CMSC 456 Midterm, Fall 2018

1. This is a closed book exam, though 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. 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 :
SID :

SCORES ON PROBLEMS (FOR OUR USE)

Prob 1:
Prob 2:
Prob 3:
Prob 4:
Prob 5:
Prob 6:
TOTAL

1. (20 points) Alice and Bob use an alphabet with 17 letters. Hence their alphabet can be viewed as $\{0, \ldots, 16\}$ with arithmetic mod 17. Answer the following questions and briefly explain why your answer is correct.

   (a) (5 points) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CAN be used, or state (no proof needed) that there is no such pair.

   (b) (5 points) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CANNOT be used, or state (no proof needed) that there is no such pair.

(c) (5 points) (Alice and Bob are still using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT. Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CAN be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

(d) (5 points) (Alice and Bob are still using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT (same as the last problem). Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CANNOT be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

SOLUTION TO PROBLEM ONE

In all cases we need the function to be invertible.

(a) $a = 2$, $b = 2$. $f(x) = 2x + 2$ is invertible since 2 is rel prime to 17.

(b) There is no such (a, b) since all $a \in \{1, \ldots, 16\}$ are rel prime to 17.

(c)

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Det is $4 - 6 = -2 \equiv 15$, rel prime to 17, so invertible.

(d)

$$\begin{pmatrix} 2 & 10 \\ 1 & 5 \end{pmatrix}$$

Det is $2 \times 5 - 1 \times 10 = 0$, NOT rel prime to 17, so not invertible.

COMMON MISTAKES

(a) Some students used numbers outside of $\{0, \ldots, 16\}$. NO! This is a mod 17 problem and the problem said only use $\{0, \ldots, 16\}$.

(b) Some students thought that in the affine cipher a has to be rel prime to b. NO, a need only be rel prime to 17.

(c) Some students thought that in the Matrix Cipher a, b, c, d have to be rel prime to each other. NO, we only need $ad - bc$ to be rel prime to 17.

(d) Some students had some of a, b, c, d over 11. Some had some of them equal. NO! The instructions said that a, b, c, d are BETWEEN 1 AND 10 AND ALL DIFFERENT.

END OF SOLUTION TO PROBLEM ONE

2. (20 points) Alice and Bob are doing Diffie-Hellman with $p = 11$ and $g = 2$

   (a) (5 points) If Alice picks $a = 3$ and Bob picks $b = 4$ then what is the shared secret?

   (b) (5 points) If Alice picks $a = 4$ and Bob picks $b = 3$ then what is the shared secret?

   (c) (10 points) You should have gotten the same answer for the last two questions. Either prove or disprove the following statement:

   > Assume Alice and Bob do Diffie Hellman with (p, g). Let $s_{x,y}$ be the secret if Alice picks x and Bob picks y. Then $s_{x,y} = s_{y,x}$.

SOLUTION TO PROBLEM TWO

(a) Alice computes $2^3 \equiv 8$, Bob computes $2^4 \equiv 16 \equiv 5$. Then Alice computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$. Just to check Then Bob computes $(2^3)^4 = 8^4 = 64 \times 64 \equiv -2 \times -2 \equiv 4$. So secret is 4

(b) Alice computes $2^4 \equiv 16 \equiv 5$. Bob computes $2^3 \equiv 8$, Then Alice computes $(2^3)^4 = 8^4 = 64 \times 64 \equiv -2 \times -2 \equiv 4$. Just to check Then Bob computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$.

(c) Yes its true: In the first case the secret is g^{xy}, in the second g^{yx}. But these are the same.

COMMON MISTAKES (I assume that everyone who got this wrong will do the hw-redo thing on this problem. However, the below ARE mistakes. Do not make them on the final.)

(a) Some students left the answer as 2^{12}. or even $2^{12} \pmod{11}$. We have always calculated the actual number using repeated squaring – that's why repeated squaring is important.

(b) Some students had the answer be something > 11. In Diffie-Hellman the answer is always in $\{1, \ldots, p-1\}$.

(c) Some students made arithmetic mistakes. On a 5-point problem which is very easy computationally on an exam with 0 time pressure (all but 10 people left 15 minutes early) that's worth 0 points.

END OF SOLUTION TO PROBLEM TWO

3. (20 points) For each of the following give BOTH an intelligent argument of why it is TRUE *and* an intelligent argument of why it is FALSE.

   (a) (10 points) When doing, RSA always use $e = 2^{16} + 1$.

   (b) (10 points) The Vig-Book Cipher is good to use.

SOLUTION TO PROBLEM THREE

There are several answers. Any one of them is fine to give.

The $e = 2^{16} + 1$ question:

(a) TRUE: e is large enough to thwart off the low-e attacks,

TRUE: Computing m^e takes only 15 mults which is a small number. This comes from the fact that we only have to do the repeated squaring part of the calculation and not the putting-together-part.

TRUE: e is prime and hence is more likely to be relatively prime to R.

FALSE: If you always use the same e then Eve can study that number REALLY INTENSELY and maybe find a way to exploit that.

The Vig-Book Cipher Question:

(a) TRUE: The key is really long and if you use an obscure book, and Eve does not have sophisticated computers, its hard to break (You can mention Freq analysis will not work.)

(b) FALSE: If Eve has sophisticated computers and letters freq she can use freq of pairs of letters to crack.

