Il presente Fascicolo C contiene i seguenti argomenti

1) Crittosistema R.S.A.
2) Schema di scambio di chiavi di Diffie-Hellman. Il problema del logaritmo discreto.

Fascicolo C

Il crittosistema R.S.A.

Si tratta del più famoso crittosistema a chiave pubblica, inventato nel 1978 (vedi Adleman L.M., Rivest R.L., Shamir A. "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21 (1978), 120-126). Naturalmente la sigla R.S.A. è un acronimo dal nome degli autori. Spieghiamo di che cosa si tratta.

Supponiamo che A (Alice) voglia costruire un crittosistema R.S.A.. Deve procedere nel modo seguente:

α) come prima cosa sceglie due primi "grandi", diciamo p, q;

β) calcola poi il prodotto $n = pq$ e la funzione di Eulero $\varphi(n) = \varphi(pq) = (p-1)(q-1)$

γ) sceglie una chiave di cifratura ("encryption key"), indichiamola con e, tale che sia relativamente prima con $\varphi(n)$, cioè

$$(e, \varphi(n)) = 1$$

δ) calcola l'inverso moltiplicativo di e mod $\varphi(n)$, cioè risolve la congruenza

$$(*) \quad eX \equiv 1 \pmod{\varphi(n)}$$

Indichiamo con d la chiave di decifratura ("decryption-key"), dove d è la soluzione della congruenza (*), cioè

$$1) \quad ed \equiv 1 \pmod{\varphi(n)}$$

A questo punto il cryptosistema è pronto: la coppia n, e è pubblica (e deve essere divulgata) mentre d è segreta (con i primi p e q e $\varphi(n)$).

Il cryptosistema funziona nel modo seguente. Supponiamo che B (Bob) voglia mandare un messaggio M ad Alice (naturalmente il messaggio M è un numero: ci sono molti modi standard che trasformano automaticamente un messaggio verbale in un numero naturale). Bob si procura la chiave pubblica di Alice, cioè la coppia n, e e calcola il cifrato C, cioè (si suppone $1 \leq M < n$, altrimenti si spezza M in più messaggi)

$$2) \quad C \equiv M^e \pmod{n}$$

cioè il cifrato è il minimo residuo positivo mod n della e-esima potenza del messaggio. Quando Alice riceve C, per decifrare e quindi recuperare il messaggio M, basta che calcoli mediante la chiave segreta d

$$3)\quad C^d \equiv M \pmod n$$

Giustifichiamo la 3). Per la 1) possiamo dire che

$$4)\quad ed = 1 + k\varphi(n)$$

per un certo $k \in \mathbb{N}$. Ne segue, elevando la 2) membro a membro alla d,

$$5)\quad C^d \equiv M^{ed} \equiv M^{1+k\varphi(n)} \equiv (M^{\varphi(n)})^k \cdot M \pmod n$$

Supponiamo ora $(M,n)=1$. Per il teorema di Eulero - Fermat, si ha

$$6)\quad M^{\varphi(n)} \equiv 1 \pmod n$$

e da 5) e 6) segue

$$7)\quad C^d \equiv 1^k \cdot M \equiv M \pmod n$$

e ciò dimostra la 3).

Si può anche dimostrare che la formula di decifrazione 3) vale anche senza l'ipotesi $(M,n)=1$. Infatti, per $1 \le M < n = pq$, supponiamo che $p \mid M$ e $q \nmid M$. Sempre per il teorema di Eulero - Fermat, si ha $M^{q-1} \equiv 1 \pmod q$ e quindi

$$8)\quad M^{(p-1)(q-1)} = M^{\varphi(n)} \equiv 1 \pmod q$$

Dalla congruenza 5), che vale anche mod q, e dalla 8) segue

$$9) \quad C^d \equiv M \pmod{q}$$

D'altra parte, se $p \mid M$ si ha anche $p \mid C$ per la 2) e quindi

$$10) \quad C^d \equiv M \pmod{p}$$

Da 9) e 10) segue ovviamente

$$11) \quad C^d \equiv M \pmod{pq}$$

cioè la 3). Allo stesso modo si ragiona se $p \nmid m$ ma $q \mid M$. Quindi, come abbiamo detto, la 3) vale sempre.

La sicurezza del crittosistema R.S.A. è basata sulla (presunta) grande difficoltà della fattorizzazione. Infatti $n = pq$ è noto (fa parte della chiave pubblica) ma non lo sono p e q (che devono essere tenuti segreti).

