta, con l'avviso dell'invasione, raggiunse indenne gli spartani, consentendo loro di bloccare i persiani alle famose Termopili. In seguito, a Serse I fu inflitta una grande sconfitta nella battaglia navale di Salamina alla fine del 480 a.C. e, l'anno seguente, l'esercito persiano fu definitivamente sconfitto a Platea.

Le scritture segrete non fiorirono solo nel bacino mediterraneo, anche se le notizie al riguardo sono incerte e di carattere inferenziale. In India, nel trattato sull'arte di governo *Arthashastra*, l'autore Kautilya (370-283 a.C.) dedica un lungo capitolo all'impiego delle spie. La cifratura dei messaggi non è espressamente menzionata, ma forme di scrittura segrete dovevano esistere giacché erano l'unico mezzo di cui le spie potessero disporre per comunicare e ricevere informazioni.

Nello stesso periodo, quando l'egemonia dell'Impero romano si estese su tutto il Mediterraneo, le esigenze belliche richiesero lo scambio rapido di messaggi, possibilmente in modo protetto. Polibio (200-118 a.C.) descrive nelle sue *Historíai* un codice, inteso nell'accezione moderna, per consentire una semplice e rapida comunicazione attraverso una catena di postazioni, su torri e alture, che impiegavano fuochi o torce. Il codice consisteva nel rappresentare ciascuna lettera dell'alfabeto greco tramite una coppia di numeri da uno a cinque (Hist. X.45.6). La regola di codifica permetteva di comunicare una lettera dopo l'altra segnalando piccoli numeri, ad esempio, mostrando il corrispondente numero di torce accese. La codifica di Polibio è descritta dalla seguente tabella

	I	II	III	IV	V
I	α	β	γ	δ	ε
II	ζ	η	θ	ι	κ
III	λ	μ	ν	ξ	ο
IV	π	ρ	σ	ς	τ
V	υ	φ	χ	ψ	ω

Per esempio, il nome latino Caio, scritto in caratteri greci come **ΚΑΙΟ**, sarebbe stato codificato come II V – I I – II IV – III V. Chiaramente, il metodo si presta in modo naturale alla cifratura per sostituzione, ordinando in modo diverso le lettere nel quadrato. Polibio non parla di cifratura, tuttavia pone l'accento sull'esigenza che i messaggi, visibili a tutti, fossero incomprensibili al nemico. Invece, l'esigenza di messaggi cifrati fu chiaramente menzionata da Caio Giulio Cesare. Nel Libro V, sezione 48, del *De bello Gallico*, scrive che, venuto a sapere delle difficoltà in cui si trovava Cicerone – in quel tempo suo generale – che era stato accerchiato dai Galli, gli inviò un messaggio per raccomandargli di resistere:

uti ad Ciceronem epistolam deferat. Hanc Graecis conscriptam litteris mittit, ne intercepta epistola nostra ab hostibus consilia cognoscantur. Si adire non possit

dato che stava accorrendo in suo soccorso con due legioni. Il messaggio fu scritto in greco, quasi certamente sconosciuto ai Galli, al fine di celarne il contenuto nel caso fosse stato intercettato. Ovviamente, un messaggio in una lingua forse sconosciuta non assicura elevata protezione, ancorché il sistema sia stato usato con successo dagli americani, nella Seconda guerra mondiale, ricorrendo a un dialetto degli indiani Navajos.

Cesare, dunque, era consapevole dell'esigenza di proteggere l'informazione e conosceva diversi metodi per farlo. Importante è il suo famoso cifrario, utilizzato anche da Cicerone nelle *Lettere familiari* per parlare di fatti delicati, e descritto dallo storico Gaio Svetonio Tranquillo (69-122 d.C.) nel *De Vita Caesarum*, quale schema usato dalla casa Giulia. Spiega Svetonio che, per cifrare un testo, ogni lettera è cambiata con un'altra, spostata di tre posizioni in avanti, ossia la lettera A è sostituita con D, B con E, e così via fino a inserire W al posto di Z. In luogo delle ultime tre lettere compaiono le prime tre, ossia X invece che A, Y invece che B e Z invece che C. Ad esempio, il testo chiaro V E N I verrebbe cifrato come Y H Q N. La regola era molto semplice e il numero tre costituiva l'informazione segreta da conoscere per crittare e decrittare; infatti, per ottenere il messaggio in chiaro, ogni lettera va surrogata con quella che la precede di tre posizioni. Tale regola, detta monoalfabetica, ovviamente non sarebbe molto sicura, anche se la lettera sostitutiva differisse di un numero di posizioni diverso da tre. Certamente furono impiegati schemi più affidabili in cui, ad esempio, l'ordinamento delle lettere dell'alfabeto non era quello naturale, ma costituiva parte dell'informazione segreta; questi metodi però non risultano mai menzionati dagli storici della Roma imperiale.

