Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Luigia Berardi, Albrecht Beutelspacher

Crittografia a chiave pubblica: la matematica pura applicata al mondo reale

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **6-A**—*La Matematica nella Società e nella Cultura* (2003), n.3, p. 509–519.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2003_8_6A_3_509_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2003.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. VI-A, Dicembre 2003, 509-519

Crittografia a chiave pubblica: la matematica pura applicata al mondo reale.

Luigia Berardi - Albrecht Beutelspacher

Lo scopo della crittografia classica è quello di trasmettere messaggi riservati attraverso canali pubblici. Il mezzo usato sono i cifrari, che prevedono un segreto comune al mittente ed al destinatario del messaggio; tale segreto è la **chiave** del cifrario. La chiave viene usata dal mittente per cifrare il messaggio e dal destinatario per decifrare il testo segreto. In altre parole, la chiave è la difesa della comunicazione degli interessati verso il resto del mondo.

Poiché è richiesto un segreto comune, esso deve essere comunicato dal mittente al destinatario, o da un ente preposto ad entrambi. È chiaro che sorgono problemi organizzativi enormi, che costituiscono il tallone di Achille della crittografia classica.

Questi problemi si ingigantiscono se le persone che vogliono comunicare tra loro in modo segreto sono molte; infatti ogni coppia di persone deve avere una chiave segreta e quindi, se le persone sono n, ognuno deve memorizzare $n-1$ chiavi segrete. Inoltre, se nel gruppo entra una nuova persona, per ognuno dei partecipanti deve essere scelta, trasmessa e memorizzata una nuova chiave. È chiaro che questi metodi non sarebbero in grado di permettere una trasmissione segreta tra i partecipanti al sistema internet!

Per fortuna la matematica fornisce una soluzione di questo problema, data dalla *crittografia a chiave pubblica*.

L'idea della crittografia a chiave pubblica.

Nel 1976 due giovani ricercatori americani, Whitfield Diffie e Martin Hellman pubblicano un lavoro rivoluzionario, *New directions in cryptography*. In questo articolo introducono l'idea della

crittografia a chiave pubblica. È molto interessante il fatto che loro non presentano un algoritmo concreto a chiave pubblica, bensì il principio generale che soggiace alla crittografia a chiave pubblica, principio che apre una strada del tutto nuova.

L'idea su cui è basata la crittografia a chiave pubblica è quella di fornire due chiavi ad ogni partecipante, qualunque sia il loro numero. Una delle due chiavi è detta **chiave pubblica** e l'altra **chiave privata** (o **segreta**). Così un partecipante P ha la chiave pubblica $E = E_P$ e la chiave privata $D = D_P$. Le due chiavi di P non sono scelte casualmente, ma in modo che verifichino le seguenti proprietà fondamentali.

Proprietà della chiave pubblica.

Non deve essere possibile ricavare la chiave privata D_P dalla chiave pubblica E_P.

«Non possibile» non vuol dire che non sia possibile da un punto di vista teorico, ma che non è possibile praticamente, in tempi accettabili, usando tutti i mezzi esistenti al momento.

Se è verificata questa proprietà, si può pubblicare la chiave pubblica senza pericolo che possa essere trovata la chiave privata.

Proprietà del decifrare correttamente.

Applicando ad un testo m prima la chiave pubblica E_P e poi quella privata D_P, si ottiene m. In altre parole, se $E_P(m) = c$, allora $D_P(c) = m$, ovvero

$$D_P(E_P(m)) = m \quad \text{per ogni } m\,.$$

Un sistema che soddisfa alle due proprietà dette si chiama **sistema di cifratura a chiave pubblica**.

Nella crittografia a chiave pubblica non si usa la stessa chiave per cifrare e decifrare, ma per cifrare si usa la chiave pubblica e per decifrare la chiave segreta corrispondente.

Se una persona vuole inviare ad un utente P un messaggio m in modo segreto, procede nel modo seguente.

- Trova la chiave pubblica E_P di P, ad esempio in un elenco contenente tutte le chiavi pubbliche, oppure la chiave pubblica gli viene trasmessa da P.

