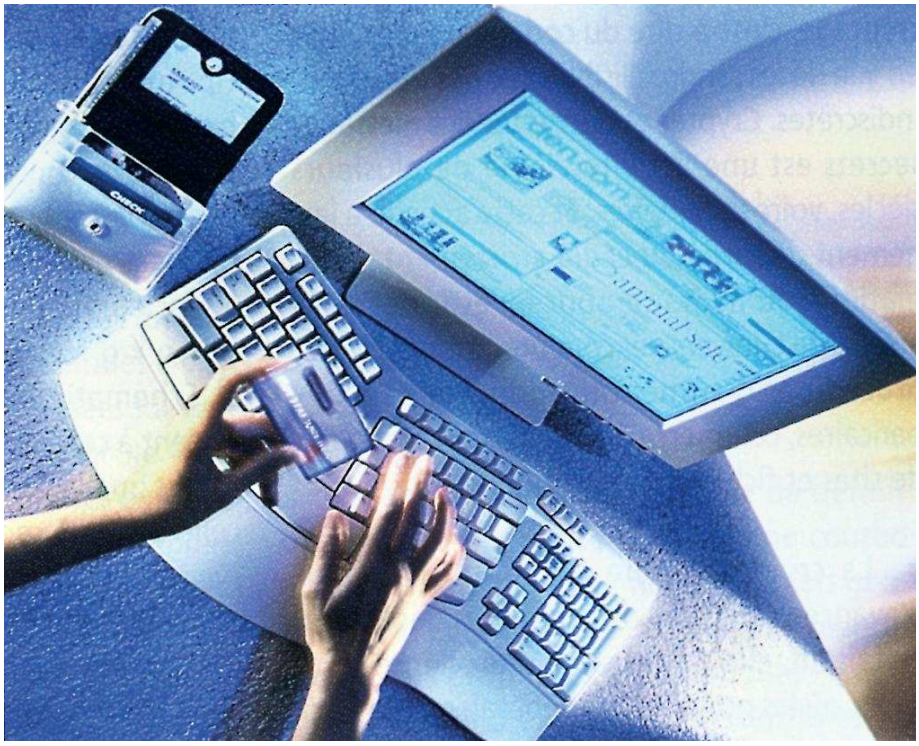
Criptaggio e decriptaggio: comunicare in tutta sicurezza

Jean Luis Nicolas

Nel mondo attuale, dove le telecomunicazioni occupano un posto cruciale, la crittografia gioca un ruolo centrale. Essa è diventata una scienza così complessa che non può fare a meno della matematica di alto livello.

Nel marzo 2000 un grosso titolo era sulla prima pagina di tutti i giornali: "Attenzione alla sicurezza delle carte bancarie". Cosa era successo? In Francia, il codice segreto delle carte magnetiche era protetto dal 1985 grazie ad un metodo di criptaggio che usava un grande numero N costituito da 97 cifre. Questo numero N doveva essere il prodotto di due grandi numeri primi, vale a dire di



Pagare con la propria carta di credito, fare acquisti su Internet: i metodi della crittografia, che trattano matematica molto bella, sono indispensabili per la sicurezza di queste operazioni. (Foto Getty Images)

numeri che, come ad esempio il 7 o il 19, sono divisibili solo per 1 e per se stessi. Il codice segreto di una carta bancaria è costituito esattamente da questa coppia di numeri primi; il calcolo a partire da N era praticamente impossibile negli anni '80. Ma con l'aumento della potenza dei calcolatori ed il miglioramento dei metodi matematici, la grandezza dei numeri N, di cui non si possono calcolare i fattori primi in tempi ragionevoli, ha oltrepassato il centinaio di cifre negli ultimi anni del secolo scorso (nel gennaio del 2002 il record era di 158 cifre). Un astuto informatico, Serge Humpich, aveva così potuto trovare i due numeri primi ultra segreti il cui prodotto valeva N e li aveva utilizzati per fabbricare carte bancarie false.

Allora, per garantire la sicurezza dei nostri piccoli rettangoli di plastica, l'organismo di gestione delle carte bancarie ha subito costruito dei nuovi numeri N nettamente più grandi.

La crittografia moderna, incrocio fra matematica e informatica

Questa vicenda illustra l'importanza considerevole che riveste oggi la scienza del criptaggio, vale a dire della codifica dei messaggi con lo scopo di renderli illeggibili ad occhi indiscreti.

