$p = 73$

$q = 59$

$n = 73*59 = 4307$

$\phi(n) = 72*58 = 4176$

$e = 191$

$d = e^{-1} \pmod{\phi(n)}$

$e*d = 1 \pmod{\phi(n)}$

$\phi(n)*a + e*d = 1$

We will use the Extended Euclidean Algorithm to find the value of d (a is not needed in this case)

$v_1 = 1$

$v_2 = 0$

$a = \phi(n)$

$b = e$

$191>0$:

$q = [a/b] = 21$

$r = a - q*b = 4176 - 21*191 = 165$

$v = v_2 - q*v_1 = -21$

$a = b = 191$

$b = r = 165$

$v_2 = v_1 = 1$

$v_1 = v = -21$

165>0:

$q = [a/b] = 1$

$r = a - q*b = 191 - 1*165 = 26$

$v = v_2 - q*v_1 = 1 - (-21) = 22$

$a = b = 165$

$b = r = 26$

$v_2 = v_1 = -21$

$v_1 = v = 22$

26>0:

$q = [a/b] = 6$

$r = a - q*b = 165 - 6*26 = 9$

$v = v_2 - q*v_1 = -21 - 6*22 = -153$

$a = b = 26$

$b = r = 9$

$v_2 = v_1 = 22$

$v_1 = v = -153$

9>0:

$q = [a/b] = 2$

$r = a - q*b = 8$

$v = v_2 - q*v_1 = 22 - 2*(-153) = 328$

$a = b = 9$

$b = r = 8$

$v_2 = v_1 = -153$

$v_1 = v = 328$

8>0:

$q = [a/b] = 1$

$r = a - q*b = 1$

$v = v_2 - q*v_1 = -153 - 328 = -481$

$a = b = 8$

$b = r = 1$

$v_2 = v_1 = 328$

v1 = v = -481

1>0:

q = [a/b] = 8

r = a - q*b = 0

$v = v_2 - q*v_1 = 328 - 8*(-481) = 4176$

a = 1

b = r = 0

$v_2 = v_1 = -481$

$v_1 = v = 4176$

result: $v_2 = -481$

$d = v_2 + \phi(n) = 3695$ (we add $\phi(n)$ because the result is < 0)

dani

m = da

M = 4*27 + 1 = 109

$M^e \pmod n = 109^{191} \pmod{4307}$

$191 = 128 + 32 + 16 + 8 + 4 + 2 + 1 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^7$

$109^{(2^0)} = 109$

$109^{(2^1)} = 109^{(2^0)} * 109^{(2^0)} = 109*109 = 3267$

$109^{(2^2)} = 109^{(2^1)} * 109^{(2^1)} = 3267*3267 = 543$

$109^{(2^3)} = 109^{(2^2)} * 109^{(2^2)} = 543*543 = 1973$

$109^{(2^4)} = 109^{(2^3)} * 109^{(2^3)} = 1973*1973 = 3508$

$109^{(2^5)} = 109^{(2^4)} * 109^{(2^4)} = 3508*3508 = 965$

$109^{(2^6)} = 109^{(2^5)} * 109^{(2^5)} = 965*965 = 913$

$109^{(2^7)} = 109^{(2^6)} * 109^{(2^6)} = 913*913 = 2318$

$109^{191} \pmod{4307} = 109^{(2^0+2^1+2^2+2^3+2^4+2^5+2^7)}=$

$= 109 * 3267 * 543 * 1973 * 3508 * 965 * 2318 = 3887 \pmod{4307}$

$3887 = 5*27^2 + 8*27 + 26 \rightarrow e(m) = EHZ$

m = ni

M = 14*27 + 9 = 387

$M^e \pmod{n} = 387^{191} \pmod{4307}$

$191 = 128 + 32 + 16 + 8 + 4 + 2 + 1 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^7$

$387^{(2^0)} = 387$

$387^{(2^1)} = 387^{(2^0)} * 387^{(2^0)} = 387*387 = 3331$

$387^{(2^2)} = 387^{(2^1)} * 387^{(2^1)} = 3331*3331 = 729$

$387^{(2^3)} = 387^{(2^2)} * 387^{(2^2)} = 729*729 = 1680$

$387^{(2^4)} = 387^{(2^3)} * 387^{(2^3)} = 1680*1680 = 1315$

$387^{(2^5)} = 387^{(2^4)} * 387^{(2^4)} = 1315*1315 = 2118$

$387^{(2^6)} = 387^{(2^5)} * 387^{(2^5)} = 2118*2118 = 2337$

$387^{(2^7)}$ =$387^{(2^6)}$*$387^{(2^6)}$= 2337*2337 = 293

387^191 (mod 4307) = $387^{(2^0+2^1+2^2+2^3+2^4+2^5+2^7)}$ =

= 387 * 3331 * 729 * 1680 * 1315 * 2118 * 293 = 3806 (mod 4307)

