

L'ipotesi di Riemann e la sicurezza di Internet

La sempre maggiore diffusione dei modelli organizzativi legati all'uso intelligente delle tecnologie internet e l'affermarsi dell'*ubiquitous computing* hanno portato ad una significativa crescita dell'utenza mobile in numerosi contesti professionali. La possibilità di utilizzare da remoto le risorse informatiche e di fruire dello stesso insieme di servizi applicativi dei quali si fa abitualmente uso dalla propria postazione d'ufficio sono divenute necessità imprescindibili per svolgere la propria attività quotidiana.

Simili modelli organizzativi, uniti all'avanzare di fenomeni sociali come la globalizzazione, hanno portato alla trasformazione degli ambienti ICT di tutte le organizzazioni, favorendo la nascita di infrastrutture di comunicazione aperte e potenzialmente accessibili a qualsiasi categoria di utenti.

Su tali infrastrutture sono nati anche nuovi modi di fare affari e offrire servizi nell'ambito della comunità: termini come *e-business*, *e-commerce*, *trading on-line*, *home banking*, *e-government* sono entrati da tempo nel linguaggio quotidiano a identificare operazioni telematiche che hanno sostituito di volta in volta un *modus operandi* basato su antiche pratiche consolidate.

E' indubbio, insomma, che oggi Internet rappresenti uno degli strumenti più potenti del nostro agire, oltre che il veicolo primario di diffusione dell'informazione.

Per queste ragioni, alla sua sicurezza è ormai legata in modo sostanziale la tranquillità del nostro operare quotidiano.

Come molti sapranno le lacune originarie della rete in termini di sicurezza sono state in parte colmate dall'introduzione di meccanismi di protezione applicati sia ai protocolli di comunicazione in uso, sia all'informazione in transito e a quella memorizzata. Pensiamo al paziente lavoro per la definizione di standard come IPSec, SSL o S/MIME e all'introduzione di meccanismi e strumenti di crittografia che a tali standard danno vita.

Proprio i meccanismi di crittografia costituiscono l'oggetto delle riflessioni che ho inteso stimolare nei lettori con le poche righe che seguono. Spesso siamo attenti a ciò che la superficie delle cose ci mostra, e trascuriamo l'infrastruttura fondamentale che queste cose sostiene: nel resto dell'articolo vorrei concentrare l'attenzione proprio sull'infrastruttura.

Cryptography is about mathematics, security is about people (B. Schneier)

In questa celebre frase di uno dei più famosi teorici della crittografia è racchiusa una profonda verità.

Le moderne tecniche di cifratura, infatti, si basano proprio sulle discipline matematiche e in particolare sulla teoria dei numeri. L'algoritmo crittografico più conosciuto, sul quale sono stati costruiti i meccanismi di cifratura a chiave pubblica maggiormente diffusi, è quello dell'americana RSA Security Inc. (ex RSA Data Security), nato nel 1978 proprio dall'idea di tre matematici: Rivest, Shamir e Adleman. I tre hanno sviluppato una tecnica di cifratura che si basa sull'impiego dei numeri primi e si affida alla sostanziale difficoltà di ricavare i numeri primi costituenti un numero intero – soprattutto quando quest'ultimo si compone di centinaia di cifre.

Lo studio di Rivest, Shamir e Adleman, che oggi a taluni può sembrare intuitivo, nasce molto lontano nel tempo ed ha legami con una congettura nota come *Ipotesi di Riemann*, corrispondente ad uno dei più grandi problemi irrisolti nel campo della matematica. L'ipotesi impegna la comunità matematica da oltre un secolo e stabilisce che i numeri primi (quelli divisibili unicamente per uno e per sé stessi) seguano un particolare andamento, noto come "*funzione zeta - $\zeta(s)$* ", scoperto da Bernhard Riemann nel 1859 [1][2].

L'ipotesi – di cui in questa sede non vengono discussi i dettagli – è stata verificata solo in via sperimentale e con riferimento ad oltre un miliardo di numeri primi, ma di essa non è mai stata data alcuna dimostrazione formale che le facesse assumere il rango di vero e proprio teorema^{1,2}. Svelare il mistero dell'ipotesi di Riemann vorrebbe dire stabilire una regola matematica che dimostri se esiste o meno una logica nella distribuzione dei numeri primi, e quindi, in ultima analisi, significherebbe comprendere se vi è regolarità o casualità totale in quest'ultima distribuzione.

Essendo collegata alla serie dei numeri primi e alle formule per il calcolo del numero di numeri primi, sta diventando pensiero diffuso il fatto che un'eventuale dimostrazione di questa ipotesi potrebbe aprire la strada alla scoperta di nuovi metodi per scomporre un numero nei suoi fattori primi (fattorizzazione) e condizionare pesantemente le applicazioni crittografiche attualmente in uso [4].

