

Fall 2006 CMSC 414: HW 2 Grading Key

Total 7 points

4. [4 points]

1- writing something

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

Let s_2 be the signature of m_2 , i.e., $s_2 = m_2^d \pmod{n}$.

Signature(m_1^j) = $s_1^j \pmod{n}$

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

b) Signature($m_1 \cdot m_2$) = $s_1 \cdot s_2 \pmod{n}$

[because $(m_1 \cdot m_2)^d \pmod{n} = (m_1^d) \cdot (m_2^d) \pmod{n}$].

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

7. [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, \dots, p_n, q are distinct primes,

then $(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n})$ and q^b are relatively prime.

c) $\phi(p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}) = (p_1-1) \cdot p_1^{a_1-1} \cdot (p_2-1) \cdot p_2^{a_2-1} \cdots (p_k-1) \cdot p_k^{a_k-1}$