Criptare e decriptare dei messaggi segreti è un'attività vecchia di molti secoli, addirittura millenni. E questa attività è largamente fuoruscita dagli ambienti strettamente diplomatici o militari per investire lembi interi dell'universo delle comunicazioni civili: procedure d'autenticazione, transazioni bancarie, commercio elettronico, protezione di siti e schedari informatici, etc...

La crittografia ha conosciuto vari sviluppi nel corso degli ultimi decenni. Di conseguenza, essa è divenuta una scienza complessa, dove i progressi sono generalmente opera di specialisti con una formazione matematica ed informatica. Questa specializzazione si è manifestata a partire dalla seconda guerra mondiale. Oggi sappiamo che la decriptazione da parte degli alleati dei messaggi codificati dalla famosa macchina tedesca "Enigma" ha giocato un ruolo importante in questo conflitto. Un eminente matematico britannico, Alan Turing, uno dei padri della informatica teorica, ha apportato un contributo essenziale a questa decriptazione.

Negli anni '70 la crittografia ha conosciuto una piccola rivoluzione: l'invenzione della crittografia a "chiave pubblica" con il metodo RSA. Di che cosa si tratta? Fino ad allora i corrispondenti che volevano scambiarsi messaggi segreti condividevano una chiave segreta ed il rischio di intercettazione di questa chiave da parte del nemico era notevole. Il protocollo RSA, chiamato così in onore dei suoi inventori (Ronald Rivest, Ad Shamia e Leonard Adleman) ha risolto questo problema.

Questo metodo usa due chiavi: una chiave di criptaggio pubblico – cioè essa può essere conosciuta da tutti – e una chiave di decriptazione, che rimane segreta. Essa si basa sul principio (utilizzato in seguito per proteggere le carte bancarie, come abbiamo visto in precedenza) che è possibile costruire dei grandi numeri primi (di cento, mille cifre, ed oltre) ma che è

estremamente difficile ritrovare i fattori primi p e q di un grande numero N, che sia $N = p \times q$, conoscendo solo N. Schematicamente, la conoscenza di N rimanda a quella della chiave pubblica di criptaggio, mentre la conoscenza di p e q rimanda a quella della chiave segreta di decriptazione.

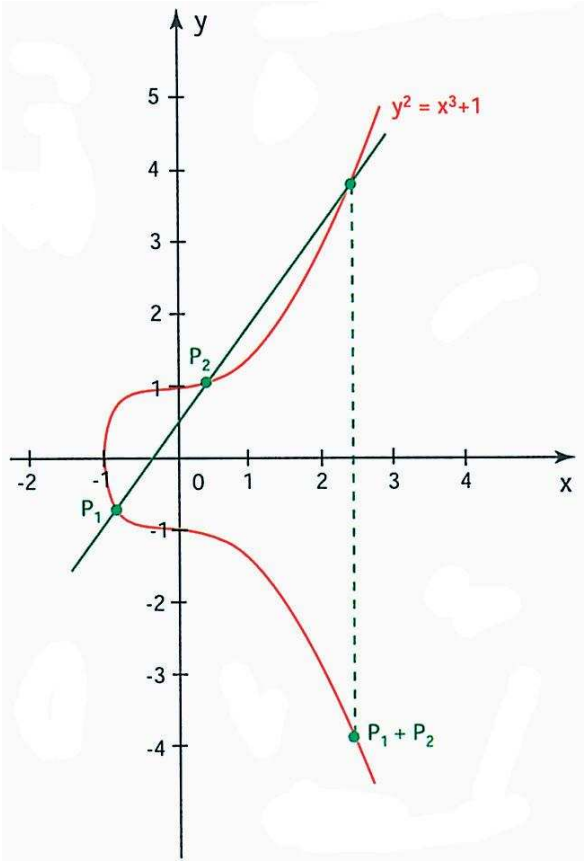
Evidentemente, se qualcuno trovasse un metodo per decomporre rapidamente nei loro fattori primi dei grandi numeri, il protocollo RSA diventerebbe inefficace. Ma potrebbe anche succedere che i matematici provino che tale metodo non esista, ciò rafforzerebbe la sicurezza del protocollo RSA. Questi sono degli argomenti di ricerca fondamentali.

