HW On Secret Sharing CMSC 456
SOLUTIONS

THIS HW IS THREE PROBLEMS

1. (30 points)

   (a) Zelda wants to do $(3, 3)$ secret sharing with polynomials. The secret is 1111 which is 15 in base 2.

   so she uses mod 17.

   (b) (20 points) Zelda does Secret Sharing with Mods. She uses $p = 17$. She picks $r_2 = 3$ and $r_1 = 7$. What shares does she give out? Give the ACTUAL NUMBER, do not just say, for example $f(1)$.

   SOLUTION

   All math is mod 17.

   $f(x) = 3x^2 + 7x + 15$

   Give A_1 $f(1) = 3 + 7 + 15 = 10 - 2 = 8$

   Give A_2 $f(2) = 3\times 4+7\times 2+15 = 12+14+15 = 26-2 = 24 = 7$

   Give A_3 $f(3) = 3\times 9+7\times 3+15 = 27+10+15 = 10+10-2 = 18 = 1$

   END OF SOLUTION

   (c) (10 points) Zelda wants to use a field of size *exactly* 16 (so using mod 17 won't work). Present a field with exactly 16 elements in it. Explain what the elements are and how to multiply. (Hint: See

   `https://math.stackexchange.com/questions/32197/find-all-irreducible-moni`

   (We'll put the link on the course website for easier access.)

)

   SOLUTION

   We need a polynomial in $Z_2[x]$ of degree 4 that is irreducible. By looking at the website reference we know that $x^4 + x + 1$ is irreducible.

   We now describe the field

- The elements are all polynomials in $Z_2[x]$ of degree ≤ 3. Note that there are 2^4 of these since this is all polynomials of the form
$$a_3x^2 + a_2x^2 + a_1x^1 + a_0x^0$$
where $a_0, a_1, a_2, a_3 \in \{0, 1\}$.
- Addition of elements is the same as poly addition.
- Multiplication of elements is done as follow: to multiply $p(x)$ and $q(x)$ first do the ordinary multiplication but then
Replace x^4 by $x + 1$
Replace x^5 by $x^2 + x$
Replace x^6 by $x^3 + x^2$

END OF SOLUTION

GOTO NEXT PAGE

2. (30 points) Zelda is going to (4,4) secret share with Alice1, Alice2, Alice3, Alice4. The secret is an element $s \in \{0,1,2,3,4,5,6\}$. She is going to use mod 7. Normally Zelda would do the following:

   Generate random $r_3, r_2, r_1 \in \{0,1,2,3,4,5,6\}$. *Let*

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

   Give

   Alice1 $f(1) \pmod 7$

   Alice2 $f(2) \pmod 7$

   Alice3 $f(3) \pmod 7$*, and*

   Alice4 $f(4) \pmod 7$*,*

   but Zelda does not want to generate THREE random numbers! She just wants to generate TWO. So she does the following:

   Generate random $r_3, r_2 \in \{0,1,2,3,4,5,6\}$. *Let* $f(x) = rx^3 + r_2x^2 + s$. *Give*

   Alice1 $f(1) \pmod 7$*,*

   Alice2 $f(2) \pmod 7$*,*

   Alice3 $f(3) \pmod 7$*, and*

   Alice4 $f(4) \pmod 7$*.*

   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) (15 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 $f(1) = 1 \pmod 7$. So Alice1 only knows that

   $$f(1) \equiv r_3 \times 1^3 + r_2 \times 1^2 + s \pmod 7$$

   $$1 \equiv r_3 + r_2 + s \pmod 7$$

The possibilities for (r_3, r_2, s) are $(1,0,0)$, $(0,1,0)$, $(6,2,0)$, $(5,3,0)$, $(4,4,0)$, $(3,5,0)$, $(2,6,0)$,
$(0,0,1)$, $(6,1,1)$, $(5,2,1)$, $(4,3,1)$, $(3,4,1)$, $(2,5,1)$, $(1,6,1)$,
I won't list the rest of them; however, for all $0 \le s \le 6$ there are 7 that have that s. Hence Alice1 learns NOTHING since ANYTHING can be s.

(b) (15 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
$1 \equiv r_3 \times 1^3 + r_2 \times 1^2 + s \pmod 7$
$0 \equiv r \times 2^3 + r_2 \times 2^2 + s \pmod 7$
SO
$r_3 + r_2 + s \equiv 1 \pmod 7$
$r_3 + 4r_2 + s \equiv 0 \pmod 7$
Subtract the first equation from the second to get
$3r_2 \equiv -1 \equiv 1 \pmod 7$
$3r_2 \equiv 6 \equiv 0 \pmod 7$
$r_2 = 2$. So now we have
$r_3 + 2 + s \equiv 1 \pmod 7$
$r_3 + 8 + s \equiv 0 \pmod 7$
SO
$r_3 + 2 + s \equiv 1 \pmod 7$
$r_3 + 1 + s \equiv 0 \pmod 7$
OH- these are the same equation, so all we have are:

$$r_3 + s \equiv 6 \pmod 7$$

Any s will work since can take $r_3 = 7 - s$.
So Alice1 and Alice2 learn NOTHING.

GOTO NEXT PAGE

3. (40 points) Zelda does $(3, 8)$ secret sharing with $A_1, \ldots, A_8$. We assume NOTHING about what she uses. The secret is of length 9. Zelda (1) gives each of $A_1, \ldots, A_6$ a share of length 10 and, (2) gives each of A_7 and A_8 a share of length 2. Fill in the following sentences and show why:

   (a) (20 points) If A_1 alone can learn XXX. Hence the secret sharing scheme is not information-theoretic secure.

   BEGIN SOLUTION

   A_1 GUESSES what the shares of A_2 and A_3 are. A_7 has one of $2^2 = 4$ shares. A_8 has one of $2^2 = 4$ shares. SO $A_2 \times A_3$ combine to have a total of 16 possible pairs-of-shares. So A_1 can get the number of possible shares down from $2^9 = 512$ to 16.

   Formally XXX is *a set of 16 possibilities for the secret.*

   END SOLUTION

   (b) (20 points) If A_1 and A_2 together can learn XXX. Hence the secret sharing scheme is not information-theoretic secure.

   BEGIN SOLUTION

   A_1 and A_2 GUESS what the share of A_7 is A_7 has one of $2^2 = 4$ shares. So A_1 andA_2 can get the number of possible shares down from $2^9 = 512$ to 4.

   Formally XXX is *a set of 4 possibilities for the secret.*

   END SOLUTION