

## CMSC 414: HW 2

- 
1. (text 5.1) Would it be reasonable to compute an RSA signature on a long message  $m$  by signing  $m \bmod n$  (i.e., using  $(m \bmod n)^d \bmod n$  as the signature).

---

  2. (text 5.6) Why do MD4, MD5, and SHA-1 require padding of messages that are already a multiple of 512-bits?

---

  3. (text 6.3) In RSA, is it possible for more than one  $d$  to work with a given  $e$ ,  $p$ , and  $q$ ?

---

  4. (text 6.8) Given your RSA signature on  $m_1$  and  $m_2$ , how can one compute your signature on  $m_1^j \cdot m_2^k$  for any positive integers  $j$  and  $k$ .

---

  5. Using the efficient algorithm, compute  $131^{25} \bmod 15$ .

---

  6. (text 7.1) If  $m$  and  $n$  are two positive integers, show that  $m/\gcd(m,n)$  and  $n/\gcd(m,n)$  are relatively prime.

---

  7. (text 7.10) If  $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$  where  $p_i$  is prime, what is  $\phi(n)$ .

---

  8. Find all the square roots mod-15 of 1, i.e., every  $x$  in  $Z_{15}$  such that  $x \cdot x \bmod 15 = 1$ .

---

  9. Find all the square roots mod-24 of 1.

---

  10. Given positive integers  $z_1, z_2, z_3, x_1, x_2, x_3$ , such that  $z_1, z_2, z_3$  are relatively prime, obtain a formula that yields a number  $x$  in  $Z_{z_1 \cdot z_2 \cdot z_3}$  such that
    - $x \bmod z_1 = x_1$
    - $x \bmod z_2 = x_2$
    - $x \bmod z_3 = x_3$
-