(c) FALSE: You cannot use a common book like the bible. (You can always use *Problems with a Point* or *Bounded Queries in Recursion Theory* or *Muffin Mathematics: Nobody wants a small piece.*)

(d) FALSE: Alice and Bob still have to meet. (I considered this a weak answer since this is true of all private key ciphers. Fortunately, everyone who said this also said something else.)

END OF SOLUTION TO PROBLEM THREE

4. (5 points) Describe the Blum-Williams variant of the Rabin Encryption (also called Rabin 2.0 — in this variant, Alice can decrypt uniquely). You need not prove correctness or security. Your answer should be such that someone who has not had the course can understand and implement your protocol. Your answer should include:

   - What Alice does to initialize the encryption.
   - What messages m Bob is allowed to send.
   - What Bob does to encrypt m producing c.
   - What Alice does to decrypt c.

SOLUTION TO PROBLEM FOUR

Rabin-BW encryption:

n is sec param.

(a) Alice gen p, q primes of length n such that $p, q \equiv 3 \pmod 4$. Let $N = pq$. Send N.

(b) Encode: To send $m \in SQ_N$, Bob sends $c = m^2 \pmod N$.

(c) Decode: Alice can find 2 or 4 m such that $m^2 \equiv c \pmod N$. Take the $m \in SQ_N$.

END OF SOLUTION TO PROBLEM FOUR

5. (15 points) In your description of the Blum-Williams Variant of Rabin, in the initial step, you chose $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. (If you didn't then go back and correct it!).

   Show what goes wrong if $p = 5$ and $q = 3$. Be CLEAR and CONCISE.

   You may want to use the following facts:

   $1^2 \equiv 14^2 \equiv 1 \pmod{15}$

   $2^2 \equiv 13^2 \equiv 4 \pmod{15}$

   $3^2 \equiv 12^2 \equiv 9 \pmod{15}$

   $4^2 \equiv 11^2 \equiv 1 \pmod{15}$

   $5^2 \equiv 10^2 \equiv 10 \pmod{15}$

   $6^2 \equiv 9^2 \equiv 6 \pmod{15}$

   $7^2 \equiv 8^2 \equiv 4 \pmod{15}$

   SOLUTION TO PROBLEM FIVE

   The only messages Bob can send are squares, so Bob can only send elements of

   $$\{1, 4, 6, 9, 10\}.$$

   To send 1, Bob sends $1^2 \pmod{15} \equiv 1$.

   Alice tries to decode. She finds the four sqrts of 1, namely

   $$\{1, 4, 11, 14\}.$$

   In the normal BW-Rabin there would be only ONE element of this set that is a square, and thats the one that Alice knows was send. But there are two: 1 and 4. Hence Alice cannot decode uniquely.

   COMMON MISTAKES

   (a) Note that we can only encode elements of $\{1, 4, 6, 9, 10\}$. Some students gave an example where they encoded something NOT in that set.

   END OF SOLUTION TO PROBLEM FIVE

6. (a) (5 points) Plain RSA had the problem that message m always got encoded the same way. Describe how we modified RSA to overcome that problem.

   (b) (5 points) Describe the Blum-Goldwasser encryption system.

   (c) (10 points) Blum-Goldwasser has the same problem as RSA – message m always encodes the same way. Modify Blum-Goldwasser so that it no longer has this problem. (DURING EXAM IT was pointed out that BG DID NOT have the same problem as RSA. This is correct. I THEN said that if they explain WHY that is true thats fine for a solution as well.)

SOLUTION TO PROBLEM SIX

1) Fixing Plain RSA: Alice and Bob need to agree that the message m will be of length exactly L_1 and r will be of length exactly L_2. (L_1, L_2 should be chosen so that their sum is close to the max length allowed.)

To send $m \in \{0,1\}^{L_1}$ rather than send m^e generate random $r \in \{0,1\}^{L_2}$ and send $(rm)^e$. NOTE- rm is r CONCAT m. Alice knows to decrypt and take the rightmost L_1 bits.

2) Blum-Goldwasser. Omitted. See slides.

3) We give two answers
ANSWER ONE:

Fixing BG: Alice and Bob need to agree that the message m will be of length exactly L_1 and r will be of length exactly L_2. (L_1, L_2 should be chosen so that their sum is close to the max length allowed.)

To send $m \in \{0,1\}^{L_1}$ rather than send $BG(m)$ generate random $r \in \{0,1\}^{L_2}$ and send $BG(rm)$. NOTE- rm is r CONCAT m. Alice knows to decrypt and take the rightmost L_1 bits.

ANSWER TWO: Bill you're a moron! Recall that BG already uses a random seed. To send $m \in \{0,1\}^L$ Bob picks a *random* $r \in \mathbb{Z}_N$ and uses it to generate a psuedo-random sequence $b_1 \cdots b_L$ and sends $(m_1 \oplus b_1) \cdots (m_L \oplus b_L)$. If he send m again he would *pick a different* r *and hence get a different psuedo-random sequence of bits.* Hence m send twice *already* does not encrypt to the same thing.

END OF SOLUTION TO PROBLEM SIX
COMMON MISTAKES

1. For 6a, the padding is to CONCATE by a random string, not MULTIPLY. Some students multiplied.

2. For 6c, some students just STATED that BG does not have the same problem as RSA but did not say why.

END OF SOLUTION TO PROBLEM SIX

Scratch Paper