Číslo cvičení: 5
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. Using Euler's totient:
   $\varphi(10) = 4, 7^4 = 1 \mod 10, 7^{(7^7)} = 7^{823543} = 7^{4\cdot 205855+3} = 1^{205855} \cdot 7^3 = 3 \mod 10$

2. $c_1 = w^{e_1} \mod n$, $c_2 = w^{e_2} \mod n$. There exist a, b such that $ae_1 + be_2 = 1$. Making both encryption equations to their respective powers of a, b and multiplying them we get:
   $c_1^a \cdot c_2^b = w^{ae_1+be_2} = w^1 \mod n.$
   $a = -162535$, $b = 372082$, $w = 3198255$
   $(3198255^{162535})^{-1} \mod 4019989 = 698291$, $2125927^{372082} \mod 4019989 = 3608440$
   $3608440 \cdot 698291 \mod 4019989 = 10873 = m$

3. $X = q^x \mod p = 5^{27} \mod 863 = 79, Y = 5^{33} \mod 863 = 285,$
   $K = X^y = Y^x \mod p = 249.$

4. Using factorization:
   $n = pq = 37 \cdot 41 \implies \varphi(n) = 1440.\ 551 = d^{-1} \mod 1440 \implies d = 311.$
   $w = c^d \mod n.\ \{1374, 1278, 682, 809, 890, 380, 0, 57\}^{311} \mod 1517 =$
   $\{20, 19, 70, 17, 190, 803, 0, 426\} \implies$
   plaintext$= 02, 00, 19, 07, 00, 17, 19, 08, 03, 00, 04, 26 =$"cathartidae"+EOT

5. (a) $(1, 4, 9, 25, 41, 82, 170, 333) \cdot 200 \mod 701 = (200, 99, 398, 93, 489, 277, 352, 5) = K$
   (b) $(200, 99, 398, 93, 489, 277, 352, 5)'(1, 0, 0, 1, 0, 1, 0, 1) = 575$
   $u^{-1} \mod 701 = 347$, $c' = 441$.
   $441 - 333 = 108,\ 108 - 82 = 26,\ 26 - 25 = 1,\ 1 - 1 = 0 \implies$
   $w = (1, 0, 0, 1, 0, 1, 0, 1)$

6. $f = 1, m = 5829672, 2807399 \cdot 5399 - 2600 \cdot 5829672 = 1 \implies v = 2807399$
   $\{16278, 49020, 43554, 00279\}^{2807399} \mod 99443 = \{73327, 67986, 69328, 97985\}$
   Plaintext is "I LOVE YOU".