LEZIONE INTRODUTTIVA

La crittografia

La crittografia nasce fin dall'antichità dall'esigenza di possedere metodi efficienti per comunicare in modo segreto e sicuro, avendo la possibilità di inviare messaggi che possano essere letti rapidamente dai destinatari e non decifrati dal nemico, o da chiunque non sia autorizzato.
Il problema è estremamente attuale, con lo sviluppo dei sistemi elettronici che facilitano le comunicazioni, ma che le rendono anche molto vulnerabili se non vengono adeguatamente protette.
Per migliaia di anni re, regine e generali hanno avuto bisogno di comunicazioni efficienti e segrete per governare i loro paesi e comandare i loro eserciti: se informazioni preziose fossero cadute in mani ostili potevano esserci conseguenze molto pericolose.
Per trovare il primo esempio di occultazione di messaggi possiamo risalire fino al V secolo a.C. alle guerre persiane.
Nelle *Storie* di Erodoto si legge che Serse, succeduto al padre Dario, dopo aver domato una ribellione in Egitto, si apprestava a muovere contro la Grecia.
Demarato, che aveva saputo dell'imminente spedizione, voleva avvertire gli Spartani senza correre il pericolo di essere scoperto dai nemici; ideò quindi uno stratagemma: prese una tavoletta per scrivere doppia, ne raschiò la cera e poi sul legno della tavoletta scrisse il piano di Serse. Fatto ciò, versò di nuovo la cera liquefatta sullo scritto in modo che, venendo portata vuota, la tavoletta non attirasse i sospetti da parte dei custodi delle strade. Ma quando la tavoletta giunse a Sparta, gli spartani non capirono cosa significasse fin quando la moglie di Leonida lo comprese e lo suggerì loro, invitandoli a raschiare la cera. Dandole ascolto trovarono il messaggio e lo spedirono agli altri greci che si prepararono così all'arrivo di Serse. Fu così che sconfissero i persiani nel 480 a.C.
Un messaggio segreto, abilmente nascosto, cambiò quindi le sorti di una guerra.

Un altro episodio, sempre dalle *Storie,* racconta che Istieo voleva dare ad Aristagora l'ordine di ribellarsi, ma essendo le strade sorvegliate non aveva modo di comunicarglielo.
Allora fece rasare la testa al suo schiavo più fidato, vi impresse dei segni e aspettò che gli ricrescessero i capelli. Non appena ricrebbero, lo spedì a Mileto con l'ordine, una volta giunto da Aristagora, di farsi radere i capelli. In questo caso però il trucco non ebbe successo, perché i nemici sospettarono che lo schiavo portasse qualche messaggio nascosto e quindi lo perquisirono in tutto il corpo, fino a rasargli la testa. Il messaggio, quindi, non fu mai consegnato al destinatario.

L'insieme dei trucchi come quelli usati in questi due esempi prendono il nome di *steganografia,* ossia procedura che consiste nel nascondere i messaggi, ed è la più antica e la più naturale forma di occultamento.
Ma questi due episodi appena raccontati sono sufficienti a mostrare la scarsissima sicurezza di questi sistemi: a chiunque sospetti che qualcuno possa aver nascosto un messaggio basterà ispezionare con la massima cura tutti i possibili nascondigli per scovarlo.

Perciò in parallelo con lo sviluppo della steganografia si assisté all'evoluzione della *crittografia*, dal greco *kryptòs,* che significa nascosto. La crittografia non mira a nascondere il messaggio in sé, ma il suo significato. Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato a suo tempo dal mittente e dal destinatario. Quest'ultimo può invertire il procedimento e ricavare il testo originale.
Anche se crittografia e steganografia sono due discipline separate e indipendenti, possono in qualche modo essere considerate come l'una l'evoluzione dell'altra in termini di sicurezza.
La crittografia ha infatti il vantaggio di rendere il messaggio irriconoscibile e inutilizzabile dal nemico anche quando questi riesce ad intercettarlo.

Egli, infatti, può sospettare l'algoritmo utilizzato per cifrare, ma non la chiave.

Uno dei primi esempi famosi di crittografia si trova nel *De Bello Gallico* di Cesare. L'autore racconta del riuscito invio di un messaggio a Cicerone, assediato e sul punto di arrendersi. Cesare usò una cifratura detta per *trasposizione,* che consisteva in un alfabeto *in chiaro* (quello ordinario) e un alfabeto *cifrante* ottenuto sostituendo ogni lettera dell'alfabeto ordinario con una lettera che lo rimpiazza nel crittogramma. Ad esempio

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

ci permette di scrivere le parole GIULIO CESARE come LNAONR FHVDUH.

