SESTO INCONTRO

SISTEMI A CHIAVE PUBBLICA

Finora abbiamo descritto dei metodi di cifratura che fanno uso di una chiave privata, cioè di una informazione grazie alla quale si può sia criptare il messaggio che decifrarlo: tale chiave deve essere necessariamente nota sia al mittente che al destinatario. Mittente e destinatario sono a conoscenza della stessa informazione.

Immaginiamo ora che il destinatario voglia comunicare privatamente con più di una persona, anzi che voglia addirittura che chiunque sia in grado di inviargli messaggi cifrati, mantenendo però la segretezza di ciascuno. Con i sistemi a chiave privata, ciò non sarebbe possibile: il destinatario è in grado di ricevere messaggi solo da persone note, con le quali ha condiviso la chiave.

E' necessario quindi un sistema diverso, un metodo che preveda due informazioni indipendenti: una per cifrare e un'altra per decifrare; l'informazione per cifrare può allora essere resa nota a tutti (e viene chiamata *chiave pubblica*), mentre l'informazione che serve per decifrare (la *chiave privata*) va tenuta rigorosamente segreta: la conosce solo il destinatario e permette a lui soltanto di leggere i messaggi.
L'idea di utilizzare un sistema a doppia chiave è dovuta a Diffie e Hellman. Nel 1976, Diffie e Hellmann mettono le basi per un sistema crittografico in cui **la chiave per cifrare non permetta di ricavare la chiave per decifrare**: in tal modo è possibile (ad esempio per una banca) rendere pubblica la chiave per cifrare, permettendo a tutti di scrivere alla banca stessa in segretezza. Solo la banca è in grado di leggere il contenuto del messaggio, perchè possiede la chiave per decifrare.
La prima realizzazione pratica (per quanto noto) è dovuta a Rivest, Shamir e Adleman del MIT (Massachusetts Institute of Tecnology) e in loro onore prende il nome di *sistema RSA:* è attualmente il sistema più diffuso di crittazione.
I sistemi a chiave privata sono detti anche *simmetrici,* mentre quelli a chiave privata *asimmetrici*, perchè mittente e destinatario hanno, nel secondo caso, ruoli decisamente differenti.

Se B vuole che chiunque sia in grado di scrivergli, ha bisogno di rendere pubbliche tutte le informazioni necessarie per cifrare, facendo in modo che da tali informazioni non sia possibile risalire alle informazioni necessarie per decifrare. Occorre a tal fine che la chiave per decifrare non siano ottenibili (in modo facile) dalla chiave che serve per cifrare.

Ci è permesso, in tal modo, divulgare sia la chiave di cifratura che il metodo, ma senza per questo rivelare contestualmente il modo di decifrare. Il metodo di cifratura deve essere una funzione matematica abbastanza semplice che tutti sono in grado di utilizzare, mentre la funzione di decifratura deve poter essere applicata agevolmente solo da chi è in possesso della "chiave privata". Il tutto è quindi basato su una funzione cifrante, la cui inversa è complessa solo apparentemente e diventa improvvisamente molto semplice non appena la si guarda attraverso l'informazione aggiuntiva (data dalla chiave).

Scopriremo più avanti di quale funzione stiamo parlando e capiremo nelle prossime lezioni quale dato riveste il ruolo della chiave e perché questa informazione sia (almeno ad oggi) indispensabile.

Tuttavia, per quanto la funzione sia semplice concettualmente, la cifratura e la decifratura richiedono conti abbastanza complessi e non molto agevoli da trattare se non si usa il metodo migliore: ci imbatteremo, infatti, nel calcolo di congruenze in cui compaiono potenze con basi ed esponenti elevati.

E' vero che, solitamente, questi conti vengono svolti dai calcolatori (anche perché i numeri coinvolti sono costituiti da tantissime cifre e quindi non sono assolutamente trattabili a mano), ma cerchiamo comunque di capire (usando ovviamente cifre più piccole) come il computer lavora per calcolare queste potenze.

