# CMSC 456 Midterm, 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 5 problems which add up to 100 points. The exam is 75 minutes.
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.*"
6. Fill in the following:

NAME :
SIGNATURE :
UID :

1. (20 points) Plutonians are about to choose an alphabet size. Let $n \in \mathbb{N}$. Assume they choose alphabet size $n$. Then let prob($n$) be the probability that if they pick a random $a \in \{0, \ldots, n-1\}$ then it will be rel prime to $n$.

   (a) The Plutonians want to pick an $n$ such that prob($n$) is large. They say it will be good for their cryptosystems. What cryptosystem are they likely using? Justify your answer.

   (b) Let $p$ be a prime.

      i. What is prob($p$)? Express in terms of $p$ with $+, -, \div, \times$. For example, you can't use a symbol like $\pi(p)$ (thats the number of primes $\le p$).

      ii. What is prob($p^2$)? Express in terms of $p$ with $+, -, \div, \times$. For example, you can't use a symbol like $\pi(p)$ (thats the number of primes $\le p$).

      iii. What is prob($p^3$)? Express in terms of $p$ with $+, -, \div, \times$. For example, you can't use a symbol like $\pi(p)$ (thats the number of primes $\le p$).

   (c) The Plutonians want to use either $p$, $p^2$, or $p^3$ as their alphabet size. What is your advice? You can tell them either which one to use, or that two of them are equally good, or that all three are equally good, or that they should use (for example) BLAH if $p \le 37$ but BLAH BLAH if $p > 37$ (that is, that it depends on $p$). But in any case, justify your answer.

**Answer this question on the NEXT page.**

**WRITE YOUR SOLUTION TO PROBLEM ONE ON THIS PAGE**

## SOLUTION TO PROBLEM 1- VERSION A

Plutonians are about to choose an alphabet size. Let $n \in \mathbb{N}$. Assume they choose alphabet size $n$. Then let prob($n$) be the probability that if they pick a random $a \in \{0, \ldots, n-1\}$ then it will be rel prime to $n$.

(a) The Plutonians what to pick an $n$ such that prob($n$) is large. They say it will be good for their cryptosystems. What cryptosystem are they likely using? Justify your answer.

**ANSWER** They want to use an affine cipher and this makes picking $a$ easier since the prob that $a$ is rel prime to $n$ is higher.

(b) Let $p$ be a prime.

i. What is prob($p$)?
**ANSWER** $\frac{\phi(p)}{p} = \frac{p-1}{p}$.

ii. What is prob($p^2$)?
**ANSWER** $\frac{\phi(p^2)}{p^2} = \frac{p^2-p}{p^2} = \frac{p-1}{p}$.

iii. What is prob($p^3$)?
**ANSWER** $\frac{\phi(p^3)}{p^3} = \frac{p^3-p^2}{p^3} = \frac{p-1}{p}$.

(c) Of $n = p$, $n = p^2$, $n = p^3$, What is the best (or if there is a tie, the 2 best or 3 best) value of $n$ to use to maximize prob($n$)?

**ANSWER** They are all equal.

## SOLUTION TO PROBLEM 1- VERSION B

Plutonians are about to choose an alphabet size. Let $n \in \mathbb{N}$. Assume they choose alphabet size $n$. Then let prob($n$) be the probability that if they pick a random $a \in \{0, \ldots, n-1\}$ then it will be rel prime to $n$.

(a) The Plutonians want to pick an $n$ such that prob($n$) is large. They say it will be good for their cryptosystems. What cryptosystem are they likely using? Justify your answer.

**ANSWER** They want to use an affine cipher and this makes picking $a$ easier since the prob that $a$ is rel prime to $n$ is higher.

(b) Let $p < q < r$ be primes.

i. What is prob($p$)?
**ANSWER** $\frac{\phi(p)}{p} = \frac{p-1}{p}$.

ii. What is prob($pq$)?
**ANSWER** $\frac{\phi(pq)}{pq} = \frac{(p-1)(q-1)}{pq}$.

iii. What is prob($pqr$)?
**ANSWER** $\frac{\phi(pqr)}{p^3} = \frac{(p-1)(q-1)(r-1)}{pqr}$.

### Problem 1 Grading (Version A)

Problem 1 has 3 parts that were graded separately.

(a) **7 points**. Students received all points for submitting the correct answer (Affine), and no points for any other answer. No explanations changed the grade.