In questo caso appare evidente che l'alfabeto cifrante non è altro che quello in chiaro traslato a destra di tre posizioni.
Questa particolare cifratura per trasposizione prende il nome di *cifratura di Cesare,* che studieremo in dettaglio e da cui partirà proprio il nostro laboratorio.

E' chiaro, però, che questo primo sistema appare facilmente attaccabile: le lettere dell'alfabeto italiano sono 21 e quindi possiamo traslare le lettere al massimo di 20 posizioni: traslando di 21, infatti, torneremmo all'alfabeto chiaro. Quindi, anche se il nostro ipotetico nemico non conosce la chiave (ovvero non sa di quanti posti sono state traslate le lettere), sospettando che la cifratura sia di Cesare, avrebbe bisogno al massimo di 20 tentativi per risalire al messaggio originale!

E' per questo che i *crittologi* hanno avvertito da subito la necessità di studiare sistemi più sofisticati e sicuri. Anche perché, accanto alla nascita della *crittologia* (la scienza praticata dai crittologi che ha lo scopo di ideare nuove tecniche) si registra quella della *crittoanalisi,* cioè la scienza dell'interpretazione di un messaggio di cui si ignora la chiave. Mentre i crittologi, da un lato, mettono a punto nuovi sistemi di scrittura segreta, dall'altro i *crittoanalisti* cercano di individuare i loro punti deboli e carpirne i segreti.

Nessun esempio mostra le potenziali conseguenze della crittoanalisi in modo più drammatico del processo a Maria Stuarda di Scozia, il cui esito dipese completamente dallo scontro tra i suoi cifratori e i decrittatori di sua cugina, Elisabetta I.
La regina di Scozia, imprigionata da Elisabetta nel 1568, rimase prigioniera per 18 anni. Nel 1586 fu organizzato un piano per liberarla e contemporaneamente uccidere la regina Elisabetta. I cospiratori ritenevano, però, che il loro piano avrebbe dovuto avere l'approvazione di Maria. Per fare ciò si servirono di messaggi nascosti (steganografia) e anche cifrati (crittografia) che venivano recapitati da un messaggero in prigione. Uno dei cospiratori fece però il doppio gioco e fu fatale alla regina di Scozia e ai suoi sudditi anche l'errata convinzione della inattaccabilità del loro sistema crittografico. I crittoanalisti di Elisabetta permisero alla sovrana di smascherare il piano, evitare che la congiura fosse portata a termine e impossessarsi di prove schiaccianti sul coinvolgimento della cugina nella cospirazione. Maria Stuarda fu così condannata a morte.

Ma, per inciso, l'importanza della crittoanalisi va oltre la semplice sfida contro i crittologi. Pensiamo, ad esempio, alle iscrizioni antiche: ovviamente l'intendimento di chi scriveva non era, in genere, di criptarle, ma per noi rappresentano di fatto un messaggio cifrato, che dobbiamo decifrare. La decifrazione di una scrittura sconosciuta rappresenta qualcosa di magico, perché ci permette di conoscere una civiltà ormai morta, di farci un quadro storico dell'epoca a cui l'iscrizione risale, ecc. Si pensi alla decifrazione dei geroglifici egiziani: c'è un famoso reperto archeologico, la *stele di Rosetta,* di basalto nero, rinvenuta nel 1799 nei pressi delle foci del Nilo e incisa nel 196 a.C. Si

tratta di un'iscrizione riguardante il decreto di un'assemblea di sacerdoti in onore del faraone ed è noto che essa reca lo stesso testo in tre versioni: egiziana geroglifica, egiziana demotica e greca. L'iscrizione in greco fu abilmente tradotta e diventò il "testo in chiaro" con cui confrontare le altre due scritture: essa costitutiva, quindi, un opportunità e una sfida irresistibile. J.F. Champollion raccolse la sfida e svelò nel 1822 il mistero dei geroglifici. La stele è oggi conservata nel British Museum a Londra.
Chiudiamo l'inciso con una curiosità: abbiamo detto poco fa che l'intendimento di chi incideva le iscrizioni non era, in genere, di criptarle. Abbiamo prudentemente scritto *in genere:* infatti alcuni scienziati hanno recentemente scoperto la presenza di procedimenti crittografici nei geroglifici egiziani. Sembra infatti che alcuni di essi siano stati crittati per ordine dei faraoni con varie tecniche, tra cui la cifratura per sostituzione.