Con la caduta dell'Impero romano la crittografia sembrò scomparire in Europa. Tuttavia, come una civiltà tramonta un'altra sorge. Nel Medio Oriente la civiltà araba raggiunse l'apice intorno al 900 d.C., dopo aver conosciuto un lungo periodo di pace e prosperità sotto la dinastia degli Abbasidi. Filosofia, scienza, letteratura, studi religiosi e matematica conobbero una fioritura senza precedenti. Fu in questo periodo che visse Abu Yusuf Ya'qub ibn Ishaq as-Sabbah Al-Kindi (801-873), filosofo e scienziato, tra le cui molte opere si annovera anche il *Manoscritto* sulla decifrazione dei messaggi crittografici. Nel trattato compare in maniera precisa l'attacco, detto di crittoanalisi, a messaggi cifrati con sostituzione monoalfabetica, basato sull'analisi della frequenza delle lettere nelle parole di una lingua. Interessante è la descrizione di Al-Kindi (ripresa da *Codici & Segreti* di Simon Singh):

Un modo di svelare un messaggio crittato, se conosciamo la lingua dell'originale, consiste nel trovare un diverso testo chiaro nella stessa lingua, abbastanza lungo da poter calcolare la frequenza di ciascuna lettera. Chiamiamo <prima> quella che compare più spesso, <seconda> quella che la segue per frequenza, <terza> la successiva, e così

via, fino a esaurire tutte le lettere del campione di testo chiaro. Esaminiamo poi il testo in cifra che vogliamo interpretare, ordinando [in base alla frequenza] anche i suoi simboli. Troviamo il simbolo più comune e rimpiazziamolo con la <prima> lettera dell'esempio chiaro; il simbolo che lo segue per frequenza sia rimpiazzato dalla <seconda> lettera, il successivo simbolo più comune sia rimpiazzato dalla <terza>, e così via, fino ad aver preso in considerazione tutti i simboli del crittogramma che intendevamo rivelare.

Il manoscritto dimostra la maturità raggiunta dalle tecniche crittografiche presso gli arabi, l'alta considerazione in cui erano tenute le scritture segrete e la raffinatezza dei metodi d'attacco a messaggi cifrati. Anche durante il Basso Medioevo la crittografia non ebbe grande fortuna in Europa, ancorché i metodi relativi che apparvero agli albori del Rinascimento fossero maturati in un lungo periodo, con continue miglorie rispetto agli schemi già in uso, prima tra i Romani e poi presso gli Arabi.

All'inizio del secondo millennio, quando la matematica araba fu introdotta in Europa principalmente per opera di Leonardo Pisano, noto come Fibonacci (1170-1240), e si diffuse assieme alla matematica greca, crebbero anche le esigenze di scritture segrete sospinte dall'incremento delle economie e dai conflitti tra Stati nazionali e, in Italia, per le spietate lotte tra i principati. Tuttavia, principi e monarchi, indotti dalla necessità, compresero che l'impiego di uomini di scienza, in particolare matematici e fisici, era indispensabile per lo sviluppo di nuovi e più sicuri sistemi di cifratura e per decifrare i messaggi degli avversari. Purtroppo, la storia della crittografia, come già ricordato, è sempre stata negletta e non molto è stato tramandato delle scritture segrete e della loro evoluzione. Di questo periodo sono ricordati alcuni successi della crittoanalisi quasi come cronaca, senza mai ben specificare gli schemi crittografici decifrati. In un'epoca di lenti e oscuri progressi, un manuale di cifratura, forse il primo in Europa, apparve nel 1379, dovuto a Gabriele de Lavinde da Parma, che servì nella segreteria di Clemente VII antipapa. Nello scenario italico, intriso di feroci lotte tra principi e d'intriganti misteri, merita di essere ricordato Francesco (Cicco) Simonetta (1410-1480). La sua ascesa presso la corte degli Sforza, in Milano, fu determinata dall'abilità nella crittoanalisi e dalle sue doti matematiche ma, come spesso accade nelle vicende umane, il suo potere cessò in modo tragico. Lasciò un trattato in latino sulla crittoanalisi, pubblicato senza molto successo nel 1474, col titolo *Regule ad extrahendum litteras ziferatas sine exemplo*.

