Aspetti matematici e crittologici della firma elettronica.

La crittografia a chiave pubblica è il fondamento della firma elettronica, firma che ci consente di attribuire ad una specifica persona il documento così contrassegnato. La tecnica di crittografia pubblica o asimmetrica che trattiamo in questo breve escursus è l'RSA [dal nome dei suoi inventori: Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman]. Vediamone i dettagli tecnici.
Gli attori di questa finzione sono Alice, che vuole comunicare riservatamente con Bob, Eva che invece vuole proditoriamente spiare tale comunicazione. Alice sceglie due numeri primi, normalmente enormi, p e q, ma nel nostro caso, per semplificare i calcoli si abbiano p = 13 e q = 23. Questi due numeri devono assolutamente rimanere segreti. Quindi Alice li moltiplica tra loro (13 · 23) = 299 ottenendo N, poi sceglie un altro numero e [esponente di cifratura] (e = 17) minore di N; e e (p - 1) · (q - 1) devono essere relativamente primi. A questo punto Alice inserisce in un elenco pubblico i suoi numeri N ed e, che costituiscono la sua chiave pubblica, mentre p e q costituiscono la sua chiave privata. Chiunque volesse inviare un messaggio cifrato ad Alice non ha che da consultare l'elenco pubblico, trovare la sua chiave N ed e e cifrare con questa il messaggio che vuole inviarle. Fatto questo, Bob ricorre alla seguente formula di cifratura:

$$\mathbf{C = M^e (mod\ N)}$$

dove C è la cifra calcolata, M il messaggio in chiaro, e ed N la chiave pubblica. mod è l'operatore aritmetico modulo, cioè il resto. [Es.: (7 mod 3) = 1, perché 7 diviso 3 ha per resto 1; (10^2 mod 4) = 0; (39 mod 5) = 4].
Immaginiamo che Bob voglia inviare per computer la lettera S ad Alice. Il computer al posto della S utilizza il numero 83 [che è il codice ASCII di S]. Perciò M = 83. Per cifrare questa lettera Bob cerca la chiave pubblica di Alice e trova N = 299 ed e = 17 e li include nell'espressione: $C = 83^{17} \pmod{299} = 135$. Il messaggio cifrato da inviare ad Alice è 135 e d'ora in avanti esso potrà essere decifrato soltanto con la chiave privata corrispondente a quella pubblica, quindi non è più decifrabile nemmeno da Bob. È da notare che la funzione impiegata è a senso unico: facile da calcolare nella forma diretta, praticamente impossibile ricavarne la funzione inversa. Perciò è estremamente difficile per Eva recuperare S da 135: Eva non può ottenere il messaggio. Lo può invece decifrare Alice poiché solo lei può calcolare l'espressione:

$$\mathbf{M = C^d\ (mod\ N)}$$

dove d [la chiave di decifrazione] deriva da $(e \cdot d) \pmod{(p-1)\cdot(q-1)} = 1$ ed è uguale a 233. d può essere ricavata soltanto da lei perché è la sola a conoscere p e q, i valori necessari a tal scopo. Quindi $M = 135^{233} \pmod{299} = 83 = S$: ecco la ricostruzione del messaggio di Bob. Da notare che Alice e Bob hanno chiavi diverse, asimmetriche e non c'è stato bisogno per loro di scambiarsele, cosa necessaria e rischiosa nella crittografia classica detta anche a chiavi simmetriche. Qui abbiamo cifrato solo una lettera, ma ripetendo n volte tale algoritmo possiamo cifrare e decifrare un qualsiasi messaggio di n caratteri.
Finora Bob ha utilizzato l'algoritmo RSA per cifrare un messaggio utilizzando la chiave pubblica di Alice che lo decifra con la sua chiave privata. Ma che succederebbe se Alice cifrasse il suo messaggio con la sua chiave privata, che solo lei conosce? Questa cifratura è debolissima, infatti chiunque andasse a prendere la chiave pubblica di Alice potrebbe decifrare il suo messaggio. Ed è ciò che avviene. Ma ciò, per converso ha un'interessante proprietà: solo Alice, detentrice esclusiva della sua chiave privata, può aver generato tale documento, che non può essere letto con nessuna altra chiave pubblica. Perciò tale documento, leggibile appunto solo con la sua chiave pubblica, si può attribuire sicuramente ed esclusivamente a lei che lo ha così firmato elettronicamente.

Silvio Coccaro
www.silcosoft.it
ex-allievo sez. D – A. S. 1972/73