Per realizzare questo metodo useremo le potenze, il teorema di Eulero, la scrittura in blocchi.

RSA

La RSA ha brevettato il sistema crittografico a chiave pubblica attualmente più diffuso. Il metodo è universalmente noto.
La RSA vende chiavi "certificate" che permettono di usarlo in sicurezza. Le chiavi vengono costruite a partire da coppie di numeri primi molto grandi.

Siamo abbastanza capaci di trovare nuovi numeri primi grandi, ma non siamo capaci di fattorizzare in modo efficiente
Tavola 6.1: criteri di divisibilita'

Cifratura

Per usufruire del sistema è necessario procurarsi una chiave pubblica da iscrivere in un elenco di dominio pubblico, al quale potrà attingere chiunque voglia scriverci.
La chiave è costituita da due numeri, che indicheremo con *n* ed *e*, che possiamo scegliere come vogliamo purché *n* sia prodotto di due numeri primi molto grandi *p* e *q* ed *e* sia un qualsiasi numero relativamente primo con *p-1* e *q-1* e diverso da *p* e *q* (le motivazioni di questa richiesta ci saranno chiare in seguito).

Il destinatario, che chiameremo per comodità B, deve pubblicare la sua chiave *(n,e):* l'unica accortezza che B deve avere è di tenere nascosti i primi *p* e *q* che, come vedremo, saranno la sua chiave privata per decifrare.
Chiave pubblica (*n = 21*, *e = 5*),
n è prodotto di due primi p *=3* e *q =7*
(p-1)(q-1)= 2 x 6 = 12: non ha fattori in comune con 5
Chiave pubblica (*n = 21*, *e = 11*),
n è prodotto di due primi p *=3* e *q =7*
(p-1)(q-1)= 2 x 6 = 12: non ha fattori in comune con 11

Vediamo, col supporto di un esempio, come deve procedere il mittente A se vuole inviare un messaggio a B.

ESEMPIO **Chiave pubblica: (1003, 3)**
Chiave privata: ?

Voglio scrivere "vieni qui"
Trascrivo in cifre: 21 08 04 13 08 16 20 08
Divido in blocchi più piccoli di 1003:
210 804 130 816 200 823
(ho aggiunto, in fondo, una x=23)

I blocchi sono:
m_1=210 m_2=804 m_3=130 m_4=816 m_5=200 m_6=823
Cifro ogni blocco, facendone la potenza di indice *e*:

$c_1 = m_1^{\,e}$ modulo *n* cioè $(210)^3$ modulo 1003 : c_1=301

c_2= $(804)^3$ modulo 1003: dunque c_2= 975

c_3= $(130)^3$ modulo 1003: dunque c_3=430

c_4= $(816)^3$ modulo 1003: dunque c_4=357

c_5= $(200)^3$ modulo 1003: dunque c_5= 72

c_6= $(823)^3$ modulo 1003: dunque c_6=445

Decifratura

Il destinatario conosce i fattori *p* e *q* di *n*. Calcola la sua chiave privata, che è il numero d tale che
ed–1 sia divisibile per *(p–1)(q–1)*
cioè
d è l'inverso di *e* mod *(p–1)(q–1).*

ESEMPIO di chiavi:

Chiave pubblica (*n = 21*, *e = 5*),
n è prodotto di due primi p *=3* e *q =7*
(p-1)(q-1)= 2 x 6 = 12: non ha fattori in comune con 5
Chiave privata: cerco un numero *d* tale che 5 *d–1* sia divisibile per *(p-1)(q-1) =12. Ho bisogno che 5 d = 1+ 12 h: osservo che*
5x *5=25 = 1+24= 1+2*x*12: dunque d =5 va bene :* ***ma è uguale alla chiave pubblica.....***