- Applica E_P al messaggio m ed ottiene il testo segreto $c = E_P(m)$. Fare questa operazione vuol dire **cifrare**.

- Invia c al destinatario P.

- P applica al testo cifrato c la sua chiave privata D_P ed ottiene $D_P(c) = m$.

Osservazioni.

1. Per cifrare e decifrare vengono usate solo le chiavi del destinatario P. Di conseguenza, anche persone che non fanno parte del sistema possono inviare a P un messaggio in modo segreto.
2. Poiché solo P conosce D_P, cioè la chiave privata corrispondente ad E_P, solo P può decifrare il messaggio c.
3. Per rompere il sistema, un attaccante dovrebbe ricavare D_P da E_P, ma la proprietà della chiave pubblica garantisce che ciò non è possibile.

Per illustrare il meccanismo della crittografia a chiave pubblica sono utili esempi della vita quotidiana, come quello delle cassette delle lettere o della chiusura delle valigie, che si possono trovare in [1], nelle pagine 110 e 137-138.

La crittografia a chiave pubblica non fornisce solo un sistema di cifratura a chiave pubblica, ma offre la possibilità di avere anche un **sistema di firma elettronica**, che è un mezzo fantastico per sostituire la firma autografa.

Un sistema a chiave pubblica dà un sistema di firma elettronica se oltre alla proprietà della chiave pubblica già detta, soddisfa anche alla seguente

Proprietà della firma elettronica.

Applicando ad un testo m prima la chiave D_P e poi la chiave pubblica E_P, si ottiene m. In altre parole se $D_P(m) = f$, allora

$E_P(f) = m$, ovvero

$$E_P(D_P(m)) = m \quad \text{per ogni } m\,.$$

Se P vuole apporre la sua firma elettronica ad un messaggio m, procede come segue.

- Usa la sua chiave privata D_P e calcola la sua firma elettronica $f = D_P(m)$.
- Invia la coppia (m, f).

Ognuno può verificare se f è autentica, applicando ad f la chiave pubblica di P, cioè verificando se $E_P(f) = m$.

Osservazioni.

1. Cifrare e firmare elettronicamente sono procedimenti «duali», nel senso che, mentre per cifrare un messaggio viene usata la chiave pubblica del destinatario, per firmare viene usata la chiave privata del firmatario.
2. Un vantaggio della firma elettronica rispetto alla firma autografa è dovuto al fatto che la firma autografa è statica, mentre la firma elettronica è funzione del messaggio. Di conseguenza viene scoperto il cambio anche di un solo bit nel messaggio.
3. Per spedire un messaggio firmato, si invia la coppia (m, f). Se si procede in modo ingenuo, f ha la stessa lunghezza di m e quindi complessivamente la lunghezza dei dati da trasmettere si raddoppia. Per evitare ciò, si usa una funzione pubblica hash h, che comprime un messaggio di lunghezza arbitraria in dati di lunghezza prefissata, ad esempio 160 bits, così ad un qualsiasi m viene associato un $h(m)$ di lunghezza fissa. Per firmare m si firma solo $h(m)$, ottenendo la firma $f^* = D_P(h(m))$. Per verificare la firma si calcolano $h(m)$, $E_P(f^*)$ e si confrontano.

Un problema esistente nella crittografia a chiave pubblica è quello della autenticità della chiave pubblica, la risposta a questo problema si può trovare ad esempio in [2].

In anni recenti sono stati pubblicati documenti comprovanti che l'idea della crittografia a chiave pubblica è nata nel Quartier genera-

le governativo delle comunicazioni di Cheltenham, ad opera, principalmente, di James Ellis e Clifford Cocks. Le idee di Ellis hanno preceduto di diversi anni quelle di Diffie ed Hellman, ad esse simili. Inoltre Cocks aveva messo a punto ben quattro anni prima l'algoritmo che sarebbe passato alla storia col nome RSA. Tutte queste scoperte erano rimaste segrete per la natura del centro di ricerca (cfr. [4], pp. 287-301).

Il prototipo degli algoritmi a chiave pubblica: l'RSA.

