Review M22 Ex 2 Win 08

(1) $23 = 7 \cdot 3 + 2$
$7 = 2 \cdot 3 + 1$ ← GCD
$2 = 1 \cdot 2 + 0$

$1 = 1 \cdot 7 - 2 \cdot 3$
$1 = 1 \cdot 7 - (23 - 7 \cdot 3) \cdot 3$
$1 = (-3) \cdot 23 + (10) 7$
$\boxed{m = -3,\ n = 10}$

(2) $42x \equiv_{46} 36$

$21x \equiv_{23} 18$ (divide 42, 36, and 46 by 2)

$7x \equiv_{23} 6$ (divide 21 and 18 by 3, leave 23 alone!)

From (1), $1 = (-3) \cdot 23 + (10) 7$
so $1 \equiv 10 \cdot 7 \pmod{23}$, and $7^{-1} \equiv 10 \pmod{23}$
Multiply both sides of $7x \equiv_{23} 6$ by 10:
$10 \cdot 7x \equiv_{23} 10 \cdot 6$
$70x \equiv_{23} 1x \equiv_{23} 60 \equiv_{23} 14$

So $x \equiv_{23} 14$ or $\boxed{x \equiv_{46} 14 \text{ or } 23+14=37}$

(3) (a) Raise $26^{11} \pmod{899}$, where $899 = 29 \cdot 31$
Decoding key: Solve $11x \equiv 1 \pmod{28 \cdot 30}$
Do this as in problem 1:
$840 = 76 \cdot 11 + 4$
$11 = 2 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$

$1 = 4 - 3$
$= 4 - (11 - 2 \cdot 4)$
$= (-1) 11 + 3 \cdot 4$
$= (-1) 11 + 3 (840 - 76 \cdot 11)$
$= 3 \cdot 840 + (-229) \cdot 11$

Therefore $1 \equiv 3 \cdot 840 + (-229) 11 \pmod{840}$
or $1 \equiv_{840} (-229) \cdot 11$

But $-229 \equiv_{840} 840 - 229 \equiv 611 \pmod{840}$
So the inverse of 11 is 611, mod 840

The decoding key is 611, and to decode we raise the message $(26^{11})^{611} \equiv 26 \pmod{899}$