# SOLUTION AND GRADING KEY

**Total points: 30. Total time: 115 minutes. 4 problems over 4 pages. No book, notes, or calculator**

**1. [10 points]**
Suppose Bob uses RSA with n=77 and e=5.
Are these valid numbers for RSA. Explain.
If you answer yes, obtain the corresponding d.

---

There are two requirements:

- n must be a product of two primes [1 point]
- e must be relatively prime to $\phi(n)$ (so that d, which equals $e^{-1}$ mod-n, exists) [1 point]

**First requirement [2 points]**
$n = 77 = 7 \cdot 11$. 7 and 11 are primes. So this holds.

**Second requirement [6 points]**
Recall that if $n = p_1^{a1} \cdot p_2^{a2} \cdots p_k^{ak}$ where $p_i$ is prime, then
$\phi( p_1^{a1} \cdot p_2^{a2} \cdots p_k^{ak} ) = (p_1-1) \cdot p_1^{a1-1} \cdot (p_2-1) \cdot p_2^{a2-1} \cdots (p_k-1) \cdot p_k^{ak-1}$

So $\phi(77) = (7-1)\cdot(11-1) = 60$.
e, which equals 5, is not relatively prime to 60.
So this requirement does not hold.

So these are not valid RSA numbers.

---

**2. [5 points]**
Assume that Bob uses RSA and the following hold:

- n=15
- Bob's signature of message m=2 is 5
- Bob's signature of message m=3 is 4

Obtain Bob's signature for the message m=12. Show your derivation here.

---

Recall that if $s_1$ is the signature of $m_1$ (i.e., $s_1 = m_1^d$ mod-n) and $s_2$ is the signature of $m_2$, then

- signature($m_1^j$) = $s_1^j$ mod-n,
- Signature($m_1 \cdot m_2$) = $s_1 \cdot s_2$ mod-n
- signature($m_1^j \cdot m_2^k$) = $s_1^j \cdot s_2^k$ mod-n

So we express message m=12 in terms of 2 and 3.
12 = 2·2·3 **[2 points]**
So signature(12) = signature(2)·signature(2)·signature(3) mod-15
= 5·5·4 mod-15
= 100 mod-15
= 10 (because 15·6 = 90)
So signature(12) = 10 **[3 points]**

---

**3. [5 points]**
How many numbers between 1 and 250000 are relatively prime to 250000? Explain

---

By definition, this equals $\phi(250000)$. [1 point]

Recall that if $n = p_1^{a1} \cdot p_2^{a2} \cdot\cdot\cdot p_k^{ak}$ where $p_i$ is prime, then
$\phi(p_1^{a1} \cdot p_2^{a2} \cdot\cdot\cdot p_k^{ak}) = (p_1-1)\cdot p_1^{a1-1} \cdot (p_2-1)\cdot p_2^{a2-1} \cdots (p_k-1)\cdot p_k^{ak-1}$

$250000 = 5\cdot5\cdot10000 = 5^2 \cdot 10^4 = 5^2 \cdot (5\cdot2)^4 = 5^6\cdot2^4$
So $\phi(250000) = (4\cdot5^5) \cdot (1\cdot2^3) = (4\cdot25\cdot25\cdot5) \cdot (1\cdot8) = 100\cdot25\cdot5\cdot8 = 100\cdot5\cdot200 = 100\cdot1000 = 100{,}000$

So there are 100000 numbers between 1 and 250000 that are relatively prime to 250000.

---

**4. [10 points]**
Using the efficient algorithm, compute $131^{25}$ mod-15

---

$25 = (11001)_2$ [25 = 16 + 8 + 1]
$131^{(1)}$ 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
So $131^{25}$ mod-15 = 11

---

**5. [10 points]**
Obtain a formula that yields a number x in $Z_{45}$ such that x mod-5 = $x_1$ and x mod-9 = $x_2$.
Or if you think such a formula does not exist, explain.

---

Note that 45 = 5·9 and that 5 and 9 are relatively prime.
Thus the CRT tells us that there is a unique x for any $x_1$ and $x_2$ and gives the formula
$x = [\, x_2 \cdot a \cdot z_1 + x_1 \cdot b \cdot z_2 \,] \bmod z_1 \cdot z_2$ where $a \cdot z_1 + b \cdot z_2 = 1$ (in this case, $z_1 = 5$ and $z_2 = 5$).
[4 points]

So the formula is $x = [\, x_2 \cdot a \cdot 5 + x_1 \cdot b \cdot 9 \,] \bmod 5 \cdot 9$, where a and b satisfy $a \cdot 5 + b \cdot 9 = 1$.
Doing Euclid(5,9) yields a and b, but in this case we can also do it by "brute force".
Because a·5 ends in 0 or 5 and hits all such numbers, it suffices if b·9 ends in 1 or 6.
[3 points]

So b=4 works. In this case, b·9 = 36, so a = –7 works [check: $(-7) \cdot 5 + 4 \cdot 9 = -35 + 36 = 1$].
So one valid formula is

$x = [\, x_2 \cdot (-7) \cdot 5 + x_1 \cdot 4 \cdot 9 \,] \bmod 5 \cdot 9$, or
$x = [\, -x_2 \cdot 35 + x_1 \cdot 36 \,] \bmod 45$

Or
b=9 also works. In this case, a= –16 [check: $(-16) \cdot 5 + 9 \cdot 9 = -80 + 81 = 1$].
So another valid formula is

$x = [\, x_2 \cdot (-16) \cdot 5 + x_1 \cdot 9 \cdot 9 \,] \bmod 5 \cdot 9$, or
$x = [\, -x_2 \cdot 80 + x_1 \cdot 81 \,] \bmod 45$

Or
b= –1 also works. In this case, a= 2 [check: $2 \cdot 5 + (-1) \cdot 9 = 10 + (-9) = 1$].
So another valid formula is

$x = [\, x_2 \cdot 2 \cdot 5 + x_1 \cdot (-1) \cdot 9 \,] \bmod 5 \cdot 9$, or
$x = [\, x_2 \cdot 10 - x_1 \cdot 81 \,] \bmod 45$ [3 points]

There are of course many more (a,b) pairs that will work.

---