

CMSC 414: HW 2 Solution and Grading

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).

No. Recall that RSA restricts the message to be signed to be smaller than n .

If m is larger than n , then message m and message $(m \bmod n)$ would have the same signature. So it would be easy to generate different messages that have the same signature.

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

Otherwise it would be easy to find two messages with the same hash. Let M' be any message that is not a multiple of 512 bits. Let M be M' padded as in MD4, so M is a multiple of 512 bits. If no padding is used for M (because it is a multiple of 512 bits) then $\text{MD4}(M)$ would be the same as $\text{MD4}(M')$.

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

Because d is the multiplicative inverse of $e \bmod (p-1)(q-1)$, it is unique modulo $(p-1)(q-1)$. [Recall e has a multiplicative inverse $\bmod (p-1)(q-1)$ iff e is relatively prime to $(p-1)(q-1)$. So multiplying the elements of $Z_{(p-1)(q-1)}$ by e results in a permutation of $Z_{(p-1)(q-1)}$, so there is only one element in $Z_{(p-1)(q-1)}$ which yields 1 when multiplied by e .]

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 .

Let s_1 be the signature of m_1 , i.e., $s_1 = m_1^d \bmod n$.

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

Signature(m_1^j) = $s_1^j \bmod n$ [because $(m_1^j)^d \bmod n = (m_1^d)^j \bmod n$].

Signature(m_1^{-1}) = $s_1^{-1} \bmod n$ [because $(m_1^{-1})^d \bmod n = (m_1^d)^{-1} \bmod n$], assuming m_1^{-1} exists.

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

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

5. Using the efficient algorithm, compute 131^{25} mod-15 .

$$\begin{aligned}
 25 &= (11001)_2 && [25 = 16 + 8 + 1] \\
 131^{(1)} \text{ mod-15} &= 11 \\
 131^{(10)} \text{ mod-15} &= 11 \cdot 11 \text{ mod-15} = 121 \text{ mod-15} = 1 \\
 131^{(11)} \text{ mod-15} &= 1 \cdot 11 \text{ mod-15} = 11 \text{ mod-15} = 11 \\
 131^{(110)} \text{ mod-15} &= 11 \cdot 11 \text{ mod-15} = 121 \text{ mod-15} = 1 \\
 131^{(1100)} \text{ mod-15} &= 1 \cdot 1 \text{ mod-15} = 1 \\
 131^{(11000)} \text{ mod-15} &= 1 \cdot 1 \text{ mod-15} = 1 \\
 131^{(11001)} \text{ mod-15} &= 1 \cdot 11 \text{ mod-15} = 11 \\
 \text{So } 131^{25} \text{ mod-15} &= 11
 \end{aligned}$$

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

By Euclid's algorithm, there exist integers u and v such that $u \cdot m + v \cdot n = \text{gcd}(m,n)$.
 Dividing both sides by $\text{gcd}(m,n)$ gives $u \cdot (m/\text{gcd}(m,n)) + v \cdot (n/\text{gcd}(m,n)) = 1$.
 So by Euclid algorithm, $m/\text{gcd}(m,n)$ and $n/\text{gcd}(m,n)$ are relatively prime (note that both are integers by definition of gcd).

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 $\phi(n)$.

We have already established the following:

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

We also have that if p_1, p_2, \dots, p_n, q are distinct primes, then $(p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_n^{a_n})$ and q^b are relatively prime.

Hence by induction

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

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

$$1^2 \text{ mod-15} = 1$$

$$2^2 \text{ mod-15} = 4$$

$$3^2 \text{ mod-15} = 9$$

$$4^2 \text{ mod-15} = 16 \text{ mod-15} = 1$$

$$5^2 \text{ mod-15} = 25 \text{ mod-15} = 10$$

$$6^2 \text{ mod-15} = 36 \text{ mod-15} = 6$$

$$7^2 \text{ mod-15} = 49 \text{ mod-15} = 3$$

$$8^2 \text{ mod-15} = 64 \text{ mod-15} = 4$$

$$9^2 \text{ mod-15} = 81 \text{ mod-15} = 6$$

$$10^2 \text{ mod-15} = 100 \text{ mod-15} = 10$$

$$11^2 \text{ mod-15} = 121 \text{ mod-15} = 1$$

$$12^2 \text{ mod-15} = 144 \text{ mod-15} = 9$$

$$13^2 \text{ mod-15} = 169 \text{ mod-15} = 4$$

$$14^2 \text{ mod-15} = 196 \text{ mod-15} = 1$$

So the square roots mod-15 of 1 are $\{1, 4, 11, 14\}$

[Check: $15 = 2^0 \cdot 3 \cdot 5$. So the formula at the end of section 7.5 tells us that there are 2^2 square roots mod-15 of 1.]

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

Before going through the numbers in Z_{24} , let's use the formula at the end of section 7.5 to see how many square roots there are. $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$, so there are 2^3 square roots.

- $1 \cdot 1 \text{ mod-24} = 1$
- $23 \cdot 23 \text{ mod-24} = 529 \text{ mod-24} = 1$
- $5 \cdot 5 \text{ mod-24} = 25 \text{ mod-24} = 1$.
- $7 \cdot 7 \text{ mod-24} = 49 \text{ mod-24} = 1$.
- $11 \cdot 11 \text{ mod-24} = 121 \text{ mod-24} = 1$
- $13 \cdot 13 \text{ mod-24} = 169 \text{ mod-24} = 1$
- $17 \cdot 17 \text{ mod-24} = 289 \text{ mod-24} = 1$
- $19 \cdot 19 \text{ mod-24} = 361 \text{ mod-24} = 1$

So the roots are 1, 5, 7, 11, 13, 17, 19, 23.

[Can one restrict the search to Z_n^* ?

Is $1 \cdot 1 \text{ mod-n} = 1$ for any n ?

Is $(n-1) \cdot (n-1) \text{ mod-n} = 1$ for any n ?]

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

$$x \bmod z_1 = x_1$$

$$x \bmod z_2 = x_2$$

$$x \bmod z_3 = x_3$$

The Chinese remainder theorem shows us that there is exactly one such x and how to compute it.

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 $\text{Euclid}(z_1, z_2)$]
- Let $p = [x_2 \cdot a \cdot z_1 + x_1 \cdot b \cdot z_2] \bmod z_1 \cdot z_2$
- Then $p \bmod z_1 = x_1$ and $p \bmod z_2 = x_2$

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 $\text{Euclid}(z_1 \cdot z_2, z_3)$]
- 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 $q \bmod (z_1 \cdot z_2) = p$ and $q \bmod z_3 = x_3$

Thus q is the number x we want.

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 $1 = a \cdot z_1 + b \cdot z_2$
-