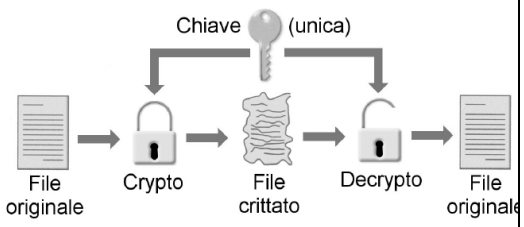
Fino a poco tempo fa si riteneva che tutti i sistemi crittografici dovessero avere chiavi simmetriche cioè dovevano servire sia a criptare sia a decriptare. La chiave era un segreto condiviso fra mittente e ricevente.

Il passaggio dalla chiave unica alla chiave pubblica

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 simmetrica a quella di cifratura. 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 cifratura e decifratura. Ma 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**.

Martin Hellman nato nel 1946 ha svolto la sua carriera professionale come ingegnere all'IBM ed al MIT, dove conobbe Diffie.

Whitfield Diffie nato nel 1944 in USA fu matematico al MIT (*Massachusetts Institute of Technology*).



Valigia con messaggio di Alice

Alice inserisce il suo lucchetto

Bob inserisce il suo lucchetto e rispedisce ad Alice

Alice toglie il suo lucchetto

Bob toglie il suo lucchetto e apre la valigia

Whitfield Diffie e Martin Hellman ebbero l'idea che cambiò la crittografia. Con il metodo del doppio lucchetto. Supponiamo che Alice (A) debba inviare un messaggio a Bob (B). A pone il messaggio in una cassetta e la chiude con un lucchetto di cui solo lei possiede la chiave ed invia a B la cassetta. B, ricevuta la cassetta, aggiunge un suo lucchetto e rispedisce il tutto ad A che, ricevuta la cassetta con doppio lucchetto, toglie il suo lucchetto e rispedisce la cassetta a B. Quando B riceve la cassetta la può aprire togliendo il suo lucchetto. Questo metodo evita lo scambio di chiavi, ma ha come problema che la cassetta viaggia più volte. Nel 1976 ***Whitfield Diffie*** e ***Martin Hellman*** idearono un sistema per cui due individui potevano scambiarsi messaggi cifrati, senza doversi scambiare alcuna chiave. Nel tentativo di scoprire nuovi algoritmi sempre più efficaci, Diffie teorizzò un crittosistema nel quale:

- la chiave di codificazione è diversa da quella di decodificazione e, ovviamente, una non è derivabile dall'altra
- delle due chiavi rende ***pubblica*** solo la prima, affinché tutti quelli che desiderano inviargli un messaggio, possano criptarlo. Una volta ricevuto il messaggio, il destinatario utilizza la sua chiave, ***privata***, per decriptare il messaggio
- ogni persona, quindi, possiede una chiave pubblica che può divulgare perché serve solo a cifrare il messaggio, e una privata che resta segreta e che serve per decifrarlo.

Il problema è quello di trovare il modo per implementare matematicamente questo sistema.

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.

CONOSCERE LA STRADA PER ANDARE

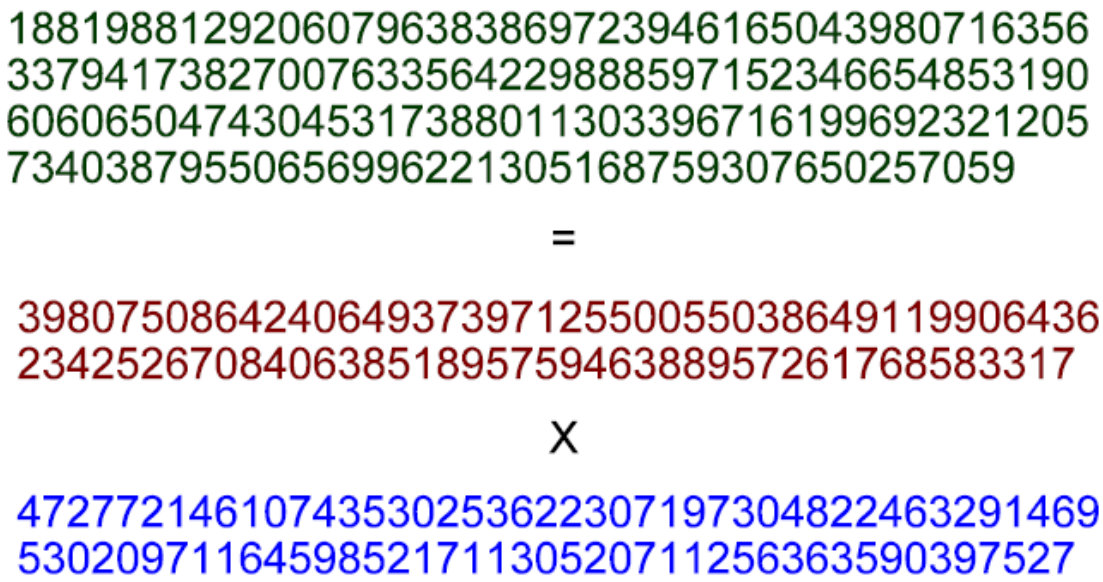
VUOL DIRE

CONOSCERE LA STRADA PER TORNARE ???