Nello splendore artistico e nell'effervescenza culturale degli albori del Rinascimento italiano, il passo più rilevante fatto dalla crittografia, dopo secoli, fu compiuto da Leon Battista Alberti (1404-1472). Nel *De componendis cyfris*, apparso nel 1466 e scritto per la crittografia vaticana, l'autore descrive un sistema di cifratura, definito, assai giustamente, molto difficile da decifrare. Il metodo è uno dei primi esempi di crittografia polialfabetica, ossia uno schema di cifratura che usava sostituzioni diverse per lettere contigue. Inoltre, introduce un disco cifrante quale ausilio alle relative operazioni divenute note come disco di Alberti, assunto a modello dell'elemento base di tutte le macchine cifranti moderne. Nel testo vengono esposti anche principi di crittoanalisi, fondati sull'analisi delle frequenze con cui le lettere si ripetono nella lingua comune, di certo derivati o appresi dai metodi arabi.

Quasi contemporaneo dell'Alberti, Johann Heidenberg, noto come Tritemius (1462-1516), teorizzò i metodi steganografici. Il suo libro più noto ha per titolo *Steganographia: Ars per occultam scripturam animi sui voluntatem absentibus* (1500). Questo trattato, ancor oggi, può essere considerato come l'opera di riferimento per tale tecnica di cifratura. Il principio base è quello degli acrostici, un'espressione linguistica in cui le iniziali di parole, scelte in modo appropriato, formano una frase. Merita ricordare che uno dei più chiari esempi di acrostico è il poema *Amorosa visione*, dedicato a una misteriosa Fiammetta (forse Maria d'Aquino) da Giovanni Boccaccio (1313-1375), in cui sono raggiunti limiti difficilmente superabili con 1502 lettere iniziali di altrettante terzine composte dai versi di tre sonetti scritti quale introduzione al poema. Quest'acrostico, ancorché facile da verificare, pare sia stato casualmente scoperto e secoli dopo ha costituito un autentico esempio di steganografia in cui un messaggio è celato usando le iniziali di parole secondo una regola nota solo allo scrivente e al destinatario.

La *Steganographia* di Tritemius comprende una settantina di codici; ognuno è presentato con un esempio, dove un lungo documento (un'orazione, una lettera, una riflessione) di senso compiuto contiene un cifrato il cui testo chiaro si deduce (per esempio) leggendo la prima lettera delle parole dispari del messaggio. Ogni chiave è costituita in parte da riferimenti mnemonici – del tipo 'leggi la prima lettera delle parole dispari' – e in parte da riferimenti cifrati con una semplice chiave mnemonica, ad esempio cifratura di Cesare. Peraltro, anche nella crittografia il contributo di Tritemius non fu banale, avendo egli proposto un miglioramento allo schema di Alberti.

In questo periodo di grande vivacità culturale e politica, il papato ricoprì un ruolo di primo piano per lo sviluppo e l'uso della crittografia. Tra i crittografi laici della Curia romana, Giovan Battista Bellaso (1505-15??) occupò una posizione di assoluto rilievo, anche se non molto riconosciuta, come rimarca Augusto Buonafalce in numerosi articoli apparsi su «Cryptologia». È opinione di David Kahn, storico della crittografia e autore di *The Codebreakers*, che il Bellaso vada considerato l'inventore della chiave segreta di cifratura. I suoi contributi tecnici consistono in intelligenti sviluppi dei concetti introdotti dall'Alberti, rendendo i metodi di cifratura efficaci ed efficienti senza dover usare il suo disco. In un primo opuscolo, *La cifra del Sig. Giovan Battista Belaso, gentil'huomo bresciano*,

