CMSC 389 Final, Winter 2018

1. This is a closed book exam, though ONE sheet of notes is allowed. **You CANNOT use a Calculators**. 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 90 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:	
TOTAL	

1. (20 points) The Vorlons use the 7-letter alphabet $\{0, 1, 2, 3, 4, 5, 6\}$.

   (a) (10 points) For each numbers in $\{1, 2, 3, 4, 5, 6\}$ give its Multiplicative Inverse Mod 7.

1	2	3	4	5	6

   (b) (10 points)
   What is the inverse mod 7 of the following 2×2 matrix
   (NOTE- the matrix you give must have all of its entries in $\{0, 1, 2, 3, 4, 5, 6\}$.)

$$\mathbf{A} = \begin{pmatrix} 3 & 6 \\ 5 & 4 \end{pmatrix}$$

$$\mathbf{A^{-1}} =$$

SOLUTION TO PROBLEM ONE

a) all $=$ are $\equiv$ mod 7
Multiplicative inverse is the number x s.t. $ax \equiv 1 \mod 7$
$1^{-1} = 1$

$2^{-1} = 4$

$3^{-1} = 5$

$4^{-1} = 2$

$5^{-1} = 3$

$6^{-1} = 6$.

b) $12 - 30 = -18 = 21 - 18 = 3$. Need that $3^{-1} = 5$. The rest is omitted.

END OF SOLUTION TO PROBLEM ONE

2. (20 points) Zelda will do Verifiable Secret Sharing with A_1 and A_2. Together they can find the secret but separately they cannot. She uses the polynomial method. Her secret is 6. She is working in mod 7. She picks random number 2. So her polynomial is

$$f(x) = 2x + 6$$

She will use generator $g = 2$.

(a) (10 points) What does Zelda give BOTH A_1 and A_2 (so they can verify).

A_1 & A_2
_____

(b) (5 points) What does Zelda give A_1 that she does not send to A_2?

A_1 & $\sim A_2$
_____

(c) (5 points) What does Zelda give A_2 that she does not send to A_1?

$\sim A_1$ & A_2
_____

SOLUTION TO PROBLEM TWO

a) Zelda gives A_1 and A_2 p, g, g^r and g^s which in this case is

$p = 7$

$g = 2$

Since $r = 2$ she gives $g^2 = 2^2 = 4$

Since $s = 6$ she gives $g^6 = 2^6 = 64 \text{mod } 7$ which is 1.

b) Zelda gives A_1 $f(1) = 2 + 6 = 8 \equiv 1$ so she gives A_1 1.

c) Zelda gives A_2 $f(2) = 10 \equiv 3$ so she gives A_2 3.

END OF SOLUTION TO PROBLEM TWO

3. (20 points) Zelda wants to share a secret s of length $|s|$ with $A_1, \ldots, A_{n+3}$ so that

   - A_1, A_2, A_3, A_4 can determine the secret,
   - A_1, A_3, A_4, A_5 can determine the secret,
   - A_1, A_4, A_5, A_6 can determine the secret,

   $\vdots$

   - A_1, A_{n-1}, A_n, A_{n+1} can determine the secret.
   - A_1, A_n, A_{n+1}, A_{n+2} can determine the secret.
   - A_1, A_{n+1}, A_{n+2}, A_{n+3} can determine the secret.

   Zelda uses the Random String Method.

   (a) Explain what Zelda does.

   (b) For $1 \leq i \leq n+3$ how many random strings does each A_i get?

A_1	A_2	A_3	A_4	A_n	A_{n+1}	A_{n+2}	A_{n+3}

SOLUTION TO PROBLEM THREE

2a) Zelda has secret s.

For each i, $1 \leq i \leq n$, Zelda produces random r_1, r_2, r_3 and then $r' = r_1 \oplus r_2 \oplus r_3 \oplus s$. She then give A_1 r', A_{i+1} r_1, $A_{i+2} r_2$, and A_{i+3} r_3.

2b)

A_1 is involved with n groups so she gets n strings.