Chiave pubblica (*n = 21*, *e = 17*),
n è prodotto di due primi p *=3* e *q =7*
(p-1)(q-1)= 2 x 6 = 12: non ha fattori in comune con 17
Chiave privata: cerco un numero *d* tale che 17*d–1* sia divisibile per *(p-1)(q-1) =12. Ho bisogno che 17 d = 1+ 12 h: osservo che*
17x*5=85 = 1+84 = 1+7*x*12: dunque d =5 va bene*
[il prodotto *ed* coincide con 1 sull'orologio con 21 ore]
(se siete preoccupati perchè avevamo appena detto che l'inverso di 5 mod 12 è proprio 5, basta osservare che 5 e 17 danno la stessa classe mod 12]

Il destinatario sa che 1003 = 17 x 59 (chiamo *p*= 17, *q*=59) Deve **calcolare la chiave privata *d*** tale che *ed–1* sia divisibile per *(p–1)(q–1)*= 16x 58 = 928. Ricava **d=619**.
Decifra ogni blocco, iniziando dal primo: **la procedura è uguale a quella della cifratura, ma l'esponente da usare è la chiave segreta**

$m_1 = c_1^{\,d}$ modulo *n* cioè $(301)^{619}$ modulo 1003: **m_1=210**

m_2= $(975)^{619}$ modulo 1003: dunque **m_2= 804**

m_3= $(430)^{619}$ modulo 1003: dunque **m_3= 130**

$m_4 = (357)^{619}$ modulo 1003: dunque $\boldsymbol{m_4 = 816}$

$m_5 = (72)^{619}$ modulo 1003: dunque $\boldsymbol{m_5 = 200}$

$m_6 = (445)^{619}$ modulo 1003: dunque $\boldsymbol{m_6 = 823}$

Ma perché questo procedimento ha funzionato? E' facile dimostrarlo sfruttando i risultati che abbiamo imparato sulle congruenze: (prendiamo $m = m_i$)

$$c^d = (m^e)^d = m^{e\,d} \bmod (n)$$

Ma d'altra parte $ed \equiv 1 \bmod (p-1)(q-1)$ e quindi, per definizione di congruenza, $ed - 1$ è un multiplo di $(p-1)(q-1)$, cioè

$$ed = 1 + k\,(p-1)(q-1) \qquad \text{per un certo } k$$

Quindi

$$m^{ed} = m^{1\,+\,k\,(p-1)(q-1)} = m \times m^{\,k\,(p-1)(q-1)} = m \times (m^{\,(p-1)(q-1)})^k$$