nuovamente da lui medesimo ridotta à grandissima breuità & perfettione, pubblicato nel 1553 con un errore di stampa nel cognome dell'autore, il Bellaso descrive delle regole di cifratura per mezzo di una tabella – detta tabella reciproca – sostitutiva del disco di Alberti. La tabella reciproca, facilmente costruibile da una chiave mnemonica segreta, evita lo scambio e l'uso del disco. Ad esempio, per costruirla con chiave segreta CRYPTO, si ripartiscono le 26 lettere in due gruppi, ciascuno di 13 lettere che si scrivono su due righe:

abc def ghi j kl m
nop qrs tuv wxy z

indi si scrive CRYPTO all'inizio nella prima riga e si eliminano tutte le lettere già utilizzate, infine quelle che nella prima riga sono oltre la tredicesima posizione vengono ordinatamente spostate all'inizio della seconda riga:

CRY PTO abd efg h
ijk lmn qsu vwx z

Per cifrare si sostituisce la lettera di testo con la lettera della tabella che le compare o sopra o sotto. Per decifrare, conoscendo la tabella, si opera nello stesso modo, da qui il nome di tabella reciproca. Se si usa una sola coppia di righe, la sostituzione è monoalfabetica. Tuttavia, il Bellaso impiegava più coppie (usualmente dieci) di righe, ciascuna generata dalla precedente, operando uno scorrimento ciclico, e cifrava le lettere del messaggio in sequenza con una periodicità pari al numero di coppie. La seconda coppia sarebbe:

z CRY PTO abd efg
h ijk lmn qsu vwx

Con una tabella corrispondente a queste due sole coppie, il nome 'bellaso' sarebbe cifrato in 'svppqbn'. Nei suoi lavori, l'autore descrive molte e più efficaci varianti d'uso della tabella reciproca, ma il principio è lo stesso. La tabella del Bellaso e altre in forme più generali apparvero anche nel *De Furtivis Literarum Notis* di Giovanni Battista Della Porta, pubblicato nel 1563. Il Bellaso migliorò le sue regole in due libricini successivi, pubblicati nel 1555 e nel 1564, arrivando a definire degli schemi ancor oggi difficili da attaccare con la crittoanalisi. Nel secondo, pubblicato in Brescia per i tipi di Giacomo Britannico il Giovane, *Il vero modo di scrivere in Cifra con facilità, prestezza, et sicurezza di Misser Giovan Battista Bellaso, gentil'huomo bresciano*, dedicato al cardinale Alessandro Farnese, appare anche, con tono vagamente polemico, l'osservazione che la tabella da lui introdotta era stata ripresentata, quindici anni dopo, dal Della Porta senza fare menzione dell'inventore. Nel testo, un sommario migliorativo dei lavori precedenti, il Bellaso pro-

pose come sfida ai crittografi contemporanei sette brevi messaggi cifrati con i suoi noti algoritmi e con l'indicazione che il contenuto di uno di questi è la sua spiegazione del perché tutti i gravi cadono con la stessa velocità. Nel 2009, l'inglese Tony Gaffney ha decifrato sei dei sette messaggi e, a oggi, solo il messaggio numero cinque

EUFEMEASGGMCN FLBNNMGTMNNBFD BLCAXTM HCFXFFCBQDCA
MECTFOCAFHGMFNMATDCMIDIOIDFEABABUHEDAPHXOBDXPCIBMDBEL
ASCAEISAF AOUMAIUUCFIPLDAHIUSTCAP

resta ancora indecifrato. Probabilmente, la difficoltà di decifrarlo sta nella sua brevità, soprattutto se la chiave di cifratura è composta di un numero di caratteri non molto minore della sua lunghezza, per cui la cifratura è in sostanza perfetta secondo i criteri di Claude Elwood Shannon (1916-2001). Alcuni degli importanti contributi del Bellaso furono ricordati, col loro autore, nel *Traicté des chiffres ou secrètes manières d'écrire*, pubblicato nel 1585 da Blaise de Vigenère (1523-1596). Nel trattato compare la tabella 'reciproca' per cifrare, che ora porta il nome di Vigenère, con alcune variazioni e dettagliate spiegazioni che fecero erroneamente riguardare per secoli tale schema come perfetto.