La fine della cifratura per sostituzione monoalfabetica avvenne ad opera dei crittoanalisti arabi: furono loro i primi, non solo ad inventare in pratica la crittoanalisi, ma anche a escogitare una tecnica che permetteva di decifrare in breve tempo qualsiasi crittogramma: l'*analisi delle frequenze.*
In ogni lingua ci sono lettere che compaiono nei testi con maggiore frequenza ed altre più raramente, ad esempio nella lingua italiana le lettere più frequenti sono nell'ordine e,a,i mentre le meno usate sono q,z. Non solo: l'analisi del testo ci fornisce altre informazioni. Ad esempio nella lingua italiana la maggior parte delle parole termina con una delle vocali a,e,i,o e ciò vorrà dire che le lettere finali delle parole del messaggio cifrato dovranno essere una di queste lettere. Si può inoltre ricorrere ad altre considerazioni, come il fatto che lettere consecutive identiche necessariamente devono essere consonanti.
E questo strumento ha permesso (anche se con un po' più di tempo e fatica) ai crittoanalisti negli anni a seguire di distruggere la sicurezza di sistemi che via via i crittologi avevano complicato, come quelli che utilizzano parole come chiave oppure quelli polialfabetici, basati sul principio di cambiare alfabeto cifrante per ogni lettera del testo chiaro, come il cifrario di Vigenére che per anni è stato definito "il cifrario indecifrabile".

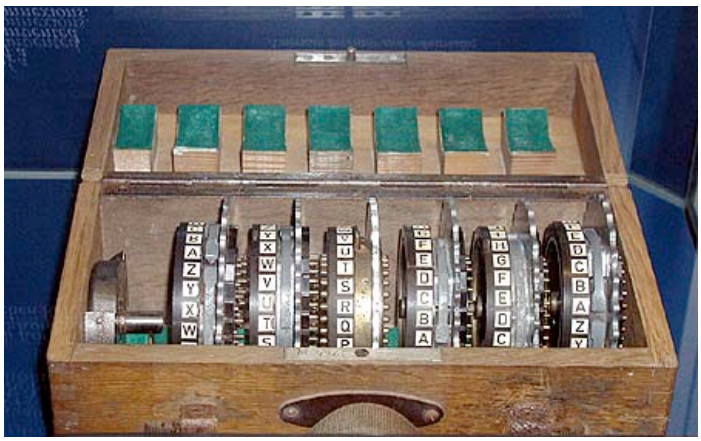
Le macchine per cifrare

Col passare degli anni e col progresso della tecnologia, la cifratura divenne sempre più automatizzata.
Tuttavia il primo vero "macchinario" per cifrare (che era solo un supporto per la cifratura manuale) è il cosiddetto *disco cifrante* di Leon Battista Alberti. Esso consiste in due dischi di rame concentrici, di diametri differenti, che sono imperniati nel centro su di un perno e possono così ruotare l'uno rispetto all'altro attorno ad esso. Lungo le circonferenze dei due dischi sono incisi due alfabeti. Per crittare un messaggio con la cifratura di Cesare traslando di due lettere, basta collocare la *a* del disco interno (che rappresenta l'alfabeto in chiaro) in corrispondenza della *C* del disco esterno (che rappresenta ovviamente l'alfabeto cifrante). Una volta fatta questa operazione, per cifrare il messaggio basta di volta in volta, senza più ruotare i dischi, vedere quali sono le lettere sul disco esterno che corrispondono alle varie lettere del disco interno. Si tratta di un congegno molto semplice e molto efficace che è stato utilizzato per secoli. Questo stesso congegno può essere usato anche per una cifratura polialfabetica: basta, infatti, ruotare il disco di quante posizioni vogliamo per ogni lettera del messaggio.

Come detto, questa macchina ha resistito parecchi secoli, fino a quando, al termine della prima guerra mondiale, non è stata soppiantata da un nuovo macchinario tedesco, basato sempre su sistemi polialfabetici, ma in modo assai più ingegnoso.
Questa nuova macchina, chiamata *Enigma,* fu ideata e realizzata da Arthur Scheribius e Richard Ritter. Essa, almeno inizialmente, consisteva di tre elementi collegati da fili elettrici:

- una tastiera sulla quale erano disposte le lettere dell'alfabeto ordinario per poter battere il testo chiaro;
- 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 ad illuminare la lampadina corrispondente alla lettera crittata.

