COMPLESSITÀ e RANDOMIZZAZIONE

ESERCIZIO 1

\# chiavi $= 2^{46}$

\# ops per chiave $= 128 * |m|$

$|m| = 1000 = 10^3$

$1\, ns = 10^{-9} s$

$$t = 2^{46} * 128 * 10^3 * 10 * 10^{-9} s =$$

$$= 2^{46} * 2^7 * 10^{-5} s = 2^{53} * 10^{-5} s$$

$$= 2^3 \cdot 2^{50} * 10^{-5} s \simeq 8 \cdot (10^3)^5 \cdot 10^{-5} s$$

$$2^{10} \simeq 10^3$$

$$\simeq 8 \cdot 10^{10} s \simeq 2500 \text{ anni}\ldots$$

ESERCIZIO 2

1. $11 \bmod 4 = 3$ ✓
   $23 \bmod 4 = 3$ ✓

   $2\left\lfloor \frac{11}{4} \right\rfloor + 1 = 2 \cdot 2 + 1 = 5$ è primo ✓

   $2\left\lfloor \frac{23}{4} \right\rfloor + 1 = 11$ è primo ✓

2. $M = 123456$

$11 * 23 = 253$

$M \bmod 100 = 56$

$x_0 = 56^2 \bmod 253 = 100 \rightarrow 0$

$x_1 = 100^2 \bmod 253 = 133 \rightarrow 1$

$x_2 = 133^2 \bmod 253 = 232 \rightarrow 0$

$x_3 = 232^2 \bmod 253 = 188 \rightarrow 0$

$x_4 = 188^2 \bmod 253 = 177 \rightarrow 1$

$x_5 = 177^2 \bmod 253 = 210 \rightarrow 0$

$x_6 = 210^2 \bmod 253 = 78 \rightarrow 0$

$x_7 = 78^2 \bmod 253 = 12 \rightarrow 0$

$x_8 = 12^2 \bmod 253 = 144 \rightarrow 0$

$x_9 = 144 \bmod 253 = 243 \rightarrow 1$

$\rightarrow$ 1 0 0 0 0 1 0 0 1 0

3. Vedi testo

ESERCIZIO 3

1. $M = 123456$

$3 \rightarrow 011$, $4 \rightarrow 100$

$C = 1\underbrace{011}\underbrace{100} = 64 + 16 + 8 + 4 = 92$

$$37^{92} \bmod 100 = 37^{64+16+8+4} \bmod 100$$

$$37^2 \bmod 100 = 69$$
$$37^4 \bmod 100 = 69^2 \bmod 100 = 61$$
$$37^8 \bmod 100 = 61^2 \bmod 100 = 21$$
$$37^{16} \bmod 100 = 21^2 \bmod 100 = 41$$
$$37^{32} \bmod 100 = 41^2 \bmod 100 = 81$$
$$37^{64} \bmod 100 = 81^2 \bmod 100 = 61$$

$$\rightarrow 37^{92} \bmod 100 = (61 * 41 * 21 * 61) \bmod 100 = 81$$

2. Esegue un numero di moltiplicazioni logaritmico nel valore dell'esponente (dunque lineare nella sua dimensione)

ESERCIZIO 4

$N = 113$ $\quad \frac{1}{4^k} < \frac{1}{50}$ $\quad$ per $k = 3$

occorrono 3 testimoni y scelti a caso in $[2, 112]$

$\boxed{y=3}$

1) $MCD(113, 3) = MCD(3, \overbrace{113 \bmod 3}^{2})$

$= MCD(2, \overbrace{3 \bmod 2}^{1})$

$= MCD(1, 0) = 1$ ✓

2) $N = 113$

$N - 1 = 112 = 2^4 \cdot 7$ $\quad w = 4, \quad z = 7$

$3^7 \bmod 113 = 3^{1+2+4} \bmod 113 =$

$3^2 \bmod 113 = 9$

$3^4 \bmod 113 = 9^2 \bmod 113 = 81$

$= (3 \cdot 9 \cdot 81) \bmod 113 = 40 \neq 1$

occorre proseguire nella valutazione del predicato

$0 \leq i \leq w-1 = 3$

$0 \leq i \leq w-1 = 3$

$i = 0$ $\quad 3^{2^0 \cdot 7} \bmod 113 = 3^7 \bmod 113 = 40 \neq -1$

$i = 1$

$$3^{2^1 \cdot 7} \bmod 113 = (3^7)^2 \bmod 113 =$$
$$= 40^2 \bmod 113 = 18 \quad \neq -1$$

$i = 2$

$$3^{2^2 \cdot 7} \bmod 113 = 18^2 \bmod 113 = 98 \quad \neq -1$$

$i = 3$

$$3^{2^3 \cdot 7} \bmod 113 = 98^2 \bmod 113 = -1 \quad \checkmark$$

ok.

