

Q1 Honor Code

1 Point

You will not need every blank on this sheet. **A complete exam will have 50/61 questions answered.**

The 5:00 PM password is:

that-piazza-developer-should-feel-much-shame-371229281

The 7:00 PM password is:

let's-make-the-grad-student-do-it-032698963

Read the honor code on Gradescope and type your name:

Tianqi Yang

Check your PDF exam frequently to make sure your question numbers are matching.

Q2 True/False

20 Points

Q2.1

1 Point

☐ True

☒ False

Q2.2

1 Point

- ☐ True
- ☒ False

Q2.3

1 Point

- ☒ True
- ☐ False

Q2.4

1 Point

- ☒ True
- ☐ False

Q2.5

1 Point

- ☒ True
- ☐ False

Q2.6

1 Point

- ☒ True
- ☐ False

Q2.7

1 Point

- ☒ True
- ☐ False

Q2.8

1 Point

- ☐ True
- ☒ False

Q2.9

1 Point

- ☐ True
- ☒ False

Q2.10

1 Point

- ☒ True
- ☐ False

Q2.11

1 Point

- ☐ True
- ☒ False

Q2.12

1 Point

- ☐ True
- ☒ False

Q2.13

1 Point

- ☐ True
- ☒ False

Q2.14

1 Point

- ☐ True
- ☒ False

Q2.15

1 Point

- ☐ True
- ☒ False

Q2.16

1 Point

- ☒ True
- ☐ False

Q2.17

1 Point

- ☐ True
- ☒ False

Q2.18

1 Point

- ☐ True
- ☒ False

Q2.19

1 Point

- ☐ True
- ☒ False

Q2.20

1 Point

- ☒ True
- ☐ False

Q3

8 Points

Q3.1

1 Point

☐ A

☐ B

☒ C

☐ D

☐ E

☐ F

Q3.2

1 Point

☒ G

☒ H

☒ I

☐ J

☐ K

☐ L

Q3.3

1 Point

☒ A☒ B☒ C☐ D☐ E☐ F**Q3.4**

1 Point

☐ G☐ H☐ I☒ J☐ K☐ L**Q3.5**

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F

If a user's name is "aaa" and password is "bbb", another user name is "aa" and password is "bbba", we will get the same hash value $H(\text{password} \parallel \text{username})$ since "bbb" + "aaa" = "bbba" + "aa" which would cause the bad things happen. We can use salt like $(\text{username}, r, H(\text{password} \parallel r))$ to prevent such things happen because of the random salts.

Q3.6

1 Point

☒ G☒ H☐ I☐ J☐ K☐ L

Q3.7

1 Point

☒ A☒ B☒ C☐ D☐ E☐ F**Q3.8**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L

Q4

8 Points

Q4.1

1 Point

☐ A☐ B☒ C☐ D☐ E☐ F**Q4.2**

1 Point

☐ G☒ H☐ I☐ J☐ K☐ L**Q4.3**

1 Point

☐ A☐ B☒ C☐ D☐ E☐ F**Q4.4**

1 Point

☐ G☒ H☒ I☐ J☐ K☐ L**Q4.5**

1 Point

☐ A☐ B☒ C☐ D☐ E☐ F**Q4.6**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L**Q4.7**

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F**Q4.8**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L

Q5

8 Points

Q5.1

1 Point

☐ A☐ B☒ C☐ D☐ E☐ F

Q5.2

1 Point

☐ G

☐ H

☐ I

☒ J

☐ K

☐ L

Q5.3

1 Point

☐ A

☐ B

☐ C

☐ D

☐ E

☐ F

16

Q5.4

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L

'\x74\x3\xfl\xff' + SHELLCODE

Q5.5

1 Point

☒ A☒ B☐ C☐ D☐ E☐ F

Q5.6

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L**Q5.7**

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F

Q5.8

1 Point

☐ G

☐ H

☐ I

☐ J

☐ K

☐ L

Q6

8 Points

Q6.1

1 Point

☒ A

☐ B

☐ C

☐ D

☐ E

☐ F

Q6.2

1 Point

☒ G☐ H☐ I☐ J☐ K☐ L

she can calculate it because b can be either 0 or 1 and she can know the guess before reveal

Q6.3

1 Point

☐ A☐ B☒ C☐ D☐ E☐ F

Since Bob does not know the b' , Alice claim that she guessed tails(1) even if she guess heads(0) because she can use random bit b' to show she is correct.

Q6.4

1 Point

☐ G☐ H☐ I☒ J☐ K☐ L**Q6.5**

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F**Q6.6**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L**Q6.7**

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F**Q6.8**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L**Q7**

8 Points

Q7.1

1 Point

☐ A

☐ B

☒ C

☐ D

☐ E

☐ F

Q7.2

1 Point

☐ G

☒ H

☐ I

☐ J

☐ K

☐ L

Q7.3

1 Point

☐ A

☒ B

☐ C

☐ D

☐ E

☐ F

Q7.4

1 Point

☐ G

☐ H

☒ I

☐ J

☒ K

☐ L

Q7.5

1 Point

☐ A☐ B☐ C☐ D☐ E☒ F**Q7.6**

1 Point

☐ G☐ H☐ I☐ J☐ K☐ L

'AB\x00' + (12 * 'A')

Q7.7

1 Point

☐ A☐ B☐ C☐ D☐ E☐ F

```
'\x00' + (11 * 'A') + (4 * 'X') + out[22:26] + (4 * 'A') + '\xa\x35\xfd\xbf'
```

Q7.8

1 Point

☐ G☐ H☐ I☐ J☒ K☐ L**A complete exam will have 50/61 questions answered.**

You can keep resubmitting your answer sheet until time is up. First click "Submit and View Assignment" and then click "Resubmit Assignment" (lower right corner).

Midterm Answer Sheet

● **UNGRADED**

STUDENT

Tianqi Yang

TOTAL POINTS

- / **61 pts**

QUESTION 1

Honor Code

1 pt

QUESTION 2

True/False

20 pts

2.1 (no title)

1 pt

2.2 (no title)

1 pt

2.3 (no title)

1 pt

2.4 (no title)

1 pt

2.5 (no title)

1 pt

2.6 (no title)

1 pt

2.7 (no title)

1 pt

2.8 (no title)

1 pt

2.9 (no title)

1 pt

2.10 (no title)

1 pt

2.11 (no title)

1 pt

2.12 (no title)

1 pt

2.13 (no title)

1 pt

2.14	(no title)	1 pt
2.15	(no title)	1 pt
2.16	(no title)	1 pt
2.17	(no title)	1 pt
2.18	(no title)	1 pt
2.19	(no title)	1 pt
2.20	(no title)	1 pt

QUESTION 3

(no title)		8 pts
3.1	(no title)	1 pt
3.2	(no title)	1 pt
3.3	(no title)	1 pt
3.4	(no title)	1 pt
3.5	(no title)	1 pt
3.6	(no title)	1 pt
3.7	(no title)	1 pt
3.8	(no title)	1 pt

QUESTION 4

(no title)		8 pts
4.1	(no title)	1 pt
4.2	(no title)	1 pt
4.3	(no title)	1 pt
4.4	(no title)	1 pt
4.5	(no title)	1 pt
4.6	(no title)	1 pt
4.7	(no title)	1 pt
4.8	(no title)	1 pt

QUESTION 5

(no title)	8 pts
5.1 (no title)	1 pt
5.2 (no title)	1 pt

5.3	(no title)	1 pt
5.4	(no title)	1 pt
5.5	(no title)	1 pt
5.6	(no title)	1 pt
5.7	(no title)	1 pt
5.8	(no title)	1 pt

QUESTION 6

(no title)		8 pts
6.1	(no title)	1 pt
6.2	(no title)	1 pt
6.3	(no title)	1 pt
6.4	(no title)	1 pt
6.5	(no title)	1 pt
6.6	(no title)	1 pt
6.7	(no title)	1 pt
6.8	(no title)	1 pt

QUESTION 7

(no title)		8 pts
7.1	(no title)	1 pt
7.2	(no title)	1 pt
7.3	(no title)	1 pt
7.4	(no title)	1 pt
7.5	(no title)	1 pt
7.6	(no title)	1 pt
7.7	(no title)	1 pt
7.8	(no title)	1 pt