CMSC 456 Final, Fall 2019- VERSION C

1. This is a closed book exam, although one sheet of notes is allowed. **You CANNOT use a calculator**. If you have a question during the exam, please raise your hand.
2. There are 6 problems which add up to 100 points; however, the first one is to **Print Your Name Neatly On Every Sheet** so that hardly counts. The exam is 2 hours long.
3. In order to be eligible for as much partial credit as possible, show all of your work for each problem, **write legibly**, and **clearly indicate** your answers. Credit **cannot** be given for illegible answers.
4. After the last page there is paper for scratch work.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

Fill in the following:

Print your Name Neatly Here:
SIGNATURE:
SID:

1. (If you do not do this we will subtract 5 points from your score)

   On every page of this exam there is a line that says:

   Print Your Name Neatly Here:

   You must do that.

   Hint: do it NOW. In the past students have said *I'll do that later* and then forget and they *lose 5 points*. Don't be that person! Really!

Print Your Name Neatly Here:

2. (20 points)

   (a) (6 points) Describe RSA, both encryption and decryption.

   (b) Alice and Bob are going to use RSA with $N = 15$ and $e = 3$.

      i. (7 points) What value of d does Alice use? Show your work. (You may use that $15 = 3 \times 5$.)

      ii. (7 points) Bob wants to send 7. What does he send? Give the actual number and NOT something like $\binom{7}{3}$. Show your work. (You may NOT use that $15 = 3 \times 5$.)

Print Your Name Neatly Here:

ANSWER

We omit the description of RSA.

Note that $N = 15 = 3 \times 5$ so $R = 2 \times 4 = 8$. Hence we need to know the inverse of 3 mod 8. That's just 3. So $d = 3$.

To send 7 Bob sends $7^3 \pmod{15}$. He sends

$7 \times 7 \times 7 \pmod{15}$.

$7 \times 49 \equiv 7 \times 4 \equiv 28 \equiv 13 \pmod{15}$

So Bob sends 13.

END OF ANSWER

3. (20 points)

A1, A2, A3, A4 have cards similar to those used in the Alice-Bob-Cards-Dating lecture. (e.g., hearts, spades, uparrows, make them clear, make them opaque, make them fit into pez dispensers). A1 has a bit a_1, A2 has a bit a_2, A3 has a bit a_3, A4 has a bit a_4. They want to compute $a_1 \wedge a_2 \wedge a_3 \wedge a_4$ such that

(a) At the end they ALL know $a_1 \wedge a_2 \wedge a_3 \wedge a_4$.

(b) At the end a_1 only knows a_1 (of course), $a_1 \wedge a_2 \wedge a_3 \wedge a_4$, and what can be deduced from these. So

i. If $a_1 = 0$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 0$ then A1 knows nothing about a_2 or a_3 or a_4.

ii. If $a_1 = 0$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 1$ THIS CANNOT HAPPEN.

iii. If $a_1 = 1$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 0$ then A1 knows $a_2 = 0$ or $a_3 = 0$ or $a_4 = 0$, but does not know which of those happens.

iv. If $a_1 = 1$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 1$ then A1 knows $a_2 = 1$ and $a_3 = 1$ and $a_4 = 1$.

(c) Similar for A2, A3, and A4.

And now **finally** the problem: Give a protocol for A_1, A_2, A_3, A_4 to use that achieves the above conditions. Recall that they can use cards.

Hint: Use a variant of one of the schemes discussed in the Alice-Bob-Cards-dating lecture

Do this on the next page

Print Your Name Neatly Here:

SOLUTION OMITED.

Variants of the Opaque card solution OR of the Pez-disp solution OR of the enter-and-exit-the-room solution worked.

DO PROBLEM HERE

Print Your Name Neatly Here:

4. (20 points) Zelda is going to send messages to Alice1, Alice2, and Alice3 using RSA.

   Zelda and Alice1 use $N = 51$ and $e_1 = 6$.

   Zelda and Alice2 use $N = 51$ and $e_2 = 15$.

   Zelda and Alice3 use $N = 51$ and $e_3 = 25$.

   Zelda sends Alice1 message m by sending c_1. (c_1 is rel prime to 51.)

   Zelda sends Alice2 message m by sending c_2. (c_2 is rel prime to 51.)

