$d = e^{-1} \bmod \varphi(n)$ $\quad \varphi(n) = 16 \cdot 22 = 352$

$dp = d \bmod \varphi(p)$ $\quad \varphi(p) = 16$

$dq = d \bmod \varphi(q)$ $\quad \varphi(q) = 22$

a	b	$\lfloor a/b \rfloor$	u	v
352	7	50	-3	$1 - 50 \cdot -3 = 151$
7	2	3	1	$0 - 3 \cdot 1 = -3$
2	1	2	0	1
1	0		1	0

$d = 151 \bmod 352 = 151$

$dp = 151 \bmod 16 = 7$

$dq = 151 \bmod 22 = 19$

$sp = (k(m))^{dp} \bmod p = (100)^7 \bmod 16$

$= ((100)^2 100)^2 100 \bmod 16$

$= ((4)^2 4)^2 4 \bmod 16$

$= (16 \cdot 4)^2 4 \bmod 16$

$= (0 \cdot 4)^2 4 \bmod 16$

$= 0 \bmod 16 = 0$

$7 = [111]_2$

$19 = 16 + 2 + 1 = [10011]_2$

$sq = (k(m))^{dq} \bmod q = (100)^{19} \bmod 22 = ((((100)^2)^2)^2 100)^2 100 \bmod 22$

$= ((((12)^2)^2)^2 12)^2 12 \bmod 22$

$= ((((144)^2)^2 12)^2 12 \bmod 22$

$= ((((12)^2)^2 12)^2 12 \bmod 22$

$= 12 \bmod 22$

$= 12$

$sp = (k(m))^{dp} \bmod p$

$= (100)^7 \bmod 17$

$= ((100)^2 100)^2 100 \bmod 17$

$= ((15)^2 15)^2 15 \bmod 17$

$= (225 \cdot 15)^2 15 \bmod 17$

$= (4 \cdot 15)^2 15 \bmod 17$

$= (60)^2 15 \bmod 17$

$= 3600 \cdot 15 \bmod 17$

$= 13 \cdot 15 \bmod 17$

$= 195 \bmod 17$

$= 8 \bmod 17$

$sq = (100)^{19} \bmod 23$

$= (((((100)^2)^2 100)^2 100)^2 100 \bmod 23$

$= (((((8)^2)^2)^2 8)^2 8 \bmod 23$

$= (((64)^2)^2 8)^2 8 \bmod 23$

$= (((18)^2)^2 8)^2 8 \bmod 23$

$= ((324)^2 8)^2 8 \bmod 23$

$= (2)^2 \cdot 8)^2 8 \bmod 23$

$= (4 \cdot 8)^2 8 \bmod 23$

$= (32)^2 8 \bmod 23$

$= 9^2 \cdot 8 \bmod 23$

$= 81 \cdot 8 \bmod 23$

$= 12 \cdot 8 \bmod 23$

$= 96 \bmod 23$

$= 4$

$s = 8 \bmod 17$

$s = 4 \bmod 23$

$s = 3 \cdot 23 \cdot 8 - 4 \cdot 17 = 280 \bmod 391 = 280$

$3 \cdot 23 - 4 \cdot 17 = 1 \bmod p \cdot q = 1 \bmod 17 \cdot 23 = 1 \bmod 391$

a	b	$\lfloor a/b \rfloor$	u	v
23	17	1	3	$-1 - 1 \cdot 3 = -4$
17	6	2	-1	$1 - 2 \cdot -1 = 3$
6	5	1	1	$0 - 1 \cdot 1 = -1$
5	1	5	0	1
1	0		1	0

$3 \cdot 23 - 4 \cdot 17 = 1$

$6q - 6d = 1$

$= gcd(p,q)$

here: $u \cdot q \cdot sp + v \cdot p \cdot sq = s \bmod n$

$280^7 \bmod 391 = 100\,8$

now, we have

$sp = sp'$

$sq = 4$

hence, $s' \equiv 3 \cdot 23 \cdot sp' - 4 \cdot 17 \cdot 4$

$= 69 \cdot sp' - 272$

$= 69 \cdot sp' + 119 \mod 391$

$k' = (s')^e \mod n$

$= (69 \cdot sp' + 119)^7 \mod n$

$= (69 \cdot sp' + 119)^7 \mod 391$ (mod 391)

say $sp' \equiv 7$ (instead of 8)

then we have

$k' = (69 \cdot 7 + 119 \mod 391)^7 \mod 391$

$= (483 + 119 \mod 391)^7 \mod 391$

$= (602 \mod 391)^7 \mod 391$

$= 211^7 \mod 391$

$= ((211)^2 \cdot 211)^2 \cdot 211 \mod 391$

$= (44521 \cdot 211)^2 \cdot 211 \mod 391$

$= (338 \cdot 211)^2 \cdot 211 \mod 391$

$= (71318)^2 \cdot 211 \mod 391$

$= 156^2 \cdot 211 \mod 391$

$= 24336 \cdot 211 \mod 391$

$= 94 \cdot 211 \mod 391$

$= 19834 \mod 391$

$= 284$

$q = \gcd(n, k' - k(m))$

$= \gcd(391, 2884 - 100)$

$= \gcd(391, 284)$

a	b	$\lfloor a/b \rfloor$
391	284	2
284	23	8
23	0	

$q = \gcd(391, 284) = 23$

$p = \frac{n}{q} = \frac{391}{23} = 17$

$q = \gcd(n, k' - k(m))$

$= \gcd(391, 225 - 100)$

$= \gcd(391, 125)$

a	b	$\lfloor a/b \rfloor$	u	v
391	125	3		
125	16	7		
16	13	1		
13	3	4		
3	1	3		
1	0			