Q1 DNSSEC

8 Points

This homework has instant feedback. When you click "Save Answer," if the answer is correct, you will see an explanation. You can resubmit as many times as you want.

Relevant lecture: DNSSEC (textbook)

This question walks you through how DNSSEC guarantees integrity on a final answer record.

A resolver is making a DNSSEC lookup for `proj3.cs161.org`. Assume the resolver's cache is empty (except for any hardcoded values).

Throughout this question, we use a checkmark `(✓)` to denote records that are validated with a signature.

Q1.1

1 Point

Which public key(s) does the resolver trust before making any queries?

☑ root's public KSK

□ root's public ZSK

□ None of the above

Q1.2
1 Point

The resolver queries root and receives these records to put in its cache:

```
2. ( ) [DNSKEY] root's public ZSK
3. ( ) [RRSIG] signature on (2)
4. ( ) [NS] domain of .org name server
5. ( ) [A] IP of .org name server
6. ( ) [DS] hash of .org's KSK
7. ( ) [RRSIG] signature on (6)
```

Whose key is used to generate the signature in record (2)?

● root's private KSK

○ root's private ZSK

○ .edu's private KSK

○ .edu's private ZSK

Q1.3
1 Point

Whose key is used to generate the signature in record (7)?

○ root's private KSK

● root's private ZSK

○ .edu's private KSK

○ .edu's private ZSK

Q1.4

1 Point

The resolver's cache after performing any verification is:

```
1. (✓) [DNSKEY] root's public KSK
2. (✓) [DNSKEY] root's public ZSK
3. ( ) [RRSIG] signature on (2)
4. ( ) [NS] domain of .org name server
5. ( ) [A] IP of .org name server
6. (✓) [DS] hash of .org's KSK
7. ( ) [RRSIG] signature on (6)
```

Which public key(s) does the resolver trust after performing all the verification steps with these records?

Hint: Any previously trusted keys from Q2.1 are still trusted.

☑ root's public KSK

☑ root's public ZSK

☑ .org's public KSK

□ .org's public ZSK

□ None of the above

Q1.5
1 Point

The resolver queries .org and receives these records to put in its cache:

```
 8. ( ) [DNSKEY] .org's public KSK
 9. ( ) [DNSKEY] _____'s public ZSK
10. ( ) [RRSIG] signature on (9)
11. ( ) [NS] domain of cs161.org name server
12. ( ) [A] IP of cs161.org name server
13. ( ) [DS] hash of _____
14. ( ) [RRSIG] signature on (13)
```

Whose public ZSK is returned in (9)?

○ root

● .org

○ cs161.org

Q1.6
1 Point

Whose public key is hashed in (13)?

○ .org's public KSK

○ .org's public ZSK

● cs161.org's public KSK

○ cs161.org's public ZSK

Q1.7
1 Point

The resolver's cache after performing any verification is:

```
 1. (✓) [DNSKEY] root's public KSK
 2. (✓) [DNSKEY] root's public ZSK
 3. ( ) [RRSIG] signature on (2)
 4. ( ) [NS] domain of .org name server
 5. ( ) [A] IP of .org name server
 6. (✓) [DS] hash of .org's public KSK
 7. ( ) [RRSIG] signature on (6)
 8. (✓) [DNSKEY] .org's public KSK
 9. (✓) [DNSKEY] .org's public ZSK
10. ( ) [RRSIG] signature on (9)
11. ( ) [NS] domain of cs161.org name server
12. ( ) [A] IP of cs161.org name server
13. (✓) [DS] hash of cs161.org's public KSK
14. ( ) [RRSIG] signature on (13)
```

Which public key(s) does the resolver trust after performing all the verification steps with these records?

Hint: Any previously trusted keys from Q2.4 are still trusted.

☑ root's public KSK

☑ root's public ZSK

☑ .org's public KSK

☑ .org's public ZSK

☑ cs161.org's public KSK

□ cs161.org's public ZSK

□ None of the above

Q1.8
1 Point

The resolver queries cs161.org and receives these records to put in its cache:

```
15. (✓) [DNSKEY] cs161.org's public KSK
16. (✓) [DNSKEY] cs161.org's public ZSK
17. ( ) [RRSIG] signature on (16)
18. (✓) [A] IP of proj3.cs161.org
19. ( ) [RRSIG] signature on (18)
```

Which public key(s) and records does the resolver trust after performing all the verification steps with these records?

Hint: Any previously trusted keys from Q2.4 are still trusted.

☑ root's public KSK

☑ root's public ZSK

☑ .org's public KSK

☑ .org's public ZSK

☑ cs161.org's public KSK

☑ cs161.org's public ZSK

☑ The final answer record

□ None of the above

Q2 Denial of Service (DoS)

2 Points

Relevant lecture: Denial-of-Service Attacks (textbook)

Bob wants to prevent people from overwhelming his pet-photo website, and is considering the following solutions. For each of these proposals, choose whether it is effective at preventing all DoS attacks.

Q2.1

1 Point

Bob sees on the news that IP spoofing has been eradicated, and no one can spoof their IP anymore! He decides to limit the amount of data any given IP address can send or ask for, and simply terminates the connection for any single IP address that violates this.

○ Good solution

● Bad solution

Q2.2

1 Point

Bob installs a firewall. If his website starts receiving a huge amount of traffic, Bob's firewall will analyze each packet and drop any suspicious packets.

○ Good solution

● Bad solution

Q3 Feedback
2 Points

As we're nearing the end of the semester, we'd appreciate any feedback for how we might improve the class in future semesters!

As always, all your feedback is anonymized and will not affect your grade.

Q3.1 Department Course Evals
2 Points

Please fill out the department course evaluations! We'll use the honor system to give you credit, but we might randomly email students requesting screenshot proof, so please do fill them out before submitting this question.

(Please leave feedback for Junyang Wang blank.)

● I filled out course evals

○ I did not fill out course evals

Q3.2 Feedback
0 Points

Optionally, feel free to include feedback.

What's something we could do to make the class better for future semesters?

If you have feedback, submit your comments here. Your name will not be connected to any feedback you provide, and anything you submit here will not affect your grade.

Thank you for all the great feedback you've provided this semester!

Homework 7

● Graded

Select each question to review feedback and grading details.

Student

Yiyun Chen

Total Points

12 / 12 pts

Question 1

	DNSSEC	**8** / 8 pts
1.1	(no title)	**1** / 1 pt
1.2	(no title)	**1** / 1 pt
1.3	(no title)	**1** / 1 pt
1.4	(no title)	**1** / 1 pt
1.5	(no title)	**1** / 1 pt
1.6	(no title)	**1** / 1 pt
1.7	(no title)	**1** / 1 pt
1.8	(no title)	**1** / 1 pt

Question 2

	Denial of Service (DoS)	**2** / 2 pts
2.1	(no title)	**1** / 1 pt
2.2	(no title)	**1** / 1 pt

Question 3

	Feedback	**2** / 2 pts
3.1	Department Course Evals	**2** / 2 pts
3.2	Feedback	**0** / 0 pts