QUINTO INCONTRO

Le potenze

Giocando con le operazioni in $\mathbf{Z_n}$, e' possibile cercare altre cifrature.
Cosa succede se, per cifrare, elevo ogni elemento ad una potenza fissata? Sto considerando l'applicazione: $\mathbf{Z_n} \to \mathbf{Z_n}$ definita da: $m \to m^t$.
Sono trasformazioni accettabili come cifrature?
Abbiamo visto che (per n>2) l'elevamento al quadrato non è una cifratura, perche [n–1] = [–1] e

$$1^2 = (-1)^2 = 1 \qquad \text{in } \mathbf{Z_n} \ .$$

Analogo risultato vale per le potenze pari.

Esiste sempre un esponente corretto da usare per ottenere una cifratura? In caso positivo, come può essere individuato?
Tavola 5.1 Potenze modulo 7
Abbiamo osservato su alcuni esempi un andamento ciclico delle potenze: ricordiamo come sia possibile prevedere analogo comportamento più in generale:

Piccolo teorema di Fermat: *Se p è un numero primo ed a non è divisibile per p, allora* $a^{p-1} = 1$ *mod p*

Tavola 5.2-5.3 Cifratura con il teorema di Fermat

Osservazione: nelle ipotesi del piccolo teorema di Fermat, $a^p = a$: in realtà non è necessario richiedere che a non sia divisibile per p. Dunque, in $\mathbf{Z_p}$ vale

$$a^s = a^{(p-1)+s} \quad \text{per ogni } s > 0$$

Dunque le potenze si ripetono ciclicamente, dopo $p-1$ passi.
Osservazione: se per caso $k(p-1)+1 = e\,d$, allora $a^{ed} = a^{k(p-1)+1} = (a^{(p-1)})^k \ a = a \bmod n$.
Ma $a^{ed} = (a^e)^d$: dunque posso usare $m \to m^e$ per cifrare e $c \to c^d$ per decifrare.

E se n non è primo?
Tavola 5.4 Potenze modulo 10
Esempio Modulo 10:

	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\mathbf{x^2}$	4	9	6	5	6	9	4	1
$\mathbf{x^3}$	8	7	4	5	6	4	2	9
$\mathbf{x^4}$	6	1	6	5	6	1	6	1
$\mathbf{x^5}$	2	3	4	5	6	7	8	9

Tavola 5.5 Teorema di Eulero
Teorema di Eulero: Se $n=pq$ è prodotto di due numeri primi distinti e MCD(a,n)=1, allora

$$a^{(p-1)(q-1)} = 1 \quad \mathbf{mod}\ n.$$

Dimostrazione: Piochè MCD(a,n)=1, sappiamo che MCD(a,p)=1 e MCD(a,q)=1. Per il Piccolo Teorema di Fermat per il primo p, sappiamo che

$$a^{(p-1)} = 1 \quad \text{mod } p \ \text{ e dunque } \ a^{(p-1)(q-1)} = 1 \quad \text{mod } p.$$

Analogamente, per il Piccolo Teorema di Fermat per il primo q, sappiamo che

$$a^{(q-1)} = 1 \quad \text{mod } q \ \text{ e dunque } \ a^{(p-1)(q-1)} = 1 \quad \text{mod } q.$$

Dunque sia p che q dividono il numero $a^{(p-1)(q-1)} - 1$: poichè p e q sono primi distinti, concludo che anche il loro prodotto n divide tale numero, e ho la tesi. ◊

***Corollario 1**: Se $n = pq$ è prodotto di due numeri primi distinti, allora*

$$a^{(p-1)(q-1)+1} = a \quad mod\ n.$$

Dimostrazione: Se $MCD(a,n)=1$, basta utilizzare il Teorema.
Ora consideriamo $a = p$: poichè $MCD(p,q)=1$, osservo che che $p^{(q-1)} = 1\ mod\ q$ per il Piccolo Teorema di Fermat, e quindi $(p^{(q-1)})^{(p-1)} = 1\ mod\ q$ per il Piccolo Teorema di Fermat: dunque il corollario è vero per $a = p$. Ma allora il teorema è vero per ogni potenza di p.

Se $MCD(a,n)=d \neq 1$, posso supporre $d=p$ a meno di scambio dei nomi: infatti, se n divide a, la tesi è sicuramente vera. Allora $a=p^m r$, ove r opportuno numero intero con $MCD(r,n) =1$; dunque

$$r^{(p-1)(q-1)+1} = r\ mod\ n$$

in base al Teorema, mentre $= p^{m[(p-1)(q-1)+1]} = p^m\ mod\ n$ per quanto appena osservato. Risulta

$$a^{(p-1)(q-1)+1} = p^{m[(p-1)(q-1)+1]}\ r^{(p-1)(q-1)+1} = p^m\ r\ mod\ n. \qquad ◊$$

Abbiamo imparato che alcuni esponenti sono sicuramente sbagliati**. Ma abbiamo imparato qualcosa di più: sappiamo scegliere alcuni esponenti giusti, e per essi sappiamo scrivere la funzione di decifratura:**

Osservazione: se per caso $(p-1)(q-1)+1 = e\, d$, allora $a^{ed} = a^{(p-1)(q-1)+1} = a \quad$ mod n.
Ma $a^{ed} = (a^e)^d$

Posso usare l'elevamento alla potenza con esponente *e* per cifrare e l'elevamento alla potenza con esponente *d* per decifrare…..
Per ovviare il problema del numero limitato di chiavi e, contemporaneamente, non utilizzare più sostituzioni monoalfabetiche, utilizziamo la cifratura a blocchi.

Riscrivo:

$$(p-1)(q-1)+1 = e\, d,$$

significa

$$(p-1)(q-1) = e\, d - 1,$$

dunque

$$e\, d = 1 \text{ modulo } (p-1)(q-1)$$

Le classi e, d sono inverse tra loro modulo $(p-1)(q-1)$

Tavola 5.6-5.7