Il primo algoritmo a chiave pubblica fu inventato nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman e fu chiamato RSA dalle iniziali dei loro nomi.

Mentre il funzionamento dell'RSA poggia su un teorema di Eulero, la sua sicurezza dipende dalla difficoltà di scomporre un numero molto grande in fattori primi.

Per un naturale n si definisce **indicatore di Eulero** $\varphi(n)$ il numero dei numeri naturali minori o uguali ad n e primi con n.

Ad esempio $\varphi(11) = 10$, $\varphi(15) = 8$. Infatti è facile vedere che $\varphi(p) = p - 1$, per ogni primo p e che $\varphi(pq) = (p-1)(q-1)$, se p e q sono due primi distinti.

Ora enunciamo un teorema di Eulero in un caso speciale, che è quello interessante per l'algoritmo RSA.

TEOREMA DI EULERO. – Siano p e q due primi distinti ed $n = pq$. Allora per ogni intero $m < n$ si ha che

$$m^{\varphi(n)+1} = m \,(\mathrm{mod}\ n)\,.$$

Più in generale, per ogni numero naturale k si ha che

$$(*) \qquad m^{k\varphi(n)+1} = m \,(\mathrm{mod}\ n)\,.$$

L'idea dell'RSA consiste nell'interpretare m come un messaggio e nel dividere l'elevamento a potenza di m, che compare in $(*)$, in due parti, una delle quali dà la cifratura di m e l'altra la decifrazione.

Ora descriviamo la generazione delle chiavi di un partecipante P.

Generazione delle chiavi.

Vengono scelti due numeri primi distinti p e q. Si calcola $n = pq$ e $\varphi(n) = (p-1)(q-1)$. Si sceglie poi un numero e, minore di $\varphi(n)$ e primo con $\varphi(n)$. Si calcola il numero d, tale che $ed = 1 \pmod{\varphi(n)}$, cioè $ed = k\varphi(n) + 1$. Questo calcolo si può eseguire usando l'algoritmo di Euclide.

I numeri e ed n costituiscono la chiave pubblica di P, mentre il numero d è la chiave privata di P.

Osserviamo che conoscendo $\varphi(n)$ oppure p oppure q, è facile determinare la chiave privata d, quindi è indispensabile che non siano noti questi numeri.

Uso dell'RSA.

Per inviare a P un messaggio in modo riservato, si fanno le seguenti operazioni.

1) Si codifica il messaggio in un messaggio numerico $m < n$; se non è sufficiente un numero, vengono usati più numeri.

2) Si trova la chiave pubblica e, n di P.

3) Si computa

$$c = m^e \pmod{n}$$

e si invia c a P.

1) Quando P riceve c, computa $c^d \bmod n$. Per il teorema di Eulero enunciato segue che P ottiene proprio m. Infatti si ha

$$c^d \pmod{n} = (m^e)^d \pmod{n} = m^{k(n)+1} \pmod{n} = m\,.$$

Sicurezza.

L'RSA è sicuro se non è possibile ricavare d, conoscendo e ed n, cioè se è verificata la proprietà della chiave pubblica.

È chiaro che, conoscendo $\varphi(n)$, si può calcolare d senza problemi. Inoltre conoscere $\varphi(n)$ è equivalente a conoscere i fattori p e q. Infatti si avrebbero le equazioni

$$pq = n \quad \text{e} \quad (p-1)(q-1) = \varphi(n)$$

nelle incognite p e q; dalle quali verrebbero determinate p e q.

Quindi perché l'RSA sia sicuro si devono scegliere i numeri p e q in modo che n non possa essere fattorizzato, più in particolare p e q devono essere numeri primi molto grandi, nella pratica devono avere un ordine di grandezza di 512 bits, quindi n ha 1024 bits.

Il record mondiale della lunghezza di un numero, prodotto di due primi, che è stato scomposto nei suoi fattori primi, è 512 bits.

È un problema trovare numeri primi di 512 bits, cioè di 154 cifre decimali? Anche qui la matematica può aiutare. Infatti il teorema fondamentale dei numeri primi dice che il numero $\pi(x)$ dei numeri primi aventi l'ordine di grandezza di x è circa $x/(\ln x)$.