Lo scambiatore è un meccanismo costituito da uno spesso disco di gomma attraversato da una complessa rete di fili elettrici. Se ad esempio vogliamo criptare la lettera *a* con la lettere *D* (cioè lo scambiatore trasla di tre lettere), si digita *a* sulla tastiera: ciò facendo la corrente elettrica entra nello scambiatore seguendo il percorso dei fili, illuminando così la lampadina corrispondente alla lettera *D*. Gli scambiatori potevano essere sostituiti in base alla chiave che si voleva usare. Successivamente la macchina fu perfezionata e lo scambiatore divenne ruotante: questo faceva sì che il disco dopo la cifratura di ogni lettera ruotasse di un ventunesimo di giro in modo da usare un nuovo alfabeto per crittare ogni lettera. Lo scambiatore individuava, infatti, 21 alfabeti cifranti diversi.



In seguito Enigma divenne ancora più sofisticata, con l'introduzione di più dischi scambiatori e di *riflettori* in grado di riflettere i segnali elettrici e rendere ancora più complicata la cifratura.
Insomma, si trattava di una macchina molto efficace per cifrare, tanto che Scheribius era convinto che Enigma generasse dei messaggi inviolabili. Tuttavia la macchina, pur avendo le dimensioni di una ventiquattr'ore, pesava ben 12 kg e inoltre non esisteva possibilità di stampa, dunque l'operatore doveva copiare a mano, carattere per carattere il messaggio cifrato da trasmettere.
Per decodificare il crittogramma bastava possedere un'altra macchina Enigma e un cifrario con l'assetto degli scambiatori invertito. Tale assetto veniva cambiato giorno per giorno.
Anche durante la seconda guerra mondiale i tedeschi continuarono ad usare una versione portatile a batteria di Enigma. Infatti i crittoanalisti si trovarono di fronte alla difficoltà di avere troppi messaggi da decifrare e non abbastanza tempo.
Nel 1943, nel corso della seconda guerra mondiale, fu impiegato dagli Inglesi il sistema *Colossus* per decifrare i codici prodotti dal sistema Enigma.
Ma fu il famoso matematico Alan Turing all'inizio della guerra a violare la sicurezza di Enigma.

La rivoluzione della chiave pubblica: RSA

Nei cifrari fin qui descritti il processo di decifratura non presenta in generale grandi difficoltà una volta che sia noto il metodo usato per cifrare e cioè la chiave. Infatti in questi casi la funzione di decifratura è, per così dire, simmetrica a quella di cifratura, ossia è, sia da un punto di vista logico che computazionale, una funzione dello stesso tipo. In particolare tutti i crittosistemi classici si riferiscono allo scambio di messaggi tra due soli utenti e sono basati sulla condivisione di una chiave che consente, in sostanza, cifratura e decifratura.
Ma facciamo un passo avanti. In un'epoca come quella attuale in cui la maggior parte dell'informazione avviene via telefono o posta elettronica o radio, ogni messaggio inviato, come anche ogni trasmissione di chiave, è soggetta ad una facile intercettazione. E' pertanto indispensabile trovare nuovi modi più sicuri di comunicazione protetta.
Questo nuovo modo è costituito dalla crittografia a chiave pubblica.
Un cifrario a chiave pubblica è un sistema che permette di divulgare il metodo ed anche la chiave di cifratura (da cui il nome), senza per questo rivelare contestualmente il modo di decifrare. In altre parole, in tali sistemi, per calcolare in un tempo ragionevolmente breve la trasformazione di decifratura, inversa di quella di cifratura, è necessario essere in possesso di altre informazioni oltre quelle rese pubbliche e di cui abbiamo parlato. Tali informazioni però sono tenute segrete e senza di esse la complessità del calcolo della decifratura è tale da renderla implausibile.
Ed è in questo modo che funziona il sistema RSA (come vedremo alla fine del laboratorio), per mezzo di una funzione che possiamo definire "a senso unico".
Ciò che rende questo sistema "inattaccabile" è il fatto che i crittologi sono in vantaggio al momento sui crittoanalisti: questi ultimi, infatti, non sono ancora riusciti a trovare i mezzi per distruggere l'RSA. Ma ciò non vuol dire che sia davvero indecifrabile: nessuno può garantire, infatti, che in futuro non siano scoperti nuovi strumenti matematici in grado di superare anche questo nuovo sistema. E nessuno, inoltre, può essere certo che nuove scoperte non siano già state fatte. Enti come il National Security Agency (NSA) americano continuano a compiere studi ultrariservati sulla crittografia; ovviamente, le conoscenze che ne derivano non sono divulgate e i loro autori restano anonimi.

