Università degli studi di Roma Tre
Corso di Laurea in Matematica, a.a. 1999/2000
Matematica Applicata 2
Quarto Test

CERCARE DI RISOLVERE IL MASSIMO NUMERO DEI SEGUENTI PROBLEMI

1. Si dimostri che se n è privo di fattori quadratici e $\nu(n)$ è il numero di divisori primi di n, allora $x^2 - 1$ ammette $2^{\nu(n)}$ radici in $\mathbf{Z}/n\mathbf{Z}$.

2. Si trovi un fattore di $n = 3111$ utilizzando l'algoritmo $p - 1$.

3. Sia $n = 33$ e $k = 2$. Si trasmetta $x = 5$ utilizzando il crittosistema di Rabin e si decodifichi $y = 8$ (se è possibile).

4. In meno dieci righe si spieghi cosa è DES e a cosa serve.

5. Un numero naturale composto n si dice di Carmichael se per ogni $b \in U(\mathbf{Z}/n\mathbf{Z})$ risulta

$$b^{n-1} \equiv 1 \pmod{n}$$

   a. Sia n un intero positivo senza fattori quadratici. Dimostrare che n è di Carmichael se e soltanto se $p - 1$ divide $n - 1$ per ogni primo p che divide n.
   b. Dimostrare che 561 è un numero di Carmichael.