   Zelda sends Alice3 message m by sending c_3. (c_3 is rel prime to 51.)

   You may want to use the following information

   Combinations of 15 and 25

a	b	$15a + 25b$
1	1	40
1	2	65
1	3	90
2	1	55
2	2	80
2	3	105
3	1	70
3	2	95
3	3	120

   Times Table for 6

6×1	6
6×2	12
6×3	18
6×4	24
6×5	30
6×6	36
6×7	42
6×8	48
6×9	54

   The PROBLEM is on the next page

   Print Your Name Neatly Here:

The Problem:

Write m as an easily computed function of c_1 and c_2 and c_3.

Your solution should NOT rely on being able to factor 51.

Use this page and if needed the next page which is blank.

Print Your Name Neatly Here:

Extra Space for Problem 3 if Needed

Print Your Name Neatly Here:

ANSWER VERSION A

If Zelda sends m to both Alice1 and Alice2 and Alice3 then Eve sees:

Alice1 get $c_1 = m^6 \pmod{51}$

Alice2 get $c_2 = m^{15} \pmod{51}$

Alice3 get $c_3 = m^{25} \pmod{51}$

Note using the table I gave you that

$$-9 \times 6 + 2 \times 15 + 1 \times 25 = 1.$$

Eve now computes, all mod 51:

$$(m^{-6})^9 \times (m^{15})^2 \times (m^{25})^1 \equiv m^{-54+55} \equiv m.$$

So m is just

$$(c_1^{-1})^9 \times (c_2)^2 \times (c_3)^1 \pmod{51}$$

Note: There are other solutions based on other combinations that equal 1. Here is one:

$$16 \times 6 - 3 \times 15 - 2 \times 25 = 1$$

Eve now computes, all mod 51:

$$(m^6)^{16} \times (m^{-15})^3 \times (m^{-25})^2 \equiv m^{96-45-50} = m$$

$$c_1^{16} \times (c_2^{-1})^3 \times (c_3^{-1})^{50} = m$$

ANOTHER ONE: Use $25 - 6 \times 4 = 1$.

ANSWER VERSION B

We first state Version B:

Zelda is going to send messages to Alice1, Alice2, Alice3 using RSA.

Zelda and Alice1 use $N = 51$ and $e_1 = 15$.

ANOTHER ONE: Use $25 - 6 \times -4 = 1$.

Zelda and Alice2 use $N = 51$ and $e_2 = 25$.

Zelda and Alice3 use $N = 51$ and $e_3 = 9$.

Zelda sends Alice1 message m by sending c_1. (You can assume that c_1 is rel prime to 51.)

Zelda sends Alice2 message m by sending c_2. (You can assume that c_2 is rel prime to 51.)

Zelda sends Alice3 message m by sending c_3. (You can assume that c_3 is rel prime to 51.)

Combinations of 15 and 25

a	b	$15a + 25b$
1	1	40
1	2	65
1	3	90
2	1	55
2	2	80
2	3	105
3	1	70
3	2	95
3	3	120

Times Table for 9

9×1	9
9×2	18
9×3	27
9×4	36
9×5	45
9×6	54
9×7	63
9×8	72
9×9	81

Use that

$-9 \times 6 + 2 \times 15 + 1 \times 25 = 1.$

END OF ANSWER

5. (20 points) Eve wants to factor N which we will assume is large. Eve does the quadratic sieve method with parameters B and M. But she made a mistake! Here is what she did:

   - $x \leftarrow \lceil N^{1/3} \rceil$.
   - For $0 \leq i \leq M$ compute $(x+i)^3 \pmod{N}$ and try to B-factor it.

   And now for our PROBLEM:

   Describe how Eve can try to use these B-factorings to find a non-trivial factor of N.

   Eve also knows that, for all a, b, $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.

   Print Your Name Neatly Here:

ANSWER

We have:

$$\begin{array}{rll} (x+0)^3 \equiv y_0 & (\text{mod } N). & \text{Try to } B\text{-Factor } y_0 \\ (x+1)^3 \equiv y_1 & (\text{mod } N). & \text{Try to } B\text{-Factor } y_1 \\ & \vdots & \vdots \\ (x+M)^3 \equiv y_M & (\text{mod } N). & \text{Try to } B\text{-Factor } y_M \end{array}$$

In the Quad Sieve Eve formed *parity vectors*. Here instead Eve will form *thrarity vectors*, which are the exponents mod 3. NOTE: the entries will be $0, 1, 2$, NOT $0, 1$.

