Ejercicio 2

David García Curbelo

Partimos de nuestro dni= 45352581. Dividimos dicho número en dos bloques, 4535 y 2581. Sean $p = 4547$ y $q = 2591$ los primeros primos mayores o iguales que los bloques anteriores. Sea $n = pq = 11781277$ y e el menor primo mayor o igual que 11 que es primo relativo con $\varphi(n)$. Sea $d = e^{-1} \pmod{\varphi(n)}$.

Tenemos así $\varphi(n) = 11774140$, $e = 11$ y $d =$

Apartado I. ***Cifra el mensaje*** $m = 0xCAFE$***.***

Apartado II. ***Descifra el criptograma anterior.***

Apartado III. ***Intenta factorizar*** n ***mediante el método*** $P-1$ ***de Polard. Para ello llega, como máximo a*** $b=8$***.***

Apartado IV. ***Intenta factorizar*** n ***a partir de*** $\varphi(n)$**.**

Apartado V. ***Intenta factorizar*** n ***a partir de*** e ***y*** d***.***