Teoria dei Numeri (Crittografia)

17/1/2011 (Esercizi)

1) Bob usa un R.S.A. con $p=17$, $q=41$, $e=13$. Calcolate sia la "decryption-key" di Bob, che la "decryption-key" minima.

2) Alice usa un El Gamal con $p=29$, $\alpha=2$, $a=12$ e $\beta=\alpha^a \pmod p$, $\beta=7$ (come al solito p è un primo, α è una radice primitiva mod p). Quindi la chiave pubblica di Alice è la terna $(p,\alpha,\beta)=(29,2,7)$ e la chiave privata è $a=12$.

   i) Bob cifra il messaggio $M=7$ per Alice usando il parametro di mascheratura $k=11$. Qual'è il cifrato che Alice riceve?

   ii) Mettetevi nei panni di Alice e decifrate il messaggio.

   iii) Alice manda a Bob il messaggio $M=10$ scegliendo $k=13$ come parametro di mascheratura. Quale sarà la terna (M,γ,δ) che Bob riceverà?

---

3) Facoltativo

Nella rappresentazione binaria di un numero n compare solo la cifra 1, cioè $n=\underbrace{11\ldots1}_{k \text{ volte}}$.

Dimostrate che

$$3 \mid n \iff k \text{ è pari}$$

Teoria dei Numeri (Crittografia)

17/1/2011 (Teoria)

1) Crittosistema R.S.A.: cifratura, decifratura e firma (spiegarne bene il funzionamento).

2) Algoritmo euclideo e suo "running-time"

3) Crittosistema di El Gamal: cifratura, decifratura e firma. Spiegarne bene il funzionamento.

4) Facoltativo

Dimostrare che $P(n) = n^5 - n \equiv 0 \pmod{30}$ per ogni $n \geq 1$.

Teoria dei Numeri (Crittografia)

(Esercizi, 4 luglio 2013)

1) Alice è titolare di un crittosistema R.S.A. con $p = 47$, $q = 103$, $e = 29$.
Si domanda
i) calcolate la "decryption-key" di Alice
ii) calcolate la "decryption-key" minima di Alice.
iii) cifrate per Alice il messaggio $M = 10$

2) Bob è titolare di un crittosistema di El Gamal con
$(p, g, \beta) = (101, 2, 53)$ (chiave pubblica)
$a = 23$ (chiave privata)
(ovviamente $2^{23} \equiv 53 \pmod{101}$)
i) cifrate per Bob il messaggio $M = 13$ con parametro di mascheratura $k = 11$
ii) Bob firma il messaggio in chiaro $M = 9$ con parametro di mascheratura $k = 19$. Qual'è la firma?
iii) verificate l'autenticità della firma di Bob

0/0

3) Trovate tutte le soluzioni della congruenza

$$18x \equiv 6 \pmod{51}$$

La congruenza $18x \equiv 6 \pmod{45}$ ha soluzione? (Giustificate la risposta)

Domande facoltative

4) In quale classe di resto modulo 7 si trova il numero $n = (725843)^{596}$? Qual'è l'ultima cifra decimale di $n = (7452431)^{723}$? Se preste trovare le risposte facendo i calcoli con carta e penna (suggerimento: utilizzate le proprietà delle congruenze ed il teorema di Eulero - Fermat).

Compito di "Teoria dei Numeri"

(27/6/05)

1) Bob usa un R.S.A. con $p=19$, $q=43$, $e=11$. Calcolate la "decryption key" d di Bob, la "decryption key" minima d_1 e un messaggio fisso non banale.

2) Alice usa un El Gamal con $p=59$, $\alpha=2$, $a=8$ e quindi $\beta \equiv \alpha^a \equiv 2^8 \equiv 20 \pmod{59}$ (2 è radice prim. mod 59)

$(p, \alpha, \beta) = (59, 2, 20)$ è la chiave pubblica di Alice

$a=8$ è la chiave segreta di Alice.

- Alice riceve da Bob il cifrato $(3, 5) = (\gamma, \delta)$. Qual'è il messaggio di Bob?
- Alice manda a Bob il messaggio, non cifrato ma firmato, $x=15$. Se Alice sceglie il parametro $k=11$ come maschera, quale terna $(x, (\gamma, \delta)) = (15, (\gamma, \delta))$ riceverà Bob?

3) Nella rappresentazione ternaria di un numero n compare solo la cifra 1, cioè $n = \underbrace{11\ldots1}_{k \text{ volte}}$.
Dimostrate che

$4 \mid n \iff k$ è pari.

4) Quanto vale la somma $\sum_{11}^{5} = \sum_{j=1}^{10} \left\{\frac{5 \cdot j}{11}\right\}$?
(come al solito $\{x\}$ indica la parte frazionaria di x)

di x). Il risultato cambia se si calcola, per $a \not\equiv 0 \ (11)$,

$$\Sigma_{11}(a) = \sum_{j=1}^{10} \left\{\frac{aj}{11}\right\} ?$$ Giustificare la risposta

29/6/09

Teoria dei Numeri

(Crittografia) (Parte teorica)

1) Crittosistema R.S.A.: cifratura, decifratura e firma (spiegare bene il funzionamento).

2) Potenza modulare e suo "running-time" (con dimostrazione)

3) Congruenza lineare $ax \equiv b \pmod m$: quando è risolubile? Se è risolubile quante sono le soluzioni? Si possono calcolare in tempo polinomiale? Esporre la teoria (con dimostrazione)

Domande facoltative

1) Calcolate le ultime due cifre decimali di $(17)^{203}$. (Ricordate che $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 5 \cdot 4 = 40$)

2) Se p è un numero primo a^{2p+1} e a^3 divisi per p danno sempre lo stesso resto per ogni $a \in \mathbb{N}$. Giustificate la risposta.

3) Se p è un numero primo a^{2p+1} e a^3 divisi per p danno sempre lo stesso resto? Giustificate la risposta.

Teoria dei Numeri (Crittografia)

(Teoria, 4 luglio 2013)

1) L'algoritmo euclideo ed il suo "running-time"
2) Il crittosistema di Rabin
3) La firma di El Gamal

Domanda facoltativa

Giochi di società

Alcune famiglie di amici (con nonni, genitori e figli) si riuniscono per una festa. Uno dei partecipanti si dichiara in grado di indovinare l'età di chiunque se gli vengono fornite queste informazioni:

- qual'è il resto dell'età della persona divisa per 4
- qual'è il resto dell'età della persone divisa per 7
- inoltre può vedere la persona

C'è da crederegli? Giustificate la risposta.