In quel periodo operarono dei crittografi professionisti che, seppur abili matematici, non divennero famosi. Tra questi, occupa una posizione di rilievo Giovanni Soro, nato da famiglia sarda a Venezia, ove morì nel 1544, alla fine di una vita trascorsa al servizio della Serenissima Repubblica di Venezia. Dal 1506 ricoprì per primo, conservandola fino al 1542, la carica di Segretario alle Cifre, con lo studio all'interno del Palazzo Ducale presso la Sala dei Segreti. Compito di tale magistratura, al diretto servizio del Consiglio dei Dieci, era decifrare i messaggi in codice degli amici e degli avversari politici e commerciali in difesa degli insediamenti mercantili disseminati nel bacino mediterraneo. Un libro dedicato alla decrittazione dei cifrari, in italiano, francese, spagnolo e latino, accrebbe la sua già grande notorietà continentale, scaturita dalla decrittazione di molti dei cifrari in uso nelle corti europee. Purtroppo, questo trattato di crittoanalisi, scritto agli albori del 1500, secondo Kahn è uno dei tanti libri perduti di crittoanalisi. Sporadicamente il Soro servì anche la Curia romana di papa Clemente VII per testare l'affidabilità dei codici crittografici vaticani. Nella seconda metà del Cinquecento, la crittoanalisi conobbe un periodo aureo diventando patrimonio anche di matematici illustri.

In Francia, François Viète Seigneur de la Bigotière (1540-1603) servì come crittografo personale i re Enrico III ed Enrico IV. Abilissimo nella crittoanalisi e come matematico fu il precursore della moderna algebra come scrittura simbolica. Il suo maggior contributo alla nascente matematica europea fu l'introduzione delle variabili, ossia l'uso delle lettere nella scrittura di formule.

In Italia, il più famoso matematico e crittografo fu il lombardo Girolamo Cardano, noto per il contributo offerto alla soluzione delle equazioni algebriche. In crittografia è ricordato, in particolare, per l'invenzione di un lucchetto a rotori che si apriva solo con una data combinazione di lettere, descritto nell'opera *De Subtilitate* libri XXI (1550).

Nel Regno Unito, il matematico John Wallis (1616-1703), considerato uno dei fondatori del calcolo infinitesimale, è anche ricordato per successi di crittoanalisi in favore della fazione dei 'Parlamentaristi' (in opposizione a quella dei 'Realisti') al tempo di Oliver Cromwell e, in seguito, al servizio della monarchia. Come il Bellaso, Wallis sostenne, seppur con minor forza, che la sicurezza dovesse basarsi sulla segretezza della chiave e non sugli algoritmi di cifratura.

Nel cosmopolita ambiente culturale del Rinascimento, la crittografia non fu praticata solo da artisti, letterati e scienziati, ma anche da eminenti uomini di Stato. Fu appunto un illustre politico inglese, Francis Bacon, (1561-1626), che con l'Alberti dette il secondo importante contributo nella caratterizzazione della crittografia come scienza. Bacon, da uomo di Stato e scienziato preparato, formulò così i principi base della buona crittografia:

1. che sia semplice cifrare;
2. che sia semplice decifrare se si conosce il meccanismo;
3. che sia difficile decifrare i messaggi, pur sapendo che sono cifrati, senza informazioni private; infine
4. che il cifrato sia insospettabile (sia cioè steganografico).

Inoltre, propose una geniale forma di crittografia, anche se di difficile realizzazione, che combinava trasformazioni crittografiche con l'idea base della steganografia allo scopo di ottenere un messaggio cifrato insospettabile.

I primi tre principi di Bacon si possono considerare assiomi della crittografia, quando completati col principio di Kerckhoff (ossia che «la sicurezza debba risiedere tutta nella segretezza della chiave», come peraltro già sostenuto da Bellaso e da Wallis).

L'evoluzione delle scritture segrete raggiunse nel Cinquecento livelli tecnici tali da consentirne l'uso anche ai non specialisti, creando le condizioni e preparando l'ambiente scientifico e culturale delle scoperte che avverranno nel ventesimo secolo e che useranno le tecniche matematiche sviluppate negli intercorsi quattro secoli