3806 = 5*(27^2) + 5*27 + 26 --> e(m) = EEZ

m = dani

e(m) = EHZEEZ

/----------

d = 3695

m = EHZ

M = $5*27^2 + 8*27 + 26 = 3887$

M^d (mod n) = 3887^{3695} (mod 4307)

$3695 = 2048 + 1024 + 512 + 64 + 32 + 8 + 4 + 2 + 1 =$

$= 2^0 + 2^1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^9 + 2^{10} + 2^{11}$

$3887^{(2^0)} = 3887$

$3887^{(2^1)} = 3887^{(2^0)} * 3887^{(2^0)} = 4120$

$3887^{(2^2)} = 3887^{(2^1)} * 3887^{(2^1)} = 513$

$3887^{(2^3)} = 3887^{(2^2)} * 3887^{(2^2)} = 442$

$3887^{(2^4)} = 3887^{(2^3)} * 3887^{(2^3)} = 1549$

$3887^{(2^5)} = 3887^{(2^4)} * 3887^{(2^4)} = 402$

$3887^{(2^6)} = 3887^{(2^5)} * 3887^{(2^5)} = 2245$

$3887^{(2^7)} = 3887^{(2^6)} * 3887^{(2^6)} = 835$

$3887^{(2^8)} = 3887^{(2^7)} * 3887^{(2^7)} = 3798$

$3887^{(2^9)} = 3887^{(2^8)} * 3887^{(2^8)} = 661$

$3887^{(2^{10})} = 3887^{(2^9)} * 3887^{(2^9)} = 1914$

$3887^{(2^{11})} = 3887^{(2^{10})} * 3887^{(2^{10})} = 2446$

$3887^{3695} \pmod{4307} = 3887^{(2^0+2^1+2^2+2^3+2^5+2^6+2^9+2^{10}+2^{11})} =$

$= 3887 * 4120 * 513 * 442 * 402 * 2245 * 661 * 1914 * 2446 =$

= 109 (mod 4307)

109 = 4*27 + 1

d(m) = da

m = EEZ

M = $5*27^2 + 5*27 + 26 = 3806$

M^d (mod n) = 3806^{3695} (mod 4307)

3695 = 2048 + 1024 + 512 + 64 + 32 + 8 + 4 + 2 + 1 =

= $2^0 + 2^1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^9 + 2^{10} + 2^{11}$

$3806^{(2^0)}$= 3806

$3806^{(2^1)} = 3806^{(2^0)}*3806^{(2^0)}$= 1195

$3806^{(2^2)}= 3806^{(2^1)}*3806^{(2^1)}$= 2408

$3806^{(2^3)}= 3806^{(2^2)}*3806^{(2^2)}$= 1242

$3806^{(2^4)}$= $3806^{(2^3)}$*$3806^{(2^3)}$= 658

$3806^{(2^5)}$= $3806^{(2^4)}$*$3806^{(2^4)}$= 2264

$3806^{(2^6)}$= $3806^{(2^5)}$*$3806^{(2^5)}$= 366

$3806^{(2^7)}$= $3806^{(2^6)}$*$3806^{(2^6)}$= 439

$3806^{(2^8)}$= $3806^{(2^7)}$*$3806^{(2^7)}$ = 3213

$3806^{(2^9)}$= $3806^{(2^8)}$*$3806^{(2^8)}$= 3797

$3806^{(2^{10})}$= $3806^{(2^9)}$*$3806^{(2^9)}$= 1680

$3806^{(2^{11})}$= $3806^{(2^{10})}$*$3806^{(2^{10})}$= 1315

3806^{3695} (mod 4307) = $3806^{(2^0+2^1+2^2+2^3+2^5+2^6+2^9+2^{10}+2^{11})}$ =

3806 * 1195 * 2408 * 1242 * 2264 * 366 * 3797 * 1680 * 1315 =

= 387 (mod 4307)

387 = 14*27 + 9

d(m) = ni

m = EHZEEZ

d(m) = dani