HW 11 CMSC 456. Morally DUE Nov 25
DEAD CAT DAY IS NOV 27
THIS HW IS TWO PAGES LONG
SOLUTIONS

1. (0 points) What is Day/Time of Final? **READ MID SOLUTIONS! Even for the problems you got right!!!!!!!!!!!!!!**

2. (30 points) Zelda wants to do $(7, 14)$ information-theoretic secret sharing. The players are $A_1, \ldots, A_{14}$. The secret string is 1001.

   (a) (15 points) Zelda wants to use the random string method. How many strings does A_1 get? (Give an actual number, not something like *the 9th JUSTIN Composite*.) How long are the strings A_1 gets?

   ANSWER

   A_1 will get a string for EVERY 7-sized set she is a member of. So that will be

   $$\binom{13}{6} = \frac{13!}{6!7!} = \frac{13 \times 12 \times 11 \times 10 \times 9 \times 8}{6 \times 5 \times 4 \times 3 \times 2}$$

   The 12 cancels with the 3×4. The 10 cancels the 2×5. So we end up with:

   $$\frac{13 \times 11 \times 9 \times 8}{6} = 13 \times 11 \times 3 \times 4 = 1716.$$

   So there are 1716 strings. Each string is the same length as the secret, so that is length 4.

   END OF ANSWER

   (b) (15 points) Zelda wants to use the polynomial method. What is the smallest prime Zelda can use? What is the degree of the polynomial that Zelda uses? How many strings does A_1 get? How long are they?

   ANSWER

   We need a prime p such that $2^4 < p$, so we take 17. The degree is 6 since 7 points determine a 6th degree polynomial. A_1 gets just one string. The string is in $\mathbb{Z}_{17}$ padded out to length 4.

   END OF ANSWER

3. (30 points)

   (a) (20 points) DESCRIBE the random-string $(3, 9)$ secret sharing scheme. You must describe both what Zelda gives out, and how any three people can determine the secret. KEY: Explain it so that someone who has never seen secret sharing can understand it. This is NOT hypothetical. A TA who does not know secret sharing is grading this problem and will learn the protocol from you! How many strings does each person get? (Give an actual number, NOT something like *the 17th MARINA number.*)

   (b) (10 points) DO AN EXAMPLE of your method.

ANSWER

We call the people $A_1, \ldots, A_9$. We give the $(3, 9)$ secret sharing method via random strings.

(a) Zelda has secret s.

(b) For every $1 \leq i < j < k \leq 9$, Zelda generates two random strings: $r_{i,j,k,i}$, $r_{i,j,k,j}$, We now visit every triple and say what Zelda gives them. All of the players will be visited many times. How many? $\binom{8}{2}$ which is the number of triples they are in.
Let $1 \leq i < j < k \leq 9$.

- Give A_i the string $(i, j, k, r_{i,j,k,i})$
- Give A_j the string $(i, j, k, r_{i,j,k,j})$
- Give A_k the string $(i, j, k, r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus s))$

(c) If A_i, A_j, A_k get together they will compute

$$r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus (r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus s) = s$$

Everyone gets $\binom{8}{2} = 28$ strings.

We omit an example.

END OF ANSWER

MORE HW ON THE NEXT PAGE

4. (40 points)

   (a) (30 points) DESCRIBE the polynomial $(4, 7)$ secret sharing scheme. You must describe both what Zelda gives out, and how any four people can determine the secret. How many strings does each person get? (Give an actual number, NOT something like *the Ninth Nathan Natural Number*.) KEY: Explain it so that someone who has never seen secret sharing can understand it. This is NOT hypothetical. A TA who does not know secret sharing is grading this problem and will learn the protocol from you!

   (b) (10 points) DO AN EXAMPLE of your method.

ANSWER

We call the people $A_1, \ldots, A_7$. We give the $(4, 7)$ secret sharing method via polynomial method.

(a) Zelda has secret s.

(b) Zelda finds a prime p such that $p > 2^{|s|}$.
Zelda generates random $r_3, r_2, r_1 \in \{0, \ldots, p-1\}$.
Zelda forms polynomial

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

(s was a string of 0's and 1's. We now view it as a number written in binary)

(c) For all $1 \leq i \leq 7$, give A_i the number $p(i) \pmod p$.

(d) If any four get together they have four points on a cubic. Hence they can recover the entire cubic, and hence the constant term which is the secret.

We omit an example.

END OF ANSWER