CRITTOGRAFIA E BANCOMAT

a cura del prof. **Alberto Colorni,** docente di Ricerca Operativa al Politecnico di Milano

Nello spettacolo viene citata una operazione inversa (la ricerca dei fattori primi di un numero), operazione che può essere lunghissima.

- Se il numero è il prodotto di due numeri primi bisogna trovare proprio quei due numeri !
- Su questo principio si basa il Bancomat, questo lo vedremo tra poco …

Chiavi condivise e chiavi asimmetriche

- Fino a pochi anni fa il principio-base della crittografia era che chi cifra/trasmette (T) e chi riceve/decifra (R) avessero in comune una "chiave", più o meno complicata ma nota a entrambi: cioè una chiave condivisa.
- Per esempio, secondo Cesare: T (colui che trasmette) sposta ogni lettera dell'alfabeto di 3 posizioni in avanti, mentre R (colui che riceve) la sposta di 3 posizioni indietro.
- Oppure si costruiscono 2 macchine a dischi rotanti, le cui posizioni vengono cambiate ogni giorno in base a un "supercodice" condiviso (era la macchina Enigma).
- Ora passiamo agli anni Settanta e cambiamo radicalmente punto di vista: usiamo una chiave per cifrare, che è pubblica (cioè nota a tutti, potrebbe essere scritta anche sui giornali), e una per decifrare, nota solo a R.
- Coloro che trasmettono possono anche essere tanti (T1, T2, …), perché tutti conoscono la chiave pubblica. E' come se R dicesse: mandatemi i messaggi scritti sui pezzi di un puzzle fatto da voi, nell'ordine che più vi piace; io ho il modo di ricostruire facilmente (attenzione, questo è importante) tutti i puzzles.

Una scoperta interessante

Finalmente, negli anni Settanta, Diffie e Hellmann fanno una scoperta interessante …

- Alice vuole mandare un messaggio segreto a Bob. Chiude il messaggio in una valigetta, chiude la valigetta con un lucchetto e si tiene la chiave; poi spedisce la valigetta a Bob.
- Bob la riceve e applica alla valigia un altro lucchetto, di cui tiene la chiave, la rispedisce ad Alice.
- Alice riceve la valigetta, apre il suo lucchetto con la sua chiave, si mette tutto in tasca e la rispedisce a Bob il quale ovviamente, essendo in possesso della chiave del lucchetto può aprirla.
- L'idea è che Alice o chiunque altro può mettere il suo lucchetto alla valigetta di Bob (cifrando così il proprio messaggio); ma è poi solo Bob che, togliendo l'ultimo lucchetto (la sua chiave privata), apre davvero la valigetta.

L' RSA

Torniamo ora ai nostri numeri primi. Il procedimento delle chiavi asimmetriche della "nuova" crittografia si basa sulla conoscenza di 4 numeri – che sono tutti numeri primi – e su qualche passaggio. Prima di spiegare il metodo (che si chiama RSA, dalle iniziali dei suoi 3 inventori), ci servono un paio di informazioni preliminari.

- La prima → le operazioni "modulo h".
- La seconda → i fattori comuni tra 2 numeri.

Le operazioni "modulo h"

- Due numeri, alfa e beta, si dicono "congruenti modulo h" se divisi per h danno lo stesso resto. La cosa si scrive come vedete e si legge "alfa è congruente a beta modulo h".
- Per esempio, 5 = 29 (mod 2): infatti 5 e 29 divisi per 2 danno lo stesso resto (resto 1, sono entrambi dispari).
- Allo stesso modo, 14 = 20 (mod 2) perchè divisi per 2 danno resto 0 (sono entrambi pari).
- Ancora: 50 = 8 (mod 7), perché divisi per 7 danno entrambi resto 1. Insomma, conta solo il resto.
- Provate voi: 16 = 31 (mod ?); 12 = ? (mod11)
- Anche le lancette dell'orologio funzionano "in modulo 12" (le 3 e le 15 sono nella stessa posizione, che è il resto della divisione per 12: infatti 3:12=0 con resto di 3; 15:12=1 con resto di 3.
- Perché sono importanti le operazioni "mod h" ? Perché con questo modo di operare contano solo i resti, l'informazione è tutta lì.
- Per esempio, se voglio sapere quanto vale 5 x 13 (mod 3), posso ottenerlo [molto più semplicemente] facendo così: 5 (mod 3) x 13 (mod 3), quindi 2 x 1 = 2. E infatti 65 è congruente a 2 (mod 3).
- Quando digitate al Bancomat il vostro codice di 5 cifre, l'operazione è basata sulla congruenza modulo h (state fornendo solo il resto di una divisione).

I fattori comuni tra due numeri

- Questo è facile: due numeri, alfa e beta, hanno r come fattore comune se r è un divisore di entrambi.
- Per esempio, 54 e 168 hanno 6 come fattore comune. Ancora una volta, però, ci interessano i fattori comuni che siano numeri primi. Quindi non conta tanto dire che un divisore comune è 6, è meglio dire che sono 2 e 3.
- Se il numero è molto grande, trovare i suoi fattori è un'impresa proibitiva.
- A questo punto siamo pronti per le chiavi asimmetriche.