Non è sempre così !

ES. Elenco del telefono

In effetti, risolvere un esercizio è pur sempre una scommessa, una sfida piena di incognite e di incertezze. Verificarne la soluzione – una volta che è stata acquisita – può essere talora faticoso, ma ha il pregio di una procedura "tranquilla". In molte situazioni cercare una soluzione può essere esperienza impegnativa, mentre controllare la soluzione trovata richiede talvolta una semplice occhiata. Ad esempio, pensiamo alla decomposizione dei numeri naturali N nei loro fattori primi. Trovare i fattori primi di un numero composto N è, ancor oggi (almeno per N grande), esercizio complicato e difficile, privo di procedure adeguatamente veloci e soddisfacenti; invece, verificare la decomposizione di N, una volta che se ne conoscono i fattori, richiede solo una semplice moltiplicazione. Nasce allora la curiosità generale di confrontare da un lato le risorse necessarie per risolvere un problema, dall'altro quelle richieste per controllarne le soluzione. In particolare, ci possiamo domandare: se la verifica può essere svolta in modo rapido (come nel caso della decomposizione), può dirsi lo stesso della soluzione? L'esempio degli interi ci mostra che la questione ha aspetti affascinanti, ma in qualche caso attende ancora una risposta definitiva.



SIMMETRICI

SISTEMI

ASIMMETRICI

In altre parole, in alcuni 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. 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** (Rivest, Shamir, Adleman) per mezzo di una funzione che possiamo definire “a senso unico” (come si vedrà nelle lezioni successive). Per questo motivo i sistemi a chiave privata sono detti anche ***simmetrici***, mentre quelli a chiave pubblica ***asimmetrici.*** L’idea concettuale che si cela dietro questo potente sistema crittografico è geniale: ci è permesso divulgare sia la chiave di cifratura che il metodo, ma senza per questo rivelare contestualmente il modo di decifrare.

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. Il “lucchetto” pubblico è in realtà una funzione matematica abbastanza semplice che tutti sono in grado di utilizzare, mentre la funzione inversa consente di tornare indietro agevolmente solo a chi è in

possesso della “chiave”. Il tutto è quindi basato su una funzione cifrante, la cui inversa è complessa solo apparentemente e diventa improvvisamente molto semplice non appena la si guarda attraverso l’informazione aggiuntiva (data dalla chiave). Nelle prossime lezioni si capirà di quale funzione stiamo parlando.

La ricerca di numeri primi era apparsa apparentemente 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”


Pierre de Fermat

“Quello che oggi è un fatto della matematica, domani sarà un trampolino per la scienza“
(Giancarlo Rota)

Strumenti per la crittografia moderna

- La crittografia moderna è stata fortemente influenzata dall’informatica e dalla matematica
- L’informatica
  - pone nuove sfide rendendo possibile decifrare in modo semplice cifrari ritenuti impossibili
  - chiede nuove applicazioni e nuove tecniche: ad esempio lo scambio di chiavi, la crittografia a chiave pubblica, la firma digitale, ...
  - fornisce hardware e soprattutto software per la crittografia

MATEMATICA E CRITTOGRAFIA

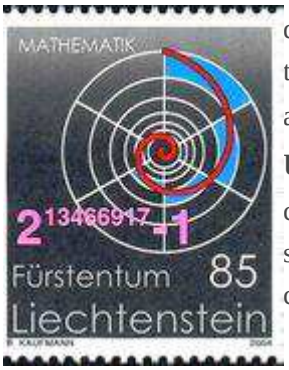
Il ruolo fondamentale dei moderni sistemi di cifratura sono **i numeri primi e la teoria dei numeri** (parte della matematica pura che si occupa delle proprietà dei numeri interi ; molti problemi aperti possono essere facilmente compresi anche da chi non è un matematico).Come si legano tra loro i due 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; 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 si basa quasi esclusivamente sulla nostra incompleta conoscenza dei numeri primi e sulla difficoltà della *fattorizzazione* di un numero .