(b) **6 points**. This problem was broken into 3 parts i-iii each generally worth 2 points. Common mistakes:

1. Some students got i wrong by saying that there are no values below $p$ that share a common factor with $p$. This misses 0. I gave them $-2$.
2. Many students got ii and iii incorrectly. This was either due to incorrectly applying $\phi$ (ie, saying $\phi(p^2) = (p-1)^2$) or because they attempted to do a counting argument, and said something like "0 and $p$ are the only factors of $p^2$ in the range" which, of course, misses multiples of $p$ like $2p$, $3p$, etc. This received a $-4$.
3. Finally, a number of students divided by $p-1$ instead of $p$ (ie, they forgot to include 0 in the count for the denominator). This resulted in incorrect answers for all parts, but I only took of $-1$ per part for a total of $-3$.

(c) This part was graded more leniently. It was all or nothing, and I included cascade error. For correct solution to (b), the answer should be all are equally good. For the last 2 errors mentioned in part (b), this resulted in $p$ being the best option. Some made the argument that if $p$ is small then they should pick $p^2$ or $p^3$, this is fine. If they had a more significant error, there perhaps was not as much to work off of to answer (c), so I accepted answers that were based off of making the key space larger and thus harder to brute force.

**Problem 1 Grading (Version A)**

Much of what was said for Version A holds for Version B as well. We note one mistake particular to Version B.

For Version B some students got ii and iii incorrect by saying $\phi(pq) = pq$ and $\phi(pqr) = pqr$ instead of $\phi(pq) = \phi(p)\phi(q)$ and $\phi(pqr) = \phi(p)\phi(q)\phi(r)$.

**END OF SOLUTION TO PROBLEM ONE**

2. (20 points) Alice and Bob use a Matrix Cipher. They pick a value of $n$ such that (1) Eve cannot crack the matrix cipher by brute force, (2) Eve cannot crack the matrix cipher with a freq analysis, and (3) $n$ is small enough so that Alice and Bob can carry out the encryption.

   Show how, even with this nice value of $n$, Eve can still crack the cipher in a real world situation.

## SOLUTION TO PROBLEM TWO VERSIONS A AND B

Eve can crack it given that she has prior messages and what they decoded to.

The $M$ matrix has $n^2$ entries.

If Eve knows $n^2$ messages and how they got coded (e.g., yesterday's messages) then she knows

$M(m_1) = c_1$

$M(m_2) = c_2$

$\vdots$

$M(m_{n^2}) = c_{n^2}$

From this she can set up $n^2$ linear equations in $n^2$ variables (the matrix entries) and solve them to find the matrix.

### Problem 2 GRADING

In order to receive credit for this problem, students needed to describe a PROCEDURE indicating how the matrix cipher can be cracked. This means that no credit is given for things like simply referencing weaknesses the NY,NY problem. Partial credit was given to those who had some right ideas but didn't describe their procedure thoroughly enough, or were unclear with some of their descriptions.

No credit was given for ideas that have nothing to do with the weaknesses of the matrix cipher in particular (e.g., bribery).

## END OF SOLUTION TO PROBLEM TWO VERSIONS

3. (20 points) Recall the Blum-Goldwasser Encryption:

   Security parameter $L$. Message length $M$.

   (a) Alice generates $p, q$ primes length $L$, $p, q \equiv 3 \pmod 4$. $N = pq$. Send $N$ to everyone (so Bob and Eve both see it).

   (b) **Encode:** Bob wants to send $m \in \{0,1\}^M$. He does the following.

      i. Bob picks random $r \in \mathbb{Z}_N^*$

      ii. Bob computes:
      $x_1 = r^2 \mod N$ and $b_1 = LSB(x_1)$ (LSB is Least Significant Bit, rightmost bit.)
      $x_2 = x_1^2 \mod N \qquad b_2 = LSB(x_2)$.
      $\vdots$
      $x_{M+1} = x_M^2 \mod N \qquad b_{M+1} = LSB(x_{M+1})$.

      iii. Bob sends $c = ((m_1 \oplus b_1, \ldots, m_M \oplus b_M), x_{M+1})$. (NOTE- Alice and Eve both see $c$.)

   (c) **Decode** Alice: From $x_{M+1}$ Alice can compute $x_M$, ..., $x_1$ by sqrt (can do since Alice has $p, q$). Then she can compute $b_1, \ldots, b_M$ and hence $m_1, \ldots, m_M$.

   **And now for the question:**

   Alice and Bob have an idea! They want to only compute $x_1, \ldots, x_M$ (so NOT $x_{M+1}$) and then have Bob send

$$c = ((m_1 \oplus b_1, \ldots, m_M \oplus b_M), x_M).$$

   Tell them why this is a bad idea.

   **Answer this question on the NEXT page.**

**WRITE YOUR SOLUTION TO PROBLEM THREE ON THIS PAGE**

## SOLUTION TO PROBLEM THREE VERSION A

Eve has $x_M$. Hence Eve has $b_M$.