La crittografia odierna utilizza in larga parte i sistemi a chiave asimmetrica, in cui una coppia di chiavi permette di cifrare e decifrare un messaggio potendo utilizzare per ciascuna operazione una sola delle due chiavi. In sostanza, nell'ambito di un colloquio tra due soggetti A e B, il criterio di cifratura asimmetrica stabilisce che un messaggio cifrato da B con la chiave pubblica di A e destinato ad A medesimo possa essere decifrato solo e soltanto da A, in quanto

¹ In matematica un'ipotesi (o congettura) corrisponde ad un'affermazione che è stata proposta come vera, ma che nessuno è stato in grado di dimostrare o confutare, mentre un teorema corrisponde ad un enunciato che viene dimostrato nell'ambito di una teoria formale.

² In effetti esiste una dichiarazione del matematico Louis De Branges de Bourcia, il quale nel giugno del 2004 ha presentato uno studio in cui asserisce di aver sviluppato la dimostrazione; la sua prova, tuttavia, è ancora al vaglio dei matematici [3].

detentore dell'unica chiave privata che fa coppia con quella pubblica usata da B. Delle due chiavi quella detta "pubblica" corrisponde ad un numero intero N risultante dal prodotto di due numeri primi p e q costituiti ciascuno da centinaia di cifre e mantenuti segreti³ [5][6]; la chiave privata viene calcolata a partire da N , attraverso un procedimento basato su complesse funzioni matematiche [7].

Questo sistema crittografico, per rendere sicura una comunicazione, fa affidamento sul fatto che la fattorizzazione di N – e quindi la possibilità di risalire a p e q e da questi alla chiave privata – sia calcolabile in tempi estremamente lunghi e al prezzo di un'enorme potenza computazionale. Poiché solo ricavando p e q è possibile decodificare un messaggio cifrato con la chiave N , modificando la chiave (ovvero la scelta di p e q) entro un periodo di tempo inferiore a quello necessario alla scomposizione di N , si garantisce l'impossibilità di risalire al contenuto in chiaro della comunicazione. In questa maniera, la chiave N può essere liberamente distribuita: la sua conoscenza non pregiudica la sicurezza dell'informazione scambiata.

E' sulla base di questo criterio che vengono protette oggi le transazioni su Internet e che i governi delle maggiori potenze mondiali scelgono le chiavi crittografiche per salvaguardare la riservatezza delle proprie comunicazioni sulla rete.

L'eventuale conoscenza della distribuzione $\zeta(s)$ permetterebbe di facilitare la fattorizzazione delle chiavi pubbliche, rendendo vana la protezione offerta dai cifrari basati su questo principio e obbligando la comunità Internet all'adozione di altre tecniche di sicurezza telematica. Forse, con un po' di presunzione, dopo questa disamina potremmo correggere la citazione di Schneier in: **security is about mathematics and people**. E forse proprio per timore della dimostrazione della congettura di Riemann sono allo studio nuovi sistemi crittografici come quelli basati sulle curve ellittiche [8] o sulla meccanica quantistica [9 – parte III].

Nonostante lo sviluppo di computer sempre più potenti in grado di contare gli zeri della funzione $\zeta(s)$ e verificare empiricamente la validità della congettura, e nonostante l'identificazione di promettenti analogie con la fisica come ad esempio quella tra gli zeri stessi della funzione $\zeta(s)$ e il caos quantistico – che tenta di accertare l'esistenza di un modello "fisico reale" della congettura – comunque, l'ipotesi di Riemann non è ancora stata dimostrata. La tranquillità del nostro quotidiano operare su Internet, per il momento, non è ancora stata minata.

C'è però una strada ancora poco battuta che potrebbe rivelare concezioni totalmente nuove: l'avvicinamento della matematica alla biologia e alla prospettiva naturalistica. Del resto Riemann è un contemporaneo di Darwin ...

Bibliografia

- [1] http://it.wikipedia.org/wiki/Ipotesi_di_Riemann
- [2] <http://www.liceofoscarini.it/studenti/crittografia/mate/zetariemann.html>
- [3] http://ulisse.sissa.it/s7_18giu04_5.jsp
- [4] M. Du Sautoy, L'enigma dei numeri primi, ed. Rizzoli
- [5] La storia della crittografia: ieri, oggi, domani – 1a parte – ICT Security nr. 39, nov. 2005
- [6] La storia della crittografia: ieri, oggi, domani – 2a parte – ICT Security nr. 40, dic. 2005
- [7] http://www.matematicamente.it/approfondimenti/cifratura_RSA.htm
- [8] http://www.certicom.com/index.php?action=ecc.about_ecc
- [9] http://www.clusit.it/download/Q01_web.pdf
- [10] B. Schneier, Applied Cryptography, 2a ed.
- [11] <ftp://ftp.rsasecurity.com/pub/pdfs/bulletn10.pdf>

Sonia Valerio – CISSP, OPSS, GCFW

Information Security Sr. Manager
 Uniautomation S.p.A.
svalerio@uniautomation.it

³ E' abitudine distruggere i numeri p e q in questione dopo aver generato N .