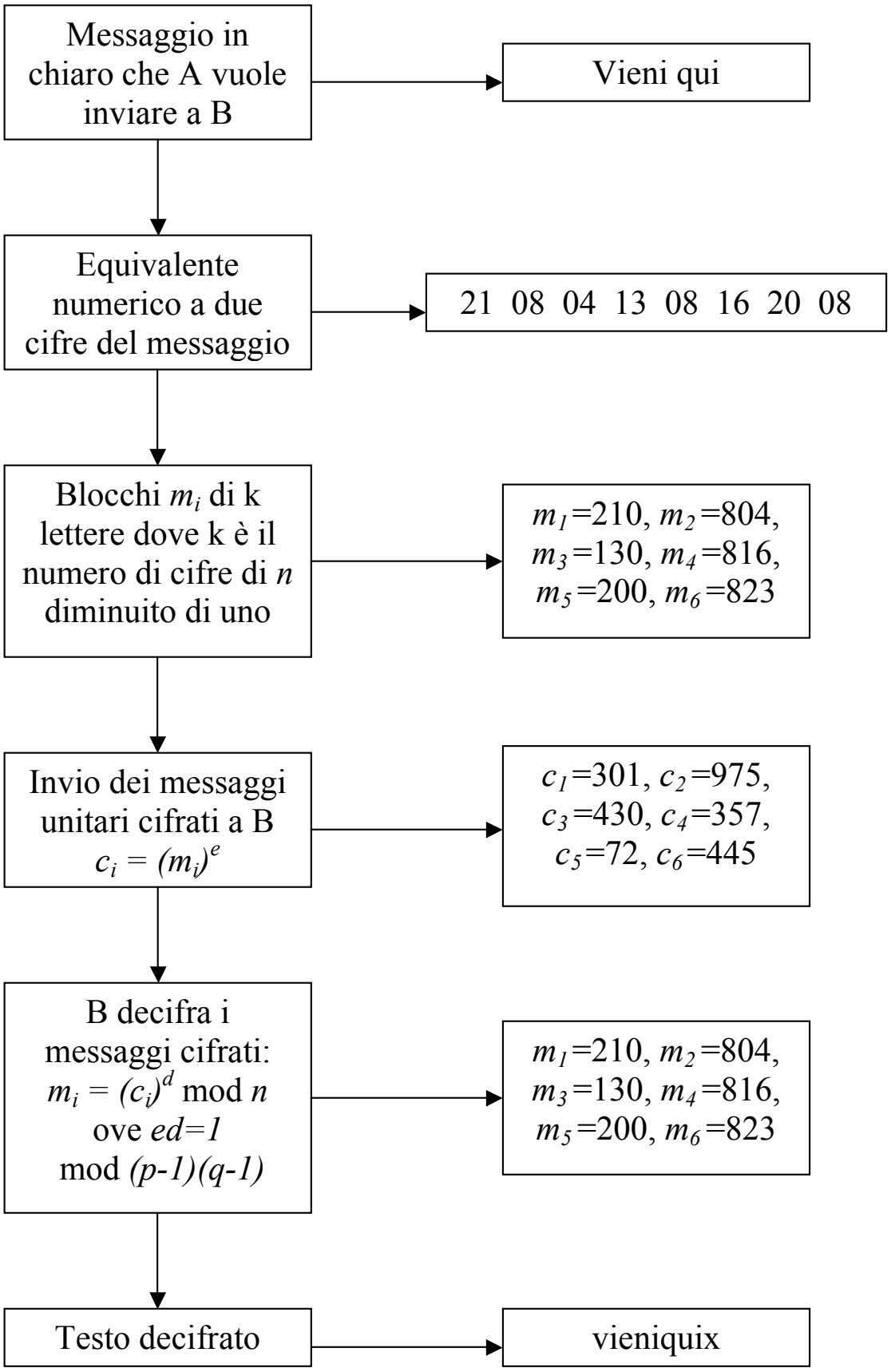
Poiché MCD(m, n) = 1, $MCD(P_i, n) = 1$, per il teorema di Eulero $m^{\,k\,(p-1)(q-1)} = m \bmod (n)$
e quindi

$$m^{e\,d} = m \bmod (n)$$

Osserviamo, infine, che quando il mittente ha cifrato il messaggio abbiamo richiesto che ciascun blocco di numeri m_i fosse minore di n: questo per garantire che non ci fosse ambiguità in fase di decrifratura nella determinazione del numero congruo a c^d modulo n.
Quest'ultimo è, infatti, l'unico numero che soddisfa la congruenza compreso tra 0 e $n-1$.

Ricostruiamo, per finire, tutto il viaggio da A a B del nostro messaggio in una tabella:

Ogni utente pubblica la coppia (n,e), dove $n=pq$ è prodotto di due numeri primi segreti e MCD $(e, (p-1)(q-1)) = 1$	⟶	B pubblica $(n,e)=(1003,3)$


Messaggio in chiaro che A vuole inviare a B
Vieni qui
Equivalente numerico a due cifre del messaggio
21 08 04 13 08 16 20 08
Blocchi m_i di k lettere dove k è il numero di cifre di n diminuito di uno
m_1=210, m_2=804, m_3=130, m_4=816, m_5=200, m_6=823
Invio dei messaggi unitari cifrati a B $c_i = (m_i)^e$
c_1=301, c_2=975, c_3=430, c_4=357, c_5=72, c_6=445
B decifra i messaggi cifrati: $m_i = (c_i)^d$ mod n ove $ed=1$ mod $(p-1)(q-1)$
m_1=210, m_2=804, m_3=130, m_4=816, m_5=200, m_6=823
Testo decifrato
vieniquix