Segue che il numero dei numeri primi di 512 bits è circa $2{,}8169 \cdot 10^{151}$.

Nella realtà si procede come segue.

- Si sceglie un numero casuale di 512 bits.
- Si sottopone a test di primalità. Se è un numero primo, va bene, altrimenti si prende il dispari successivo ad esso e si ripete il procedimento.

Osserviamo che i test di primalità sono molto efficienti (cfr. par. 4.2 di [3]).

Algoritmi basati sul logaritmo discreto.

Il problema fondamentale della crittografia a chiave pubblica è quello di trovare problemi matematici sui quali si possano basare sistemi a chiave pubblica.

Oltre alla fattorizzazione dei numeri naturali, c'è il problema del logaritmo discreto, che permette di costruire vari algoritmi a chiave pubblica.

Descriviamo il problema del logaritmo discreto. Sia dato un numero primo p ed un numero $g < p$. È molto facile calcolare tutte le potenze di g; d'altro canto, dato un numero $h < p$, è difficile decidere se h è una potenza di g modulo p e, se lo è, determinare un a tale che $h = g^a \bmod p$. Determinare a va sotto il nome del **problema del logaritmo discreto**. L'ordine di grandezza dei numeri p usati nella pratica è di 1024 bits.

Osserviamo che fissare p primo vuol dire che la struttura algebrica fissata è il gruppo moltiplicativo $\boldsymbol{Z}_p^*$. È ovvio che possiamo formulare il problema del logaritmo discreto in un qualsiasi gruppo.

Questa banale osservazione comporta un'importante conseguenza, precisamente l'uso delle curve ellittiche (vedere il seguito).

Già nel primo lavoro di Diffie ed Hellman sulla crittografia a chiave pubblica è presentato un protocollo basato sul problema del logaritmo discreto. Esso non è un algoritmo a chiave pubblica in senso stretto, ma risolve il problema fondamentale della crittografia classica, lo scambio delle chiavi.

Chiamiamo A e B due persone che hanno bisogno di una chiave segreta comune da usare in un algoritmo di cifratura classico. Supponiamo che siano stati già fissati un numero primo p, tale che sia difficile calcolare il logaritmo discreto modulo p ed un numero naturale $g < p$. Gli utenti A e B procedono come segue.

1) A sceglie e tiene segreto un numero naturale a, analogamente B sceglie b.

2) A calcola $\alpha = g^a \pmod p$ e B calcola $\beta = g^b \pmod p$.

3) A invia α a B e B invia β ad A.

Osserviamo che nessun attaccante può calcolare a o b conoscendo α o β, infatti vorrebbe dire risolvere il problema del logaritmo discreto.

4) A calcola β^ae B calcola α^b. Si ha che

$$\beta^a = (g^b)^a \pmod p = (g^a)^b \pmod p = \alpha^\beta \pmod p,$$

quindi A e B hanno un segreto comune.

Nel 1985 ElGamal ha usato il problema del logaritmo discreto per costruire sia un sistema a chiave pubblica che un sistema di firma elettronica.

Descriviamo solo lo schema della cifratura. Sono fissati un primo p ed un naturale g, comuni a tutti i partecipanti. Un utente B ha come chiave segreta un intero b e come chiave pubblica il numero $\beta = g^b \pmod p$. Se A vuole mandare a B un messaggio m in modo segreto, sceglie un numero a, poi calcola il numero $g^a \pmod p$; usando la chiave pubblica di B, computa anche il numero $k = \beta^a \pmod p$, che sarà usato come chiave per cifrare il messaggio m. A usa un algoritmo simmetrico f per ottenere il testo cifrato $c = f_k(m)$ e poi invia a B due dati: il numero $g^a \pmod p$ ed il testo cifrato c.

Usando la sua chiave segreta b, B può computare da $g^a \pmod p$ la chiave $k = (g^a)^b \pmod p$ e quindi può decifrare c.

Il sistema di firma elettronica di ElGamal, basato sul logaritmo discreto, è molto complicato e del tutto dissimile dal sistema di cifratura descritto; è possibile trovare la sua descrizione in [3], paragrafo 11.5.2.