Come funziona l'RSA

- Bob, che vuole ricevere i messaggi e decifrarli (è R). Sceglie 2 numeri primi p e q [molto grandi, anche se per il nostro esempio li prendiamo piccoli] → p = 3, q = 7. Bob li moltiplica tra loro ottenendo un numero N: nel nostro caso N = 21 (attenzione: i fattori primi di N sono solo p e q).
- Bob sceglie poi un altro numero e; per ragioni "tecniche" (è il teorema di Eulero-Fermat) questo numero non deve avere fattori comuni con (p-1) e(q-1), quindi Bob sceglie ancora un numero primo). Supponiamo che scelga e = 5. A questo punto Bob può rendere nota la coppia (N, e), che è la sua chiave pubblica: per noi la chiave pubblica è (21, 5).
- Alice vuole cifrare un messaggio per Bob, diciamo un numero M (nei moderni PC tutti i caratteri corrispondono a un codice numerico, quindi possiamo considerare M un numero): M = 11.
- Per cifrarlo Alice usa la chiave pubblica: calcola il valore C = M^e (mod N) → C = 11^5 (mod 21) = 2. Infatti 161.051 (mod 21) = 2, che è il resto. Alice trasmette solo il valore del resto, cioè 2. Nessuno è in grado di risalire da 2, che è il resto, a 161.051 (né tantomeno da lì a 11, che è il messaggio originale).
- Bob riceve 2 e deve essere in grado di decifrare (facilmente) il messaggio. Per farlo gli serve un ultimo numero d, la sua chiave privata, che Bob ricava risolvendo una semplice equazione di primo grado, in cui sono noti p, q, e: e*d = 1 (mod (p-1)*(q-1)). Nel nostro esempio 5d = 1 (mod 2x6) → d = 5.
- Nessun altro (che non conosca p e q) sa risolvere l'equazione che determina d. La spia, infatti, conosce N (prodotto p*q) ma dovrebbe provare a cercarne i fattori primi per tentativi, finché non trova proprio p e q.
- Bob decifra il messaggio con l'operazione M = C^d (mod N) → M = 2^5 (mod 21) = 32 (mod 21) = 11. La sua chiave privata (d) gli ha consentito di decifrare il messaggio con un semplice elevamento a potenza e un'operazione di modulo.

I punti base

- Riassumendo, numeri primi sono alla base del sistema più evoluto di cifratura, quello basato sulle chiavi asimmetriche.
- Quando prelevate i soldi al Bancomat, fate viaggiare solo il resto di una divisione "di modulo N". Ciò corrisponde a spedire alla banca sempre un solo messaggio, del tipo: "sono proprio io che ordino l'operazione che segue" (prelievo, pagamento, ecc.). La banca lo decifra e, se riconosce che siete voi, opera come è stato ordinato.

Alberto Colorni

Professore ordinario di Ricerca Operativa, lavora al Politecnico dove è presidente del *Centro METID* (Metodi E Tecnologie Innovative per la Didattica), responsabile del Corso di laurea in Ingegneria Informatica on line, delegato del Rettore per le attività di e-learning, direttore scientifico del *Consorzio Poliedra*, membro di alcune commissioni di Ateneo. E' presidente della *Società Italiana di e-Learning* (SIe-L), l'associazione scientifica nazionale che si occupa di formazione on line. E' inoltre consulente del *MiUR* (Ministero dell'Università e della Ricerca), del *CNIPA* (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), membro del gruppo di lavoro e-learning della *CRUI* (Conferenza dei Rettori delle Università Italiane).

Le sue *attività di ricerca* hanno coperto aree molto diverse, dalla modellistica matematica dei processi decisionali alle applicazioni informatiche nei settori dell'ambiente e del territorio, dall'e–learning all'uso della multimedialità. All'inizio degli anni 90 ha dato l'avvio, con due altri colleghi, allo studio dei sistemi di ottimizzazione basati sui sistemi naturali, con una serie di lavori sull'ACO (Ant Colony Optimization). Ha pubblicato circa 200 lavori scientifici e didattici. Ha partecipato e coordinato numerosi progetti di ricerca nazionali ed europei nel settore dei trasporti e dell'e-learning. E' editor di *4OR*, la rivista europea di Ricerca Operativa, nonché membro del Comitato scientifico delle riviste *Journal of E-learning and Knowledge Society* (Je-LKS) e *E-Learning & Knowledge Management*. Nel 1989 ha vinto il *Premio Philip Morris* per la Ricerca Scientifica con il progetto del primo servizio italiano di trasporto a chiamata (il sistema Prontobus). Nel 1999 è stato finalista di *Europrix Multimedia Art* con il progetto di un gioco di ruolo territoriale e del *Prix Moebius* (sezione lingua italiana) con un CD–rom didattico sulla Ricerca Operativa. Nel 2001, come direttore METID, ha vinto il *Premio Cenacolo* in Editoria e Innovazione.

Tra il 1995 e il 2002 è stato presidente del Comitato scientifico di *MeglioMilano*, un'associazione per il miglioramento della qualità della vita a Milano.