Numeri primi

Che cos'è un *numero primo*? La risposta appare semplice a primo impatto: sappiamo, infatti, già dalle scuole medie che un numero si dice *primo* quando non è divisibile per nessun altro numero se non per se stesso e per 1.
Apparentemente quindi questi numeri, pur avendo una caratteristica che li distingue dagli altri, non sembrano essere poi così importanti. Sono numeri con una particolare proprietà, così come ce ne sono tanti con proprietà diverse: ad esempio 4 ha la proprietà di essere pari oppure di essere il quadrato di 2; 6 ha la proprietà di essere un numero perfetto, cioè di essere la somma di tutti e soli i suoi divisori.
Ma guardiamo la proprietà dei numeri primi sotto un'altra luce: un numero primo, per com'è definito, non può essere scritto come prodotto di due numeri più piccoli (ovviamente diversi da se stesso e da 1), mentre qualsiasi altro numero possiede questa caratteristica: 35 non è primo e può essere scritto come 5x7, oppure 42 non è primo e si può scrivere come 6x7…ma iterando il ragionamento si osserva subito che in quest'ultima *fattorizzazione* lo stesso 6 non è primo, ma è dato dal prodotto di 2 e 3 e quindi possiamo riscrivere 42 come 2x3x7.
In entrambi i casi (e lo stesso vale per qualsiasi altro numero non primo) abbiamo scomposto il numero di partenza nel prodotto di numeri più piccoli *primi.*
Già da questa osservazione viene forse naturale il sospetto che questi numeri primi abbiano una caratteristica davvero speciale rispetto a quelli non primi: ci permettono di "generare" qualsiasi altro numero, semplicemente moltiplicandoli tra di loro. Per usare una metafora, è come se i primi

costituissero gli atomi della matematica, come se fossero una sorta di tavola periodica degli elementi (come quella usata in chimica che ci permette di creare le molecole presenti nel mondo fisico) a partire dai quali si "creano" i numeri.
E' chiaro che per un matematico la loro importanza non si esaurisce qui: esiste in matematica tutta una branca, che va sotto il nome di *teoria dei numeri*, in cui i primi assumono un ruolo centrale e che è continuamente oggetto di studio e di ricerca.
Non ci occuperemo di teoria dei numeri vera e propria in questo laboratorio, ma vedremo come la matematica e i numeri primi in particolare entrino nella vita pratica di tutti i giorni attraverso un potente strumento come il computer. Di come, cioè, i *crittologi* si servano di questa importante teoria per ideare e sviluppare dei sistemi in grado di *cifrare* messaggi in modo sicuro e di garantire la privacy di quanti vogliono comunicare privatamente a distanza, ma soprattutto la sicurezza di transazioni finanziarie attraverso le banche, i bancomat, le carte di credito ecc. Ogni volta che ordiniamo qualcosa su un sito web, il nostro computer usa la sicurezza fornita dall'esistenza di numeri primi di cento cifre, attraverso un sistema noto col nome di *RSA*.
Ad oggi sono più di un milione i numeri primi che sono già stati usati per proteggere il mondo del commercio elettronico.
Quindi la ricerca di numeri primi può apparentemente sembrare un'attività inutile. E fino a non molto tempo fa la reale importanza "pratica" di tale ricerca era nascosta perfino agli stessi matematici. G.H. Hardy, matematico di Cambridge, nel suo libro "Apologia di un matematico", riferendosi alla teoria dei numeri afferma:
<< Tanto un Gauss quanto dei matematici meno importanti possono a buona ragione rallegrarsi del fatto che qui c'è comunque una scienza la cui stessa lontananza dalle ordinarie attività umane dovrebbe mantenere amabile e pura>>.
Ma a partire dagli anni Settanta, come vedremo, i numeri primi conquistarono il centro della scena nel mondo del commercio.