I metodi che, come il protocollo RSA, fanno intervenire elaborate teoria dei numeri, portano un grande insegnamento: le ricerche matematiche (sui numeri primi specialmente) fatte disinteressatamente, possono rivelarsi, anni o decenni più tardi, cruciali per svariate applicazioni; questo in maniera imprevedibile. Nel suo libro "L'apologia di un matematico", il grande teorico dei numeri britannico G. H. Hardy (1877-1947), che era un fervente pacifista, si vantava di lavorare in un campo perfettamente puro, l'aritmetica, e di non aver mai fatto niente che poteva essere considerato "utile". I suoi lavori erano forse "inutilità" nella sua epoca. Oggi è falso.

Curve ellittiche: la geometria algebrica al servizio degli agenti segreti

E tutto ciò non riguarda soltanto la teoria dei numeri. Altri campi della matematica pura considerati privi di applicazione, contribuiscono alla sicurezza del criptaggio.

Metodi crittografici promettenti basati su principi vicini a quelli del protocollo RSA sono apparsi nel corso degli ultimi anni. È così per il metodo detto del "logaritmo discreto". Questo è servito a sua volta a concepire dei metodi che si basano sulle proprietà delle *curve ellittiche*. Non si tratta di curve aventi la forma di una ellisse, ma di curve il cui studio è



Il grafico della curva ellittica di equazione $y^2 = x^3 + 1$. Le curve ellettiche hanno una notevole proprietà: si possono "addizionare" i loro punti secondo il procedimento indicato sul disegno. La "somma" così definita rispetta le consuete leggi aritmetiche; ad es. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Certi metodi attuali di crittografia necessitano delle curve ellittiche e delle loro proprietà algebriche.

iniziato nel secolo XIX per risolvere il difficile problema del calcolo del perimetro di una ellisse. Queste curve, per le quali le coordinate (x, y) dei loro punti verificano una equazione del tipo $y^2 = x^3 + a\,x + b$, hanno interessanti proprietà il cui studio fa parte della *geometria algebrica* - settore di grande interesse nella matematica attuale. Per esempio, con l'aiuto di una appropriata costruzione geometrica, è possibile definire una somma fra i punti di una curva ellittica. In generale, le curve ellittiche sono oggetti geometrici che possiedono delle proprietà aritmetiche – che sono sotto continua indagine – in grado di rendere un utile servizio alla crittografia. In tal modo è stato sviluppato un metodo crittografico detto *logaritmo discreto sulle curve ellittiche*.

Recentemente si è sviluppato un altro orientamento. Al congresso internazionale dei matematici a Berlino nel 1998, Peter Shor, dei laboratori della AT&T, ha ottenuto il premio *Nevanlinna* per i suoi lavori sulla *crittografia quantistica*. Che cosa significa questo termine? Da qualche anno alcuni fisici e matematici hanno immaginato che un giorno sarà possibile realizzare un calcolatore quantistico, vale a dire un calcolatore il cui funzionamento sfrutterebbe le leggi bizzarre della fisica quantistica, quelle che regnano nel mondo dell'infinitamente piccolo. Ci si è resi conto che un tale calcolatore, se fosse realizzabile, sarebbe capace di fattorizzare molto più velocemente grandi numeri e renderebbe quindi inefficace il metodo RSA. Alcuni ricercatori considerano concreta la realizzazione di un calcolatore quantistico, d'altronde ci sono state pubblicazioni molto recenti sulla rivista britannica *Nature* a favore di tale ipotesi (vedere riferimento bibliografico). D'altro canto, dei ricercatori hanno elaborato alcuni protocolli di crittografia quantistica, vale a dire dei metodi di criptaggio che utilizzano degli oggetti (fotoni, atomi, etc...) obbedienti alle leggi quantistiche. Questi protocolli quantistici potrebbero garantire una sicurezza infallibile. Tutto ciò è in fase di elaborazione e potrebbe diventare operativo tra qualche anno.

Jean Lous Nicolas
Istituto Gerard Desargues, Matematica, Università Claude-Bernard (Lione 1)

Alcuni riferimenti bibliografici:

- D. Kahn, *La guerre des codes secrets* (Interéditions, 1980).
- J. Stern, *La science du secret* (Odile Jacob, 1998).
- S. Singh, *Histoire des codes secrets* (J.-C. Lattès, 1999).
- J.-P. Delahaye, *Merveilleux nombres premiers* (Belin/Pour la Science, 2000).
- D. Stinson, *Cryptographie, théorie et pratique* (Vuibert, 2001).
- L. M. K. Vandersypen et al., "*Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*", Nature, vol. 414, pp. 883-887 (20 décembre 2001).