Programmazione.it

Matematica e crittografia (1/2)

Scritto da Davide Panceri il 07-09-2007 ore 13:35

Il sito dell'American Mathematical Society pubblica un interessante contributo di Neal Koblitz sulle non facili relazioni tra matematica e crittografia, che presenta diversi spunti di riflessione legati anche alla storia più recente della disciplina. In questa prima parte, mi soffermerò sui collegamenti storici, politici ed economici della disciplina e della sua evoluzione nell'ultima parte del ventesimo secolo. Nella seconda cercherò di avvicinarmi, con timoroso rispetto, ad alcuni spunti teorici tra quelli segnalati dall'autore, e dirò qualcosa sulle contaminazioni tra discipline.

In primo luogo è d'obbligo una riflessione sui confini tra estetica, scienza speculativa e applicazioni pratiche. Da un lato, abbiamo la posizione di Paul Halmos, che si preoccupa di non contaminare la scienza matematica con applicazioni pratiche — *"Applied Mathematics Is Bad Mathematics"*, ma gli sviluppi applicativi (militari e civili, e soprattutto quelli legati all'uso del denaro) hanno contribuito molto al progresso teorico. Probabilmente la visione speculativa della matematica in generale ha una sua ragion d'essere, ma le applicazioni — quando non si cerca il risultato a ogni costo — possono servire da stimolo per ricerche anche innovative.

Di questo capitolo fa parte anche la preoccupazione di vedere la teoria dei numeri applicata a scopi militari, abbastanza comprensibile in un clima di guerra fredda e minacce nucleari più o meno verosimili, e di cui oggi si sente molto meno il peso rispetto agli anni Settanta-Ottanta del Novecento. E' curioso ad ogni modo osservare gli scambi tra studiosi russi e americani in materia, rallentati più dalla posta che dalla CIA, in un periodo nel quale la Rete era uno strumento di difesa militare, e non serviva per lo scambio di informazioni tra ricercatori.

Come osserva Neal Koblitz, le applicazioni pratiche stimolano nuove ricerche, e appagano i ricercatori, in termini non solo economici, ma anche di sfida intellettuale. Probabilmente anche la matematica sottostante alla poca crittografia in circolazione nel secolo passato poteva essere davvero poco interessante, ma al giorno d'oggi il livello di complessità raggiunto è notevole. Anche per questo, diversi anni fa poteva capitare che qualcuno all'IBM non pensasse di brevettare un algoritmo (quello della curva ellittica o ECC per l'esattezza), ritenendolo una brillante costruzione teorica senza risvolti pratici a breve termine. Naturalmente, la corsa ai brevetti può anche avere effetti deleteri sulla ricerca, perché limita la condivisione del sapere che, a sua volta, ne alimenta la crescita. Non sto prendendo una posizione dogmatica, ma credo che questo problema sia molto difficile da risolvere, come testimoniano le numerose controversie sulla proprietà intellettuale contro la libera circolazione del sapere.

Nell'attività di chi si occupa di crittografia, la componente di sfida intellettuale è peculiare: i risultati delle ricerche non sono garantiti come assiomi e teoremi, e possono essere messi in crisi anche dall'evoluzione delle macchine, sempre più potenti nel portare attacchi del tipo *brute force*. Questi argomenti saranno il tema della seconda parte di questa segnalazione. Nell'attesa ,è possibile scaricare e leggere l'intervento da cui ho preso spunto, nel quale gli argomenti sono sviluppati in modo più dettagliato.

Programmazione.it

Matematica e crittografia (2/2)

Scritto da Davide Panceri il 11-09-2007 ore 08:31

Mentre nella prima parte di questa segnalazione mi sono soffermato su alcune considerazioni storiche e generali riguardanti i legami tra crittografia e matematica, in questa seconda parte vorrei sottolineare alcuni aspetti più tecnici e teorici, e alcune conseguenze della contaminazione tra le due discipline, da estendere ai rapporti tra scienza e applicazioni commerciali più in generale.

In primo luogo, un cenno minimo alla storia: può essere interessante sapere che risale al 1977 l'idea della crittografia RSA, ad opera di tre scienziati del (solito) MIT, Ron Rivest, Adi Shamir e Len Adleman. Questa informazione comprende anche la chiave per decrittare, se necessario, l'acronimo. Il metodo proposto da questi studiosi è basato sull'uso di numeri primi, e a dimostrare in pratica quanto fosse (e sia tuttora) difficile fattorizzare un numero con parecchie cifre, fu Martin Gardner con un noto articolo per Scientific American; a questo proposito, una ricerca su RSA-129 può essere illuminante.

Per quanto riguarda gli aspetti più propriamente tecnici della materia, ho letto con molto interesse il racconto di come sia stato possibile smontare una congettura dal nome improbabile, che avrebbe a sua volta reso inutilizzabile EEC. E' possibile leggere alcuni riferimenti al cosiddetto Xedni Calculus tramite un certo numero di citazioni bibliografiche, anche se gli abstract sono un po' succinti, oppure approfondire in Rete, o tramite libri o riviste. Purtroppo, se viene richiesto di fornire username e password non è concesso rispondere *"devo leggere l'articolo per vedere di bypassare questa pagina"*.

Per chi volesse farsi un'idea circa gli sviluppi delle ricerche riguardanti l'applicazione alla crittografia delle curve ellittiche, o magari cercare un lavoro all'estero, è utile la consultazione del sito dell'Università di Waterloo. Anche il sito di Carl Pomerance contiene parecchi spunti e collegamenti interessanti. Infine, per chi preferisce la lingua italiana segnalo un corso introduttivo di livello universitario su EEC.

Un ultimo punto degno di nota — ma ce ne sono altri molto interessanti, ed è probabile che ne riprenda prossimamente qualcuno — riguarda i rapporti tra crittografia come scienza e come prodotto commerciale, ovvero, come conoscenza sottostante alla progettazione e implementazione di algoritmi inclusi poi nelle applicazioni commerciali. Come è logico immaginare, negli ultimi anni si assiste ad un proliferare di lavori in materia, anche in campo teorico e speculativo. Come è logico aspettarsi, la qualità del materiale presentato tende a scadere, anche per quanto riguarda quello inviato per i concorsi.

A quanto sembra, si tende a scrivere di più in sempre meno tempo e con poco controllo su quello che si scrive. I tempi della matematica e quelli della crittografia, influenzata dall'informatica e magari con una certa pressione dell'industria, sono parecchio diversi: un matematico scrive poco, e solo quando è sicuro di quello che dice. In ambito commerciale sono molto più frequenti le anticipazioni anche sbagliate, e spesso si cerca la presenza più della sostanza.

Concludo segnalando che parte delle informazioni contenute nell'articolo provengono dal libro **Random Curves: Journeys of a Mathematician**, in uscita presso Springer-Verlag, che si può già prenotare da Amazon.