Eve also has $m_M \oplus b_M$.

Eve can compute

$$(m_M \oplus b_M) \oplus b_M = m_M$$

So Eve gets one bit of the message!

## SOLUTION TO PROBLEM THREE VERSION B

The only difference between version A and B was that we swapped the $M$ and the $L$. So the only diff in the answer is replacing $M$ with $L$:

Eve has $x_L$. Hence Eve has $b_L$.

Eve also has $m_L \oplus b_L$.

Eve can compute

$$(m_L \oplus b_L) \oplus b_L = m_L$$

So Eve gets one bit of the message!

## PROBLEM THREE GRADING

- If you stated that Eve can determine $m_M$ by computing $(m_M \oplus b_M) \oplus b_M$, where $b_M$ is just the last digit of $x_M$, then you get full credit.
- If you only gave false reasons that Alice and Bob's idea is bad, then you get zero credit. Occasionally there were submissions which gave false reasons and also included something that was vaguely on the track of the correct answer. These submissions were given 5 points.
    - Some people gave the correct answer and then incorrectly stated that Eve can continue the process in some way to find all of the $x_i$ values and decrypt the message. This is false, but no credit was removed. The final exam grading may be more strict.

- A common mistake was to say that Alice cannot decrypt the message anymore. This is not true, the first step in decryption is to compute $x_{M-1}$; if Bob sends $x + M - 1$ directly we can just skip that step and proceed with the rest of the decryption process.
- The other common mistake was to say that Eve can decrypt the entire message. This is in general false, and without further information Eve can only determine the final bit of the message.

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

Zelda and Alice1 use $N = 39$ and $e_1 = 7$.

Zelda and Alice2 use $N = 39$ and $e_2 = 11$.

Zelda sends Alice1 message $m$ by sending $c_1$. (You can assume that $c_1$ is rel prime to 39.)

Zelda sends Alice2 message $m$ by sending $c_2$. (You can assume that $c_2$ is rel prime to 39.)

You may want to use the following times-tables for 7 and 11.

| | |
|---|---|
| $7 \times 1$ | 7 |
| $7 \times 2$ | 14 |
| $7 \times 3$ | 21 |
| $7 \times 4$ | 28 |
| $7 \times 5$ | 35 |
| $7 \times 6$ | 42 |
| $7 \times 7$ | 49 |

| | |
|---|---|
| $11 \times 1$ | 11 |
| $11 \times 2$ | 22 |
| $11 \times 3$ | 33 |
| $11 \times 4$ | 44 |
| $11 \times 5$ | 55 |
| $11 \times 6$ | 66 |
| $11 \times 7$ | 77 |

**AND NOW THE PROBLEM:**

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

Your solution should NOT rely on being able to factor 39.

**Answer this question on the NEXT page.**

**WRITE YOUR ANSWER TO PROBLEM FOUR ON THIS PAGE**

## SOLUTION TO PROBLEM FOUR VERSION A

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

Alice1 get $c_1 = m^7 \pmod{39}$

Alice2 get $c_2 = m^{11} \pmod{39}$

Note that

$$11 \times 2 - 7 \times 3 = 1$$

Eve now computes, all mod 39:

$$(m^{11})^2 \times (m^{-7})^3 \equiv m^{22-21} \equiv m.$$

So $m$ is just

$$c_2^2 \times c_1^{-3} \pmod{39}$$

## SOLUTION TO PROBLEM FOUR VERSION B

We first state Version B:

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

Zelda and Alice1 use $N = 39$ and $e_1 = 8$.

Zelda and Alice2 use $N = 39$ and $e_2 = 13$.

Zelda sends Alice1 message $m$ by sending $c_1$. (You can assume that $c_1$ is rel prime to 39.)

Zelda sends Alice2 message $m$ by sending $c_2$. (You can assume that $c_2$ is rel prime to 39.)

You may want to use the following times-tables for 8 and 13 (omitted from this sol set).

And now the answer:

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

Alice1 get $c_1 = m^8 \pmod{39}$

Alice2 get $c_2 = m^{13} \pmod{39}$

Note that

$$13 \times 5 - 8 \times 8 = 1$$

Eve now computes, all mod 39:

$$(m^{13})^5 \times (m^{-8})^8 \equiv m^{65-64} \equiv m.$$

So $m$ is just

$$c_2^5 \times c_1^{-3} \pmod{39}.$$

**HOW IT WAS GRADED (Just Version A, Version B is similar)**

(a) If you had that Zelda sends Alice1 $m^7$ and Zelda sends Alice2 $m^{11}$ then you got 5 points.