Un concetto molto antico

I numeri primi erano noti fin dall'antichità, o almeno ci sono delle tracce e degli studi che ci permettono di ipotizzare che già molto prima della nascita di Cristo antiche civiltà come i greci e i cinesi fossero a conoscenza dell'esistenza di numeri "speciali", pur non comprendendone né apprezzandone a fondo la vera importanza.
La più antica, anche se incerta, prova è un osso risalente al 6500 a.C., l'osso di Ishango, scoperto nel 1950 fra i monti dell'Africa equatoriale centrale. Vi sono incise quattro serie di tacche disposte su tre file. In una delle file si contano 11, 13, 17 e 19 tacche, cioè un elenco completo dei numeri primi compresi tra 10 e 20. Non è chiaro se quest'antico osso, conservato all'istituto reale di Scienze Naturali di Bruxelles, rappresenti davvero uno dei primi tentativi da parte dei nostri antenati di comprendere i numeri primi oppure se le incisioni siano una scelta casuale di numeri e che solo per caso siano primi.
Ci sono anche prove del fatto che prima del 1000 a.C. i cinesi avevano elaborato un modo fisico per comprendere che cos'è che rende i primi, fra tutti i numeri, particolari: se prendete 15 fagioli, li potete disporre in un perfetto rettangolo composto da tre file di cinque righe; se però prendete 17 fagioli, l'unico rettangolo che potete costruire è quello formato da una sola riga di 17 fagioli.
Ma i primi a scoprire la reale potenza dei numeri primi furono i greci, nel IV secolo a.C.: essi compresero che ogni numero poteva essere creato moltiplicando fra loro dei numeri primi.
Per secoli quasi tutti i più grandi matematici si dedicarono allo studio dei primi, facendo molte scoperte importanti, ma ancora oggi il problema è aperto. Nessuno, infatti, è mai riuscito a stabilire il criterio con cui questi numeri si dispongono e a trovare un modo rapido per calcolarli. Non è infatti possibile sapere quale sarà, ad esempio, il millesimo numero primo senza calcolare i 999 precedenti. Oggi, in realtà, ciò è possibile poiché esistono delle tavole con i primi, che arrivano

anche a numeri molto elevati, ma sono state compilate con grossi sforzi e nel corso di centinaia di anni.
La prima tavola risale a Eratostene, bibliotecario ad Alessandria, che nel III secolo a.C. scoprì una procedura ragionevole per determinare quali fossero i numeri primi compresi, per esempio, tra 1 e 1.000, che va sotto il nome di *Crivello di Eratostene.* Egli scriveva per esteso i numeri da 1 a 1.000, poi prendeva il numero primo più piccolo, cioè 2, e a partire da quello depennava dall'elenco un numero ogni due, ovvero i multipli di 2. I numeri cancellati non erano primi perché erano divisibili per 2. Quindi passava al numero successivo che non era stato eliminato, ovvero3, e a partire da quello depennava tutti i multipli di 3 che, essendo divisibili per 3, non erano primi. E continuava così, prendendo il numero successivo che non era stato cancellato e depennando tutti i suoi multipli: ogni numero primo crea un "crivello" che permette di eliminare una parte dei numeri non primi. Arrivato a 1.000, i numeri rimasti sono tutti primi.
La cosa che saltò all'occhio di tutti i matematici fu che in queste tavole non c'era un ordine apparente, che i numeri primi sembravano essere disposti totalmente a caso. Non c'è una formula che li lega, non c'è un criterio per stabilire, dato un qualsiasi primo, quale sarà quello successivo senza andare più o meno per tentativi su tutti i numeri.
Questo problema ha accompagnato e accompagna tuttora i matematici di tutto il mondo: la *struttura* che si nasconde dietro la sequenza dei primi. Tutti noi almeno una volta ci siamo cimentati nella risoluzione di giochi in cui data una sequenza di numeri si deve trovare il successivo ricostruendo la regola che c'è dietro, come ad esempio:
1, 1, 2, 3, 5, 8, 13,…. in cui ciascun numero è somma dei due precedenti (nota come la sequenza di *Fibonacci*), ma una regola simile per i numeri primi non è stata ancora trovata. Esiste perfino un cospicuo premio in denaro per chi riesca a risolvere questa *congettura.*
Molti nomi illustri hanno finora fallito: Euclide, Fermat, Eulero, Gauss, Riemann e molti altri ancora. Il loro contributo è stato indubbiamente fondamentale: Euclide negli *Elementi* ha dimostrato che esistono infiniti numeri primi; Fermat pensava di aver trovato una formula che permettesse di trovare alcuni numeri primi (anche se non tutti) e di fornirne almeno un elenco in modo piuttosto semplice:
si trattava dei numeri della forma $2^{2^N}+1$, ma in seguito si scoprì che Fermat sbagliava perché per *N=5* non si ottiene un numero primo, solo che gli strumenti a sua disposizione erano insufficienti per scoprirlo.
Sulla sua scia si mise Mersenne, un monaco francese appassionato di matematica, che sistemando ciò che aveva fatto Fermat scoprì che i numeri della forma 2^N-1 per alcuni valori di *N* davano effettivamente un numero primo. Con gli scarsi mezzi che aveva a disposizione riuscì misteriosamente a scoprire che era primo il numero con *N=257*, un numero di ben 77 cifre! Ma ancora oggi non sappiamo se gli *N* per cui si ottiene un primo siano infiniti. Il più grande primo di Mersenne conosciuto finora è il 37esimo, un numero a ben 909.526 cifre!