- La matematica è lo strumento fondamentale per la crittografia
  - fornisce metodi per cifrare, decifrare, firmare e controllare messaggi
  - garantisce la sicurezza della crittografia
  - studia (unitamente all'informatica) come svolgere velocemente le operazioni crittografiche

Qualche osservazione sulla ricerca di numeri primi

"I matematici hanno tentato, sinora invano, di scoprire una regolarità nella successione dei numeri primi, e abbiamo ragione di credere che in essa sia riposto un mistero che lo spirito umano non penetrerà mai. Per convincersene, d'altronde, basta gettare uno sguardo su una tavola di numeri primi: ci si convince, allora, che non vi regnano né ordine né regola" Leonhard Eulero (1707- 1783)

1991 : la comunità scientifica brinda a una nuova scoperta. È stato trovato un nuovo numero primo, e non uno qualsiasi, ma il più grande e per giunta un numero primo di Mersenne, particolarmente rari. A trovarlo è stato il professor Curtis Cooper dell'Università del Missouri, all'interno di un progetto avviato diciassette anni fa e denominato Great Internet Mersenne Prime Search (Gimps), che utilizza i computer messi a disposizione dai volontari per elaborare calcoli su un algoritmo sviluppato dall'ex Apple Richard Randall nel 1990 e liberamente scaricabile. Il numero è così lungo che a scriverlo con cifre di un centimetro di larghezza coprirebbe la distanza di 170 km.



Nel 1996 è stato lanciato il programma **GIMPS** (Great Internet Mersenne Prime Search) a cui tutti possono partecipare mettendo a disposizione le proprie risorse informatiche (i numeri primi di Mersenne l'hanno fatta da padroni ed a tuttora occupano le prime cinque posizioni.) Il fatto è che la ricerca è bella in sé, è una sfida della nostra capacità di pensare nei confronti di quantità tanto grandi da non corrispondere a niente che esista nell'universo.

FEBBRAIO 2013 : Scoperto il più grande numero primo, ha 17 milioni di cifre

Ha anche la particolarità di appartenere a uno specifico gruppo di numeri primi: quelli di Mersenne [un **numero primo di Mersenne** è un numero primo esprimibile come:

$M_n = 2^n - 1$,con n intero positivo primo.]

I numeri primi di Mersenne prendono il nome dal matematico francese Marin Mersenne (1588-1648)]

Il numero primo più grande che c'è

Scoperto il più grande numero primo sin qui noto, una cifra che ha richiesto più di un mese di calcolo non-stop e che rappresenta una peculiare categoria di numeri primi rari

I ricercatori del progetto GIMPS (Great Internet Mersenne Prime Search) hanno confermato la scoperta del più grande numero primo mai calcolato, un "mostro" composto da ben 17.425.170 cifre che straccia il precedente campione della categoria individuato nel 2008 e lungo appena 12.978.189 cifre.

Questa ricerca dei numeri megaprimi, al di là della grande gara, limitata un tempo all'ambiente dei matematici e allargata oggi a tutti i possessori di un PC riuniti in rete fra loro, ha introdotto nuove tecniche di calcolo nella moltiplicazione dei grandi numeri, utili in molte applicazioni tecniche e scientifiche, innanzitutto nei codici cifrati. La Intel usa una versione modificata del programma di Woltman per scoprire possibili difetti dei suoi Pentium.
La caccia continua e chi volesse aderire all'iniziativa tenga presente che da alcuni mesi è disponibile anche la versione italiana del sito del GIMPS. L'indirizzo al quale collegarsi per avere tutte le informazioni e scaricare il programma necessario per partecipare alla caccia è il seguente:

http://www.mclink.it/personal/MC5225/mersenne/prime-it.htm

Con un po' di fortuna si potrebbe così scoprire un nuovo numero primo da record e vedere il proprio nome scritto accanto a quello dei grandi matematici, studiosi della teoria dei numeri. Ci sono inoltre alcuni premi in palio offerti dalla Electronic Frontier Foundation, una fondazione finanziata da un anonimo mecenate. Il fine dichiarato della EFF è di "incoraggiare i normali utenti di Internet a contribuire alla soluzione di grandi problemi scientifici": 100 mila dollari per chi scoprirà un numero primo con almeno 10 milioni di cifre, 150 mila dollari per chi riuscirà a superare i 100 milioni di cifre e 250 mila dollari, un premio da lotteria, per un numero primo con almeno un miliardo di cifre. Il principio è semplice: dato che parte del processore del proprio computer è generalmente inutilizzato durante le operazioni di routine, gli utenti in rete decidono di cedere parte della potenza di calcolo della macchina per svolgere operazioni e calcoli, contribuendo così a un progetto scientifico. Funziona allo stesso modo SETI@Home, in cui sono scaricati e analizzati i dati dei radiotelescopi per la cosiddetta *Search for Extraterrestrial Intelligence* (Seti, per l'appunto, ovvero *Ricerca dell'Intelligenza Extraterrestre*). Gimps può contare su circa 160mila processori, in grado di eseguire 150 trilioni di calcoli al secondo.