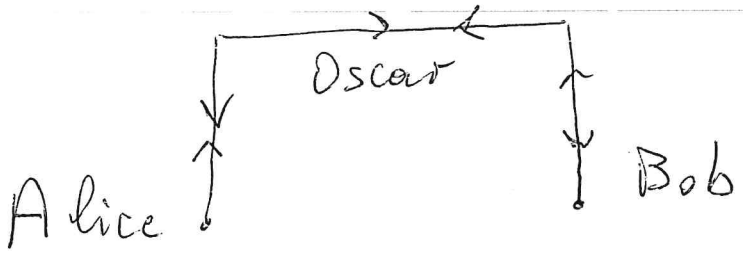
Se p e q sono primi che hanno almeno quattro-cinquecento cifre binarie l'uno non sono noti algoritmi in grado di fattorizzare n in tempi ragionevoli. Lo stesso dicasi per il calcolo di $\varphi(n) = (p-1)(q-1)$, se p e q non sono noti.

Il problema di Diffie - Hellman

Nel 1976 W. Diffie e M.E. Hellman pubblicarono un fondamentale lavoro, precisamente

"New directions in cryptography"
IEEE Transactions on information theory, 22 (1976), 644 - 654.

In questo lavoro proposero il seguente (importante) schema di scambio di chiavi su un canale spiato. Supponiamo che A (Alice) e B (Bob) vogliano scambiarsi una chiave segreta (un numero) su un canale insicuro, spiato da O (Oscar).



Alice e Bob procedono come segue

I) si accordano (su) un numero primo p grande, diciamo con 400 cifre binarie. Questo p può essere reso pubblico.

II) si accordano anche su una radice primitiva $g \bmod p$. Anche g può essere resa nota a tutti.

III) Alice sceglie un numero a (da mantenere segreto) e calcola $g^a \equiv \alpha \pmod p$. Trasmette poi α a Bob. (Si intende che α è il minimo residuo positivo di $g^a \bmod p$)

IV) Bob a sua volta sceglie un numero b (da mantenere segreto) e calcola $g^b \equiv \beta \pmod p$. Trasmette poi β ad Alice (ovviamente β è il minimo residuo positivo di $g^b \bmod p$).

V) Alice, conoscendo β ed a, calcola

$$\beta^a \equiv (g^b)^a \equiv g^{ba} \pmod p$$

e Bob, conoscendo α e b, calcola

$$\alpha^b \equiv (g^a)^b \equiv g^{ab} \pmod p$$

A questo punto Alice e Bob sono entrambi a conoscenza del numero

$$\gamma \equiv g^{ba} = g^{ab} \pmod p$$

(anche qui γ è il minimo residuo positivo di $g^{ab} \bmod p$). Il numero γ costituisce la chiave segreta.

Supponiamo che Oscar abbia ascoltato tutte le comunicazioni. Oscar conosce

$$p,\ g,\ \alpha \equiv g^a \pmod p \text{ e } \beta \equiv g^b \pmod p$$

me non conosce né a, né b. Per calcolare la chiave f, Oscar dovrebbe riuscire a ricavare $g^{ab} \pmod p$ dalla conoscenza di $g^a \pmod p$ e $g^b \pmod p$. Questo è il problema di Diffie-Hellman: non è noto nessun modo per risolverlo in tempi ragionevoli, se p, a, b sono numeri molto grandi (con più di 200 cifre binarie per a e b).

Il problema del logaritmo discreto

Il problema si enuncia molto facilmente:

"Dato un primo p, una radice primitiva $g \bmod p$ e $\alpha \equiv g^a \pmod p$, calcolare a"

Se il primo p è "piccolo" si tratta di un problema banale: basta tentare con

$$a = 1, 2, 3, \ldots, p-1$$

Se p ha più di 400 cifre binarie le cose cambiano. Questo problema è celebre e non è noto nessun metodo per risolverlo in tempi ragionevoli. È chiaro che se si riuscisse a risolvere "velocemente" il problema del logaritmo discreto si riuscirebbe anche a risolvere "velocemente" il problema di Diffie-

Hellman. Infatti Oscar, essendo a conoscenza di $\alpha \equiv g^a \pmod{p}$, potrebbe calcolare rapidamente a e conoscendo anche $\beta \equiv g^b \pmod{p}$, calcolerebbe anche $\beta^a \equiv g^{ba} \equiv \gamma \pmod{p}$, la chiave.

—