Il sistema di firma elettronica detto è più generale di quelli descritti, infatti la verifica della firma non consiste nel ritrovare da essa il messaggio.

Crittografia e curve ellittiche.

È stupefacente che le curve ellittiche, che costituiscono una pietra miliare della matematica del novecento, siano usate per costruire crittosistemi molto efficienti.

Una curva ellittica è una cubica piana, non singolare. Se la caratteristica del campo è diversa da 2, 3, ogni curva ellittica C si può rappresentare nella forma canonica $y^2 = x^3 + ax + b$, dove $4a^3 + 27b^2 \neq 0$.

Data una curva ellittica C in forma standard si può definire una addizione che associa ad ogni coppia di punti di C un altro punto di C nel modo seguente.

Siano P e Q due punti distinti di C. Dal teorema di Bezout segue che la retta per P e Q interseca C in un altro punto R. Il simmetrico di R rispetto all'asse x è ancora un punto di C, che viene definito come $P + Q$.

In modo simile si definisce $P + P$: la tangente in P a C interseca C in un altro punto S. Il simmetrico di S rispetto all'asse x è $P + P$.

Si può dimostrare che l'insieme dei punti della curva C con il punto all'infinito della curva stessa, strutturato con l'operazione di addizione appena definita, è un gruppo, che ha come elemento neutro il punto all'infinito.

L'operazione definita geometricamente si può tradurre algebricamente, facendo uso delle coordinate. Ciò ci permette di definire l'operazione di addizione anche se la curva C è definita in un campo qualsiasi, in particolare nei campi finiti, che giocano un ruolo fondamentale nell'ambito della crittografia.

È possibile parlare di logaritmo discreto anche se il gruppo è quello di una curva ellittica su un campo finito; di conseguenza possiamo generalizzare tutti gli algoritmi crittografici basati sul logaritmo discreto modulo p considerando «gruppi ellittici».

Il vantaggio principale che si ottiene usando gruppi ellittici, è il seguente. Ad oggi esistono algoritmi che permettono di risolvere il problema del logaritmo discreto su $\mathbf{Z}_p$.

Per calcolare il logaritmo discreto in un gruppo qualsiasi G ci sono alcuni algoritmi, ad esempio il baby-step giant-step algorithm, che ha una complessità dell'ordine $\sqrt{|G|}$. Ci sono algoritmi speciali per computare il logaritmo discreto nel gruppo $\boldsymbol{Z}_p$, ad esempio l'index-calculus algorithm (cfr. [3], 3.68). Questo algoritmo è leggermente migliore degli algoritmi generali, ma funziona solo in $\boldsymbol{Z}_p$. Di conseguenza, per ottenere la stessa sicurezza, si devono prendere gruppi $\boldsymbol{Z}_p$ con p più grande. La sicurezza che si ottiene in $\boldsymbol{Z}_p$, se p ha 1024 bits, si può ottenere con curve ellittiche su un campo avente l'ordine di 160 bits.

Questo mostra che le curve ellittiche sono una cosa molto pratica.

BIBLIOGRAFIA

[1] L. BERARDI - A. BEUTELSPACHER, *Crittologia*, FrancoAngeli, Milano, (1996).

[2] L. BERARDI - A. BEUTELSPACHER, *Come rendere sicura la posta elettronica*, Archimede, **3** (1999), 1-7.

[3] A. J. MENEZES - P. C. VAN OORSCHOT - S. A. VANSTONE, *Handbook of applied Cryptography*, CRC Press (1997).

[4] S. SINGH, *Codici & Segreti*, Rizzoli (1999).

[5] I. BLAKE - G. SEROUSSI - N. SMART, *Elliptic Curves in Cryptography*, Cambridge University Press (1999).

L. Berardi, Dipartimento di Ingegneria Elettrica
I-67040 Monteluco di Roio (L'Aquila). E-mail: berardi@ing.univaq.it

A. Beutelspacher, Mathematisches Institut, Justus-Liebig-Universitat
Arndtstr. 2 D-35392 Giessen. E-mail: albrecht.beutelspacher@math.uni-giessen.de