Il numero scoperto, $2^{57885161} - 1$, fa parte di una categoria particolare di primi, i cosiddetti **primi di Mersenne**, scoperti dal monaco francese **Martin Mersenne** più di 300 anni fa, tutti nella forma $2^p - 1$, dove p è esso stesso un numero primo. Finora, compreso l'ultimo, ne sono stati scoperti solo 48. *"È un'impresa analoga alla scalata dell'Everest"*, sostiene George Woltman, informatico in pensione e fondatore di Gimps: *"Le persone provano piacere cercando di scoprire qualcosa fino ad allora sconosciuta"*.

Sebbene il modo più intuitivo di cercare numeri primi possa sembrare quello di dividere ogni *candidato* per i numeri minori, non è così: sarebbe troppo dispendioso in termini di tempo computazionale. *"Procedendo in questo modo"*, continua Woltman: *"si impiegherebbe un tempo più lungo dell'età dell'Universo"*. Al contrario, i matematici hanno messo a punto una strategia molto più scaltra, che riduce notevolmente il tempo necessario a scovare gli sfuggenti numeri, permettendo di controllare molti meno divisori.

Numero Primo	Cifre	Autori	Anno
$2^{13\,466\,917} - 1$	4 053 946	Cameron & GIMPS	2001
$2^{6\,972\,593} - 1$	2 098 960	Hajratwala & GIMPS	1999
$2^{3\,021\,377} - 1$	909 526	Clarkson & GIMPS	1998
$2^{2\,976\,221} - 1$	895 932	Spence & GIMPS	1997
$2^{1\,398\,269} - 1$	420 921	Armengaud &GIMPS	1996
$843832^{65536} - 1$	388 384	Gallot, Fougeron	2001
$2^{1\,257\,787} - 1$	378 632	Slowinski e Cage	1996
$108368^{65\,536} + 1$	329 968	Bodenstein, Gallot	2001
$48594^{65\,536} + 1$	307 140	Scott, Gallot	2000
$3 \times 2^{916\,773} + 1$	275 977	Cosgrave, Jobling, Woiltman, Gallot	2001

La pagina più completa e accurata sui numeri primi è quella di Chris K. Caldwell, matematico dell'Università del Tennessee

http://www.utm.edu/research/primes

Per proprietà dei numeri primi:

Jean Paul Delahaye *Stupefacenti numeri primi. Viaggio nel cuore dell'aritmetica* Ghisetti e Corvi ed.

Numerosi sono i testi e i siti sulla crittografia. Qui ve ne segnalo alcuni interessanti per l'aspetto della storia, ricordando che

"Una volta un tale che doveva fare una ricerca andava in biblioteca, trovava dieci titoli sull'argomento e li leggeva; oggi schiaccia un bottone del suo computer, riceve una bibliografia di diecimila titoli, e rinuncia"

Umberto Eco, La Bustina di Minerva, 2000

TESTI

- Simon Singh, *"Codici e Segreti – La storia affascinante dei messaggi cifrati dall'antico Egitto ad Internet"* BUR Saggi
- Joan Gomez Urgelles *Matematici, spie e pirati informatici* Mondo Matematico

SITI INTERNET

- http://matematica.unibocconi.it/articoli/invito-alla-crittografia
- www.matematicamente.it/storia/crittografia.htm
- http://www2.dm.unito.it/paginepersonali/roggero/Crittografia.pdf
- www.icosaedro.it/crittografia/chiavi-simmetriche.html (qui trovi una "*Crittomacchina Vigenère* " in programma JavaScript che realizza la crittazione di Vigenère).

Se vuoi " cogliere lo spirito" di Bletchley Park: *ENIGMA*, film di Michael Apted (coproduzione inglese, statunitense, tedesca e olandese, 2001) tratto dall'omonimo libro di Robert Harris.

“E’ difficile dare un’idea della vasta distesa della matematica moderna. La parola “distesa” non è esatta; intendo alludere a un’estensione ricca di particolari, non uniforme come una pianura liscia e senz’alberi, a una zona facente parte di un bel paese che si ammira da principio a distanza, ma che si merita di essere percorsa da un capo all’altro, studiata in tutti i suoi particolari: colline, vallate, corsi d’acqua, cime rocciose, boschi e fiori. ***Ma bisogna dire che avviene della matematica come di qualunque altra cosa: la sua bellezza può essere sentita, non spiegata****.* “ (Cayley)

2000 anno mondiale della matematica

Manifesto nella metropolitana di Londra