Eulero, invece, realizzò una tavola dei primi fino a 100.000, ma una delle sue scoperte più curiose fu una formula che si serviva dei polinomi per generale una quantità inspiegabile di primi, ma non riuscì a perfezionarla.
Ad esempio, inserendo (come egli stesso fece) tutti i numeri compresi tra 0 e 39 nel polinomio x^2+x+41, ottenne il seguente elenco di primi:

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1.033, 1.097, 1.163, 1.231, 1.301, 1.373, 1.447, 1.523, 1.601.

E lo stesso lungo elenco poteva essere costruito usando *q*=2, 3, 5, 11, 17 nella formula al posto di 41 e inserendo tutti i numeri tra 0 e *q-2.*

Ma nonostante questa scoperta, lo stesso Eulero disse: <<Ci sono alcuni misteri che la mente umana non penetrerà mai. Per convincercene non dobbiamo far altro che gettare un'occhiata alle tavole di numeri primi. Ci accorgeremo che non vi regna né ordine né legge>>.

Fra tutti Gauss e Riemann fecero, forse, le più grandi scoperte.
Il primo riuscì a stimare il numero di primi presenti in un intervallo, attraverso una funzione che usava il logaritmo e che indicava con $\pi(N)$.
Da questo calcolo cominciava ad emergere una struttura: per esempio, il numero di primi compresi tra 1 e 100 è 25. Gauss, servendosi delle tavole di Euclide che aveva a disposizione, osservò come cambiava questa funzione tra 1 e 1.000 e tra 1 e 10.000 e così via e realizzò una tabella simile a quella riportata qui sotto, in cui inserì anche la distanza media tra due primi successivi:

N	Numero di primi compresi fra 1 e *N*, che spesso si indica con $\pi(N)$	Distanza media fra due numeri primi successivi
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

Nell'ultima colonna a destra emerge questa possibile struttura: se ad esempio consideriamo l'intervallo da 1 a 100 (prima colonna) abbiamo 25 numeri primi (seconda colonna) e quindi uno ogni 4 (terza colonna), quindi in media per trovare il numero primo successivo bisogna aggiungere 4. Se consideriamo i numeri fino a 10.000, troviamo 1.229 primi, in media uno ogni 8.1. E si può osservare, inoltre, che superato 10.000 l'incremento della terza colonna è sempre di circa 2.3.
Perciò Gauss scoprì che ogni volta che moltiplicava *N* per 10 doveva aggiungere 2.3 circa al rapporto fra i numeri primi e *N*. E semplicemente osservando che tale relazione tra moltiplicazione e addizione è la stessa che intercorre tra i logaritmi (quando si moltiplicano due numeri i loro logaritmi si sommano) Gauss riuscì a trovare un nesso importante tra numeri primi e logaritmi in base *e*, ovvero che per i numeri compresi fra 1 e *N,* grossomodo ogni *log N* numeri ce ne sarà uno primo.

[altre osservazioni sulla tabella potrebbero farle i ragazzi, tipo che il rapporto ci da la probabilità di trovare un primo nell'intervallo (se lo sanno) oppure che il rapporto aumentando N diminuisce e quindi la probabilità di trovare i primi è di meno].

E, a giudizio di Gauss stesso, aumentando *N* questa approssimazione risultava sempre migliore, ma non fu in grado di dimostrarlo.

Ci riuscì parecchi anni dopo Bernhard Riemann, che non solo perfezionò la funzione ideata da Gauss e la trasformò in un'altra funzione *R(N)* che approssimava con maggior precisione il numero dei primi presenti in un certo intervallo, come si può apprezzare dalla tabella