(b) If you seem to know that you need a combo of 7 and 11 to add to 1, thats 5 points.

(c) If you assume you an factor 39 or can find $\phi(39)$ be factoring it, this is incorrect.

(d) If you use the Chinese Remainder Theorem, that is incorrect.

(e) If you had $\frac{c_2^2}{c_1^3} \pmod{39}$ I allowed it now but WILL NOT ALLOW THIS ON THE FINAL.

(f) If you had $c_2^2 - c_1^3 \pmod{39}$ but all of your work before then indicates that you really knew it was $c_2^2 c_1^{-3}$ then you got THE FULL 20 POINTS now but WILL NOT ALLOW THIS ON THE FINAL. $c_1^{11} + c_2^7$ is just wrong. (Some did $c_1^{11} + c_2^7$ which is just WRONG.)

(g) If you left out the $\pmod{39}$ then you still got FULL CREDIT now but WILL NOT ALLOW THIS ON THE FINAL.

(h) If you assumed that $m^{39} \equiv m \pmod{39}$ this is INCORRECT.

(i) General Warning: If I have a question like this on the FINAL it will be graded MUCH more harshly now that you now how to do it, and what NOT to do.

**COMMON MISTAKES**

(a) Assuming you can factor 39. I said you could not use that. (This is how I can have a crypto exam and not allow calculators.)

(b) If you computed $\phi(39)$ by factoring 39, that was wrong, since you can't factor.

(c) Using CRT. I think this means the students were doing a low-$e$ attack copied off of their cheat sheets rather than the same-$N$ attack copied off of their cheat sheets. More generally, do not just copy off of your cheat sheets. It does not work.

**END OF SOLUTION TO PROBLEM FOUR**

5. (20 points) For this problem you can assume there are programs to do the following quickly:

   - FIND-PRIME-AND-GEN: given $L$, find a prime $p$ of length $L$ and a generator $g$ for $\mathbb{Z}_p^*$.
   - POWER: given $a, b, p$ find $a^b \pmod{p}$ ($p$ need not be a prime).
   - INVERSES: given $a, p$ where $p$ is a prime and $a \not\equiv 0 \pmod{p}$, can find $a^{-1} \pmod{p}$.

   And of course you CANNOT say something like *Do the Pallier Public Key Protocol* (that was an example – you won't need to do that.)

   And NOW finally the problem:

   (a) (10 points) Describe the ElGamal Public Key Crypto System, including both the key generation procedure and the encryption procedure.

   (b) (10 points) Describe how to MODIFY the ElGamal Public Key Crypto System to avoid the NY,NY problem (that is, we want that if Alice sends $x$ and later on sends $x$ again, Eve can't tell she sent the same string).

   **Answer this question on the NEXT page.**

**WRITE YOUR SOLUTION TO PROBLEM FIVE ON THIS PAGE**

**SOLUTION TO PROBLEM FIVE- VERSIONS A AND B WERE THE SAME**

a) ElGamal:

(a) The security parameter is $L$.

(b) Alice picks prime $p$ of length $L$ and generator $g$ for $\mathbb{Z}_p^*$. Alice sends $(p, g)$. All arithmetic is mod $p$.

(c) Alice picks secret $a \in \{\frac{p}{3}, \ldots, \frac{2p}{3}\}$. She computes and sends $g^a$.

(d) Bob picks secret $b \in \{\frac{p}{3}, \ldots, \frac{2p}{3}\}$. He computes and sends $g^b$.

(e) Alice computes $s = (g^b)^a$. Bob computes $s = (g^a)^b$. Now they both have the same key $s$. They both compute $s^{-1}$.

(f) NOW Bob wants to send message $m$ to Alice. He sends $c = ms$ (that is multiplication) to Alice.

(g) Alice can decode by computing $s^{-1}c = s^{-1}ms = m$

b) How to avoid the NY,NY problem:

Since $p$ is of length $L$, they can send messages of length $L$. They agree to only send messages of length (say) $L/2$.

To send a message $m \in \{0,1\}^{L/2}$ Bob will first generate a random $r \in \{0,1\}^{L/2}$ of length $L/2$, and then encrypt $rm$ (that is concatenation). When Alice gets it, she will know how to decrypt.

**COMMON MISTAKES ON PROBLEM FIVE**

(a) Many students said ”do DH”, without describing DH.

(b) Concatenation and multiplication is ambiguous in $rmg^{ab}$, which some students wrote.

(c) People described ElGasarch instead of ElGamal.

(d) People were padding the ciphertext, not the plaintext to solve NY, NY.

(e) People used randomized shift for part (b), which was right if explained correctly.

**END OF SOLUTION TO PROBLEM FIVE**

Scratch Paper