Eve tries to find a set I such that (1) every $i \in I$ is such that $(x+i)^3$ was B-factored, and (2) the sum of the tharity vectors MOD 3 is $\vec{0}$. Formally:

Let the linear combination be $\sum_{i=1}^{B} c_i \vec{v}_i = 0$ where $c_i \in \{0, 1, 2\}$ and we do the arithmetic mod 3.

Hence we have that $\prod_{i=1}^{B} y_i^{c_i}$ is a cube. Call it X^3. Note also that

$y_i \equiv (x+i)^3$, so the product mod N is also a cube, call it Y^3. Now we have

$$X^3 - Y^3 \equiv 0 \pmod{N}.$$

$$(X-Y)(X^2+XY+Y^2) \equiv 0 \pmod{N}$$

$GCD(N, X-Y)$ or $GCD(N, X^2+XY+Y^2)$ probably yields a non-trivial factor.

END OF ANSWER

6. (20 points) Zelda is going to (4,4) secret share with Alice1, Alice2, Alice3, Alice4. The secret is an element $s \in \{0, 1, 2, 3, 4\}$. She is going to use mod 5. Normally Zelda would do the following:

   Generate random $r_3, r_2, r_1 \in \{0, 1, 2, 3, 4\}$. *Let*

   $$f(x) = r_3x^3 + r_2x^2 + r_1x + s.$$

   Give

   Alice1 $f(1) \pmod 5$

   Alice2 $f(2) \pmod 5$

   Alice3 $f(3) \pmod 5$, *and*

   Alice4 $f(4) \pmod 5$,

   but Zelda does not want to generate three random numbers. She just wants to generate one. So she does the following:

   Generate random $r \in \{0, 1, 2, 3, 4\}$. *Let* $f(x) = rx^3 + s$. *Give*

   Alice1 $f(1) \pmod 5$,

   Alice2 $f(2) \pmod 5$,

   Alice3 $f(3) \pmod 5$, *and*

   Alice4 $f(4) \pmod 5$.

   And now **FINALLY** our question.

   Zelda does secret sharing her way, over mod 5.

   Alice1 gets 1, Alice2 gets 0, Alice3 gets 3, Alice4 gets 2

   (a) (10 points) Can Alice1 working alone determine the secret? If not then can Alice1 working alone determine ANYTHING about the secret (e.g., it's not 1)? Explain your answer and show your work.

   ANSWER: Alice1 has $f(1) = 1 \pmod 5$. So Alice1 only knows that

   $$f(1) \equiv r \times 1^3 + s \pmod 5$$

   $$1 \equiv r + s \pmod 5$$

The possibilities for (r, s) are $(0, 1)$, $(1, 0)$, $(2, 4)$, $(3, 3)$, $(4, 2)$. Hence s can be ANYTHING so Alice1 can determine NOTHING about the secret.

(b) (10 points) Can Alice1 and Alice2 together determine the secret? If not then can Alice1 and Alice2 together determine ANYTHING about the secret (e.g., it's not 1)? Explain your answer and show your work.

ANSWER: They can determine the secret! Together they know

$1 \equiv r + s \pmod 5$

$0 \equiv 3r + s \pmod 5$

So they know that $2r \equiv -1 \equiv 4$, so $r = 2$. Since $r + s \equiv 1$, $s = 4$. So they actually find out the secret!

PUT YOUR ANSWER ON THE NEXT PAGE

Print Your Name Neatly Here:

WRITE YOUR ANSWER TO THE PROBLEM HERE
USE NEXT PAGE IF YOU NEED TO

Print Your Name Neatly Here:

EXTRA PAGE IF YOU NEED IT

Print Your Name Neatly Here:

Scratch Paper

DO NOT DETACH THIS PAPER!!!! IF you detach this page then you lose 5 points

Print Your Name Neatly Here:

More Scratch Paper

DO NOT DETACH THIS PAPER!!!! IF you detach this page then you lose 5 points

Print Your Name Neatly Here: