Solutions to HW11 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers **reads them** and uses it to help their teaching. Especially the comments.

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers **reads them** and uses it to help their teaching. Especially the comments.
2. The teaching eval comm **reads them** to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers **reads them** and uses it to help their teaching. Especially the comments.
2. The teaching eval comm **reads them** to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)
3. These evals are used in the promotion process (e.g., Tenure). It is our hope that because the Teaching Eval Comm helps people become better teachers, there is NO bad teaching so this is not an obstacle for promotion.

FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers **reads them** and uses it to help their teaching. Especially the comments.
2. The teaching eval comm **reads them** to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)
3. These evals are used in the promotion process (e.g., Tenure). It is our hope that because the Teaching Eval Comm helps people become better teachers, there is NO bad teaching so this is not an obstacle for promotion.
4. And you can help us! By filling out the forms!

On TV likely not in Real Life

On TV likely not in Real Life

1. Alice is interrogating Bob but actually Alice is a double agent on Bob's side.

On TV likely not in Real Life

1. Alice is interrogating Bob but actually Alice is a double agent on Bob's side.
2. Alice has to pass Bob information, telling what to say, while she is interrogating him. How does she do this?

On TV likely not in Real Life

1. Alice is interrogating Bob but actually Alice is a double agent on Bob's side.
2. Alice has to pass Bob information, telling what to say, while she is interrogating him. How does she do this?
3. ON TV: Alice punches Bob in **Morse code**!

On TV likely not in Real Life

1. Alice is interrogating Bob but actually Alice is a double agent on Bob's side.
2. Alice has to pass Bob information, telling what to say, while she is interrogating him. How does she do this?
3. ON TV: Alice punches Bob in **Morse code**!
4. Realistic? Discuss.

HW11, Problem 1

Z has s. Will share with $A_1, \ldots, A_6$. Access Structure:
$\{A_1, A_2\}$,
$\{A_2, A_3\}$,
$\{A_3, A_4\}$,
$\{A_4, A_5\}$,
$\{A_5, A_6\}$,
$\{A_1, A_3, A_5\}$.

HW11, Problem 1

Z has s. Will share with $A_1, \ldots, A_6$. Access Structure:
$\{A_1, A_2\}$,
$\{A_2, A_3\}$,
$\{A_3, A_4\}$,
$\{A_4, A_5\}$,
$\{A_5, A_6\}$,
$\{A_1, A_3, A_5\}$.

Give Info Theoretic Sec Sharing Scheme.

HW11, Problem 1

Z has s. Will share with $A_1, \ldots, A_6$. Access Structure:
$\{A_1, A_2\}$,
$\{A_2, A_3\}$,
$\{A_3, A_4\}$,
$\{A_4, A_5\}$,
$\{A_5, A_6\}$,
$\{A_1, A_3, A_5\}$.

Give Info Theoretic Sec Sharing Scheme.

State what sizes of shares everyone gets.

HW11, Problem 1 SOLUTION: The protocol

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_2:$(23, r)$, A_3:$(23, r \oplus s)$.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_2:$(23, r)$, A_3:$(23, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_3:$(34, r)$, A_4:$(34, r \oplus s)$.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_2:$(23, r)$, A_3:$(23, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_3:$(34, r)$, A_4:$(34, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_4:$(45, r)$, A_5:$(45, r \oplus s)$.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_2:$(23, r)$, A_3:$(23, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_3:$(34, r)$, A_4:$(34, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_4:$(45, r)$, A_5:$(45, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_5:$(56, r)$, A_6:$(56, r \oplus s)$.

HW11, Problem 1 SOLUTION: The protocol

Note The r's below are all separate and independent.

Z gen rand $r \in \{0,1\}^n$. A_1:$(12, r)$, A_2:$(12, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_2:$(23, r)$, A_3:$(23, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_3:$(34, r)$, A_4:$(34, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_4:$(45, r)$, A_5:$(45, r \oplus s)$.

Z gen rand $r \in \{0,1\}^n$. A_5:$(56, r)$, A_6:$(56, r \oplus s)$.

Z gen rand $r_1, r_2 \in \{0,1\}^n$. A_1:$(135, r_1)$, A_3:$(135, r_2)$, A_4:$(135, s \oplus r_1 \oplus r_2)$.

HW11, Problem 1 SOLUTION: Size of Shares

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

A_2 is in 2 protocols: 12 and 23, so gets $2|s| + O(1)$.

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

A_2 is in 2 protocols: 12 and 23, so gets $2|s| + O(1)$.

A_3 is in 3 protocols: 23, 34, 135, so gets $3|s| + O(1)$.

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

A_2 is in 2 protocols: 12 and 23, so gets $2|s| + O(1)$.

A_3 is in 3 protocols: 23, 34, 135, so gets $3|s| + O(1)$.

A_4 is in 2 protocols: 34, 45, so gets $2|s| + O(1)$.

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

A_2 is in 2 protocols: 12 and 23, so gets $2|s| + O(1)$.

A_3 is in 3 protocols: 23, 34, 135, so gets $3|s| + O(1)$.

A_4 is in 2 protocols: 34, 45, so gets $2|s| + O(1)$.

A_5 is in 3 protocols: 45, 56, 135, so gets $2|s| + O(1)$.

HW11, Problem 1 SOLUTION: Size of Shares

A_1 is in 2 protocols: 12 and 135, so gets $2|s| + O(1)$.

A_2 is in 2 protocols: 12 and 23, so gets $2|s| + O(1)$.

A_3 is in 3 protocols: 23, 34, 135, so gets $3|s| + O(1)$.

A_4 is in 2 protocols: 34, 45, so gets $2|s| + O(1)$.

A_5 is in 3 protocols: 45, 56, 135, so gets $2|s| + O(1)$.

A_6 is in 1 protocols: 56, so gets $|s| + O(1)$.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a “brilliant” idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
- She picks ONE random $r \in \mathbb{Z}_p$.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
- She picks ONE random $r \in \mathbb{Z}_p$.
- She formulates the polynomial $f(x) = rx^2 + s_1 x + s_2 \pmod{p}$

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
- She picks ONE random $r \in \mathbb{Z}_p$.
- She formulates the polynomial $f(x) = rx^2 + s_1 x + s_2 \pmod{p}$
- For $1 \le i \le 6$ she gives A_i the number $f(i)$.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
- She picks ONE random $r \in \mathbb{Z}_p$.
- She formulates the polynomial $f(x) = rx^2 + s_1x + s_2 \pmod{p}$
- For $1 \leq i \leq 6$ she gives A_i the number $f(i)$.
- If any three get together they will have three points on a degree-2 equation and hence they can find the equation $f(x)$, and hence they can find s_1, s_2.

HW11, Problem 2

Z is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She uses polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

- She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
- She picks ONE random $r \in \mathbb{Z}_p$.
- She formulates the polynomial $f(x) = rx^2 + s_1x + s_2 \pmod{p}$
- For $1 \le i \le 6$ she gives A_i the number $f(i)$.
- If any three get together they will have three points on a degree-2 equation and hence they can find the equation $f(x)$, and hence they can find s_1, s_2.

Show why this is a BAD idea.

HW11, Problem 2, SOLUTION

All math is mod p.

HW11, Problem 2, SOLUTION

All math is mod p.

A_1 has $f(1) = r + s_1 + s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

HW11, Problem 2, SOLUTION

All math is mod p.

A_1 has $f(1) = r + s_1 + s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

Mult the first eq by 4 and then subtract:

HW11, Problem 2, SOLUTION

All math is mod p.

A_1 has $f(1) = r + s_1 + s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

Mult the first eq by 4 and then subtract:

A_1 has $4f(1) = 4r + 4s_1 + 4s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

HW11, Problem 2, SOLUTION

All math is mod p.

A_1 has $f(1) = r + s_1 + s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

Mult the first eq by 4 and then subtract:

A_1 has $4f(1) = 4r + 4s_1 + 4s_2$.
A_2 has $f(2) = 4r + 2s_1 + s_2$.

A_1 and A_2 know $4f(1) - f(2) = 2s_1 + 3s_2$.
This LIMITS the number of poss for (s_1, s_2) and hence leaks info.

HW11, Problem 2. Example of Solution

$p = 37$. All math is mod 37.
$f(1) = 9$
$f(2) = 10$

HW11, Problem 2. Example of Solution

$p = 37$. All math is mod 37.
$f(1) = 9$
$f(2) = 10$

$4f(1) - f(2) = 2s_1 + 3s_2$. Hence

HW11, Problem 2. Example of Solution

$p = 37$. All math is mod 37.
$f(1) = 9$
$f(2) = 10$

$4f(1) - f(2) = 2s_1 + 3s_2$. Hence
$2s_1 + 3s_2 = 4f(1) - f(2) = 36 - 10 = 16$.

HW11, Problem 2. Example of Solution

$p = 37$. All math is mod 37.
$f(1) = 9$
$f(2) = 10$

$4f(1) - f(2) = 2s_1 + 3s_2$. Hence
$2s_1 + 3s_2 = 4f(1) - f(2) = 36 - 10 = 16$.
Multiply by inverse of 2, which is 9.

$$18s_1 + 27s_2 = 9 \times 16 = 9 \times -1 = -9 = 8$$

$$s_1 + 10s_2 = 8$$

$$s_1 = 8 - 10s_2.$$

HW11, Problem 2. Example of Solution

$p = 37$. All math is mod 37.
$f(1) = 9$
$f(2) = 10$

$4f(1) - f(2) = 2s_1 + 3s_2$. Hence
$2s_1 + 3s_2 = 4f(1) - f(2) = 36 - 10 = 16$.
Multiply by inverse of 2, which is 9.

$$18s_1 + 27s_2 = 9 \times 16 = 9 \times -1 = -9 = 8$$

$$s_1 + 10s_2 = 8$$

$$s_1 = 8 - 10s_2.$$

Once s_2 is known, s_1 is known. Hence there are only 37 options for (s_1, s_2) instead of 37^2.

HW11, Problem 3

In class (Nov 16 lecture A-B-Love-Cards) we did several protocols (using cards and other devices) such that A and B can determine if they want a second date; however, if A wants a second date but B doesn't B does not know that (and vice versa).

HW11, Problem 3

In class (Nov 16 lecture A-B-Love-Cards) we did several protocols (using cards and other devices) such that A and B can determine if they want a second date; however, if A wants a second date but B doesn't B does not know that (and vice versa).

A, B, C, D all get together for dinner. They want to see if they want to have dinner again. If ALL want to dine again, they will. If at least ONE person does not, they won't.

HW11, Problem 3

In class (Nov 16 lecture A-B-Love-Cards) we did several protocols (using cards and other devices) such that A and B can determine if they want a second date; however, if A wants a second date but B doesn't B does not know that (and vice versa).

A, B, C, D all get together for dinner. They want to see if they want to have dinner again. If ALL want to dine again, they will. If at least ONE person does not, they won't.

Come up with a protocol so that at the end they all know if they want to have dinner together again, but if the answer is NO then the people who voted NO do not know how anyone else voted. You can use any of the devices in the talk on A and B.

HW11, Problem 3 SOLUTION

A, B, C, D all come with two cards- one opaque and one glass. They all put their card in a box. Glass if YES, opaque if NO.

HW11, Problem 3 SOLUTION

A, B, C, D all come with two cards- one opaque and one glass. They all put their card in a box. Glass if YES, opaque if NO.

Light is shown through the box.

HW11, Problem 3 SOLUTION

A, B, C, D all come with two cards- one opaque and one glass. They all put their card in a box. Glass if YES, opaque if NO.

Light is shown through the box.

If light goes all the way through then all said glass, so YES, they all dine together.

HW11, Problem 3 SOLUTION

A, B, C, D all come with two cards- one opaque and one glass. They all put their card in a box. Glass if YES, opaque if NO.

Light is shown through the box.

If light goes all the way through then all said glass, so YES, they all dine together.

If light does not go through then at least one person said NO, but side from that person nobody knows who it was.