CMSC 414: HW 2 Grading Key

Total 20 points

---

4. [4 points]

1- writing something

2- saying d is unique in $Z_{(p-1)\cdot(q-1)}$

3,4-a)saying d is unique in $Z_{(p-1)\cdot(q-1)}$

b)e has a multiplicative inverse mod $(p-1)\cdot(q-1)$ iff e is relatively prime to $(p-1)\cdot(q-1)$. So multiplying the elements of $Z(p-1)\times(q-1)$ by e results in a permutation of $Z(p-1)\times(q-1)$

c) d is the multiplicative inverse of e mod-$(p-1)\cdot(q-1)$

Note: If you say that d is not unique and you give examples of different d's, then also you will get full points.

---

5. [4 points]

1- writing something

2,3,4- a)Let s_1 be the signature of m_1, i.e., $s_1 = m_1^d$ mod-n.

Let s_2 be the signature of m_2, i.e., $s_2 = m_2^d$ mod-n.

Signature(m_1^j) = s_1^j mod-n

Signature(m_1^{-1}) = s_1^{-1} mod-n , assuming m_1^{-1} exists.

b)Signature($m_1 \cdot m_2$) = $s_1 \cdot s_2$ mod-n [because $(m_1 \cdot m_2)^d$ mod-n = $(m_1^d)\cdot(m_2^d)$ mod-n].

c)Signature($m_1^j \cdot m_2^k$) = $s_1^j \cdot s_2^k$ mod-n [from above].

---

6 [3 points] (Correct answer without explanation will lose points.)

a)25 = $(11001)_2$ [25 = 16 + 8 + 1]

b)$131^{(1)}$ mod-15 = 11

$131^{(10)}$ mod-15 = 11·11 mod-15 = 121 mod-15 = 1

$131^{(11)}$ mod-15 = 1·11 mod-15 = 11 mod-15 = 11

$131^{(110)}$ mod-15 = 11·11 mod-15 = 121 mod-15 = 1

$131^{(1100)}$ mod-15 = 1·1 mod-15 = 1

$131^{(11000)}$ mod-15 = 1·1 mod-15 = 1

$131^{(11001)}$ mod-15 = 1·11 mod-15 = 11

c)131^{25} mod-15 = 11

---

8. [3 points]

1- writing something

2- a)$\phi(p^a) = (p-1)\cdot p^{a-1}$ for p prime and a > 0

$\phi(p\cdot q) = \phi(p)\cdot\phi(q)$ for p and q relatively prime

b)If p_1 , p_2, ···, p_n, q are distinct primes, then $(p_1^{a1}\cdot p_2^{a2} \cdots p_n^{an})$ and q^b are relatively prime.

c) $\phi(p_1^{a1} \cdot p_2^{a2} \cdots p_k^{ak}) = (p_1-1)\cdot p_1^{a1-1} \cdot (p_2-1)\cdot p_2^{a2-1} \cdots (p_k-1)\cdot p_k^{ak-1}$

---

9 [2 points]

2- correct answer

---

11. [4 points]

a) Applying the CRT to z_1 and z_2 yields the following:

- Let a and b satisfy $1 = a \cdot z_1 + b \cdot z_2$ [a and b can be computed by Euclid(z_1, z_2)]
- Let $p = [\ x_2 \cdot a \cdot z_1 + x_1 \cdot b \cdot z_2\ ] \bmod z_1 \cdot z_2$
- Then p mod-z_1 = x_1 and p mod-z_2 = x_2

b)Applying the CRT to $z_1 \cdot z_2$ and z_3 yields the following:

- Let c and d satisfy $1 = c \cdot (z_1 \cdot z_2) + d \cdot z_3$ [c and d can be computed by Euclid($z_1 \cdot z_2$, z_3)]
- Let $q = [\ p \cdot c \cdot (z_1 \cdot z_2) + x_3 \cdot d \cdot z_3\ ] \bmod z_1 \cdot z_2 \cdot z_3$
- Then q mod-($z_1 \cdot z_2$) = p and q mod-z_3 = x_3

Thus q is the number x we want.

c)In summary, $x = [\ p \cdot c \cdot (z_1 \cdot z_2) + x_3 \cdot d \cdot z_3\ ] \bmod z_1 \cdot z_2 \cdot z_3$ where

- $p = [\ x_2 \cdot a \cdot z_1 + x_1 \cdot b \cdot z_2\ ] \bmod z_1 \cdot z_2$
- c and d satisfy $1 = c \cdot (z_1 \cdot z_2) + d \cdot z_3$
- a and b satisfy $1 = a \cdot z_1 + b \cdot z_2$

Note: For problem 5 and problem 11, giving the final answer with no explanation is ok.