N	Numero di primi $\pi(N)$ compresi fra 1 e N	Sovrastima data dalla funzione di Riemann $R(N)$	Sovrastima data dalla funzione di Gauss $Li(N)$
10^2	25	1	5
10^3	168	0	10
10^4	1.229	-2	17
10^5	9.592	-5	38
10^6	78.498	29	130
10^7	664.579	88	339
10^8	5.761.455	97	754
10^9	50.847.534	-79	1.701
10^{10}	455.052.511	-1.828	3.104
10^{11}	4.118.054.813	-2.318	11.588
10^{12}	37.607.912.018	-1.476	38.263
10^{13}	346.065.536.839	-5.773	108.971
10^{14}	3.204.941.750.802	-19.200	314.890
10^{15}	29.844.570.422.669	73.218	1.052.619
10^{16}	279.238.341.033.925	327.052	3.214.632

ma diede vita a una delle teorie più celebri della matematica dall'800 ad oggi: la *congettura di Riemann.*
Si tratta di una teoria abbastanza sofisticata (su cui non vogliamo intrattenerci) che servendosi di funzioni sinusoidali e numeri immaginari riesce a ipotizzare a ragione un ordine nell'apparente casualità dei numeri primi. Riemann ebbe il grande merito di "guardare" le cose nel modo giusto: l'ordine c'è sempre stato, i mezzi per scoprirlo anche…era necessario servirsene nel modo giusto.
Tuttavia Riemann non riuscì a dimostrare la sua congettura, la questione è attualmente aperta e c'è perfino un premio in denaro di un milione di dollari per chiunque riesca a dimostrarla!

Congruenze

Un altro potente strumento matematico di cui si serve la crittografia è il concetto di congruenza, che impareremo ad usare in questo laboratorio.
La prima intuizione su questo argomento è dovuta ancora una volta a Gauss, con l'invenzione del suo *calcolatore a orologio.*
Il nome è dovuto al fatto che l'idea è analoga al funzionamento di un orologio, anche se nella mente di Gauss non si trattava di una macchina materiale, ma solo di un'idea astratta: se l'orologio dice che sono le 9 e aggiungiamo 4 ore, la lancetta delle ore si sposta sull'una. Allo stesso modo il calcolatore a orologio di Gauss fornisce 1 invece di 13 come risultato di 9+4. E volendo fare un

calcolo più “complicato”, come ad esempio 7x7, il calcolatore a orologio gli forniva il risultato della divisione di 49 (ossia 7x7) per 12, cioè di nuovo 1.
Ma era quando Gauss voleva calcolare 7x7x7 che la potenza dello strumento cominciava ad emergere: invece di moltiplicare un’altra volta 49x7, Gauss poteva limitarsi a moltiplicare per 7 l’ultimo risultato ottenuto, cioè 1, per ottenere la risposta, cioè 7, senza dover calcolare effettivamente 7x7x7=343. Egli sapeva così con minor fatica quanto faceva 343 diviso 12.
Ma il calcolatore dimostrò davvero tutta la sua potenza quando Gauss cominciò ad usarlo con numeri molto grandi, che oltrepassavano le sue stesse capacità di calcolo manuale. Ad esempio, pur non avendo idea di quanto facesse 7^{99}, il suo calcolatore a orologio col procedimento appena descritto gli diceva che quel numero diviso per 12 dava come resto 7.
Il passo successivo avvenne quando Gauss si rese conto che non c’era nulla di speciale nel numero 12 (quello utilizzato dall’orologio) e che quindi l’idea poteva essere applicata a qualsiasi numero intero. Introdusse, perciò, l’idea di una nuova aritmetica, chiamata *aritmetica modulare,* basata su orologi con qualsiasi numero di ore. Per esempio, se inseriamo il numero 11 in un calcolatore a orologio diviso in 4 ore, la risposta che otterremo sarà 3, come il resto della divisione di 11 per 4.
Impareremo quindi ad usare questa nuova aritmetica e capiremo come il mondo della crittografia e della sicurezza informatica si basano su questa geniale idea di Gauss. Anche se si usano in questo ambito immaginari “orologi” con numeri di ore dell’ordine di centinaia di cifre.

Matematica e crittografia

Come si legano tra loro i due concetti cardine del nostro laboratorio, le congruenze e i numeri primi, con la crittografia? E’ questo l’obiettivo che ci prefiggiamo di raggiungere al termine di questo percorso laboratoriale; scopriremo, infatti, che le funzioni di cifratura e decifratura (di tutti i sistemi che passeremo in rassegna) si tengono in piedi sulla solida struttura delle congruenze e che la sicurezza attuale del sistema RSA, cui abbiamo accennato precedentemente, si basa quasi esclusivamente sulla nostra incompleta conoscenza dei numeri primi. Daremo a tal proposito nella lezione conclusiva un’idea della *fattorizzazione* dei numeri in primi e vedremo quali difficoltà presenta sia manualmente che con l’importante contributo del calcolatore.