CS182 **Homework 6 Sketch of Solution** **Spring 2012**

Question 1.

1. Compute $u = x^2$, $v = u^2$, $w = v^2$, and the answer as $u * v * w$
2. Compute $u = x^2$, $v = u^2$, $w = v^2$, $x = w^2$ and the answer as $w * x$

Question 2.

- `EEuclid`$(172, 20)$, returns $(4, 2, -17)$
- `EEuclid`$(20, 12)$, returns $(4, -1, 2)$
- `EEuclid`$(12, 8)$, returns $(4, 1, -1)$
- `EEuclid`$(8, 4)$, returns $(4, 0, 1)$
- `EEuclid`$(4, 0)$, returns $(4, 1, 0)$

Question 3. Any two numbers from the set $\{3, 5, 7\}$ have gcd of 1. We can therefore use the Chinese Remainder Theorem to get the answer:

$2 * 35*$(multiplicative inverse mod 3 of 35) + $3 * 21*$(multiplicative inverse mod 5 of 21) + $2 * 15*$(multiplicative inverse mod 7 of 15) =

$70*$(multiplicative inverse mod 3 of 2) + $63*$(multiplicative inverse mod 5 of 1) + $30*$(multiplicative inverse mod 7 of 1) $= 70 * 2 + 63 * 1 + 30 * 1 = 233$

which, after reducing modulo 105, gives $x = 23$.

Question 4. Ciphertext for 112 is 18. $p = 11$, q =13, $d = 103$. Plaintext for 7 is 123.