Per gli altri 2 valori di y si procede in modo analogo

ESERCIZIO 5

Vedi testo

CIFRARI STORICI

ESERCIZIO 1

1) This exercise is easy $k=21$
2) This exercise is not difficult either

ESERCIZIO 2

$a = 11 \qquad b = 14$

infatti:

$$\begin{cases} pos(N) = (a\,pos(H) + b) \mod 26 \\ pos(O) = (a\,pos(A) + b) \mod 26 \end{cases}$$

con

$pos(N) = 13, \quad pos(H) = 7$

$pos(O) = 14, \quad pos(A) = 0$

da cui

$$\begin{cases} 13 = (7 \cdot a + b) \mod 26 \\ 14 = (0 \cdot a + b) \mod 26 \end{cases}$$

Risolvendo il sistema si ottiene

$b = 14$

$a = (13 - b) * 7^{-1} \mod 26$

da cui

$$a = -1 * 7^{-1} \mod 26$$

$$= -1 * 15 \mod 26 = 11$$

$(7^{-1} \mod 26 = 15)$

$\Rightarrow$

$$pos(Y) = (11\, pos(X) + 14) \mod 26$$

ESERCIZIO 3

Alfabeto di 27 caratteri

a deve essere primo con $27 = 3^3$

$\hookrightarrow$ a può assumere i valori tra 1 e 26 che non sono multipli di 3

$\hookrightarrow$ $\phi(27) = \phi(3^3) = 2 \cdot 3^2 = 18$

funzione di Eulero

infatti $\phi(p^k) = (p-1)\, p^{k-1}$

p primo

b può assumere tutti i valori in [0, 26]

$\Rightarrow$ # chiavi $= 18 * 27 - \underbrace{1}_{\text{si esclude la coppia (1,0) che lascia il messaggio inalterato}} = 485$

Alfabeto di 29 caratteri

29 è primo

$\Rightarrow$ a può assumere tutti i valori in $[1, 28]$ $(\rightarrow \phi(29) = 28)$

e b può assumere tutti i valori in $[0, 28]$

$\#$ chiavi $= 28 * 29 \underbrace{- 1}_{\text{si esclude } (1,0)} = 811$

ESERCIZIO 4

$$C_2(C_1(x)) = (a_2 \, C_1(x) + b_2) \bmod 26$$

$$= (a_2(a_1 x + b_1) + b_2) \bmod 26 =$$

$$= (a_1 a_2 x + a_2 b_1 + b_2) \bmod 26$$

$$= (a_3 x + b_3) \bmod 26$$

con

$$a_3 = a_1 a_2 \bmod 26$$

$$b_3 = a_2 b_1 + b_2 \bmod 26$$

ESERCIZIO 5

1. Parte della permutazione che definisce il cifrario.
(più precisamente si trova l'immagine cifrata di 22 caratteri su 26)

2. 24 chiavi.
infatti mancano le corrispondenze per 4 caratteri, e se ne potrebbero costruire $4! = 24$ differenti.

3. THE WEASEL RUN AWAY FROM LONDON ZOO

ESERCIZIO 6

Con le prime 4 lettere del mio cognome come chiave si ottiene il crittogramma

DVZGUSXEBJZN

ATTACCO: vedi testo / lucidi

ESERCIZIO 7

2. In generale $26! - 1$.
Ma per decifrare il crittogramma ottenuto cifrando "APPELLO DI FEBBRAIO" occorrono meno prove.
Infatti il crittogramma contiene 10 lettere

diverse tra loro, da decifrare

$\Rightarrow$

$\#\text{prove} = 26 \cdot 25 \cdot \ldots \ldots \cdot 17 \longrightarrow$ # possibilità per la 10ª lettera

$\swarrow$ # possibilità per la 1ª lettera

$\searrow$ # possibilità per la 2ª lettera ...

$\Rightarrow$

$$\#\text{prove} = 26 \cdot 25 \cdot \ldots \cdot 17 = \frac{26!}{16!} \simeq 2 \cdot 10^{13}$$

3. Crittoanalisi statistica: vedi testo

ESERCIZI 8, 9, 10, 11

Vedi libro di testo / lucidi