A_2 is involved with 1 group so she gets 1 string

A_3 is involved with 2 groups so she gets 2 strings

A_4, ..., A_{n+1} are involved with 3 groups so they get 3 strings.

A_{n+2} is involved with with 2 groups so she gets 2 strings.

A_{n+3} is involved with 1 group so she gets 1 string.

END OF SOLUTION TO PROBLEM THREE

4. (20 points) In this problem we examine what happens if Alice and Bob do Diffie Helman but DO NOT use a generator. As an example think of $p = 17$ and $g = 9$. Note that 9 is NOT a generator:

   $9^0 \equiv 1 \pmod{17}$

   $9^1 \equiv 9 \pmod{17}$

   $9^2 \equiv 13 \pmod{17}$

   $9^3 \equiv 15 \pmod{17}$.

   $9^4 \equiv 16 \pmod{17}$.

   $9^5 \equiv 8 \pmod{17}$

   $9^6 \equiv 4 \pmod{17}$

   $9^7 \equiv 2 \pmod{17}$

   $9^8 \equiv 1 \pmod{17}$.

   (a) If $p = 17$ and $g = 9$, Alice picks $a = 3$, and Bob picks $b = 5$, then what is the shared secret key? Does it take Alice and Bob fewer steps to calculate the keys because 9 is NOT a generator?

key
_____

   (b) If Alice and Bob use a large prime p and a number g that is NOT a generator then is Diffie-Helman less secure?

SOLUTION TO PROBLEM FOUR

(a) (10 points) $9^{3*5} \mod 17$- no problem for Alice and Bob to use a non generator.

(b) (10 points) LESS SECURE! Normally Discrete Lot takes p steps since, given g, x, to find y such that $g^y = x$, you have to go through EVERY y. If g is not a generator then there are $\leq p/2$

(perhaps far less) powers of g. Hence Eve has to go through $\leq p/2$ possibilities which is less than p.

END OF SOLUTION TO PROBLEM FOUR

5. (20 points)

(a) (10 points) EITHER describe an information-theoretic secure scheme for secret s, 10 people, need that any 3 can recover the secret but no 2, where SOMEONE gets a string of length $< |s|$ (the other players can get arbitrarily long strings), OR explain why there is no such scheme.

(b) (10 points) Zelda has used polynomial secret sharing with $A_1, \ldots, A_9$ such that if any two of get together to learn the secret, but one person alone cannot. She does this over mod 7.

Zelda is dishonest!

She wants to give A_1 the share $f(1) = 1$ (nothing bad about that, but wait).

She wants A_1 and A_2 to think the secret is 0 (nothing bad about that, but wait).

She wants A_2 and A_3 to think the secret is 1 (WOW- not what A_1 and A_2 think- this is evil!)

What should she give A_2? What should she give A_3?

A_2	A_3
_____	_____

SOLUTION TO PROBLEM FIVE

(a) There is no such scheme. If there was then let Alice get a share that is $< |s|$, say $|s|-1$.. If Bob and Carol get together (just TWO people so they should learn NOTHING) they look at all $2^{|s|-1}$ possible shares Alice could have and use this to find $2^{|s|-1|} < 2^{|s|}$ possible secrets. Hence the secret is not info-theoretic secure.

(b) Zelda wants to find b, c such that the

- The linear function going through $(1,1)$ and $(2,b)$ has constant term 0.
- The linear function going through $(2,b)$ and $(2,c)$ has constant term 1.

The linear function going through $(1,1)$ and $(2,b)$ is

$$f(x) = (b-1)x + (2-b).$$

So we will want $b = 2$.

The linear function going through $(2,b)$ and $(3,c)$ is

$$f(x) = (c-b)x + 3b - 2c.$$

So we will want $3b - 2c = 1$

Since $b = 2$ we want

$$2c = 3b - 1 = 3 \times 2 - 1 = 5$$

The inverse of 2 mod 7 (from problem 1!) is 4. So

$$4 \times 2 \times c = 4 \times 5 = 20$$

$$c = 20 = 6.$$

So we can take $(a, b, c) = (1, 2, 6)$.

SOLUTION TO PROBLEM FIVE

Scratch Paper