CSE534 HOMEWORK 1:

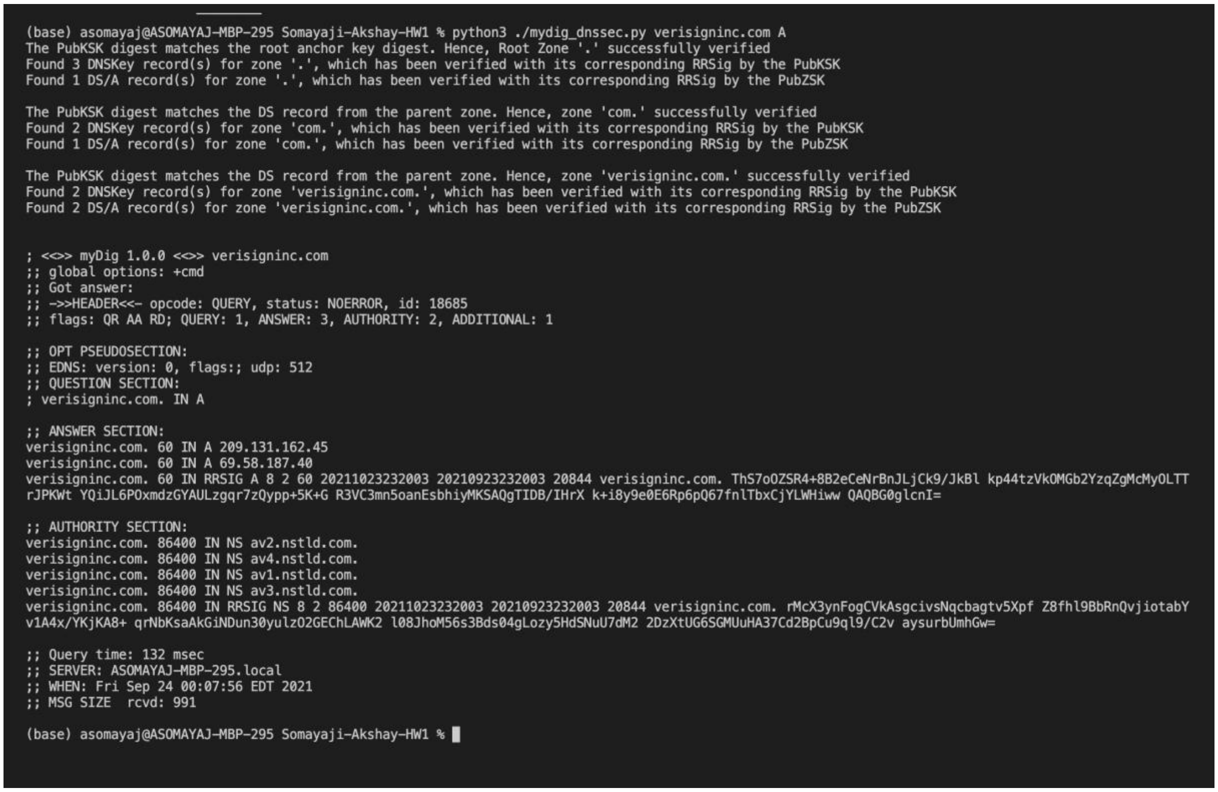
MY IMPLEMENTATION OF DNSSEC

A. Successful DNSSEC implementation

For question 1 of Part B, where we must verify a successful instance of a DNSSEC implementation, I will be summarizing the steps I followed below, making use of '**verisigninc.com**' as an example. You can also refer to comments in mydig_dnssec.py which contains more line-by-line explanations and descriptions of some of the acronyms we are using here.

1. Go to http://data.iana.org/root-anchors/root-anchors.xml to fetch the digest of the currently active root anchor key (the one with validity from 2017), which acts as the root public Key Signing Key (root PubKSK).
2. Make an iterative query for the domain name to be resolved to any of the 13 global root servers by passing the +dnssec flag.
3. From the root DNS response, we will then look for the DNSKEY RRSet (contains root zone's PubKSK and PubZSK (public Zone Signing Key)) and its corresponding RRSig, which is the digital signature of the RRSet signed using the root zone's PvtKSK. We can confirm the authenticity of this RRSet by decrypting the RRSig using the root PubKSK and matching with it.
4. We will also look for a DS RRSet (which contains the PubKSK for the child zone, which is 'com.' in this example) and its corresponding RRSig, which we can decrypt using the root zone's PubZSK to verify its authenticity.
5. Finally, we verify the root zone itself by comparing the root zone's PubKSK with the anchor root key. Thus, we have verified the root zone, and begin the next iterative query to the 'com.' TLD zone.
6. We repeat steps 3-5 by making another iterative query to the '.com' TLD server. We will now obtain the DS record for the next child zone ('verisigninc.com.' zone) and have verified the 'com.' zone by comparing the PubKSK obtained from the root server in step 4 with the 'com.' zone server's PubKSK which is present in the DNSKEY RRSet that it returns.
7. If there are other name servers in the hierarchy, we repeat the same set of steps as explained above, until we finally reach the Authoritative name server (verisigninc.com.) which contains the A records which we can use to resolve the IP of the domain. Here, instead of a DS record, we will have an A RRSet and its corresponding RRSig, which we can decrypt using the zone's PubZSK. On also verifying the DNSKEY RRSet with its RRSig (decrypted using the zone's PubKSK) and the 'verisigninc.com.' zone itself by making use of the DS record obtained in step 6, we have successfully verified the DNSSEC protocol for this domain.

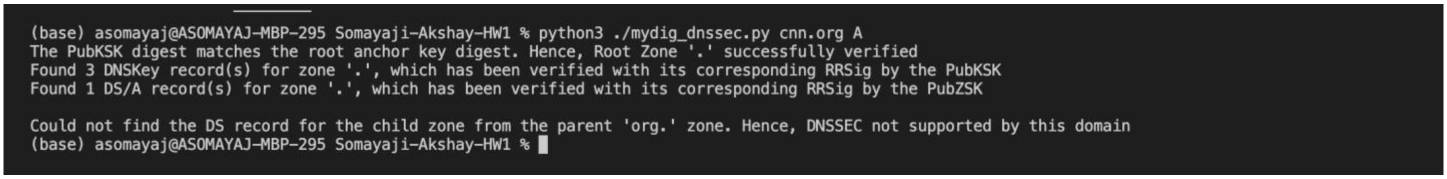
I will now post the output of my custom mydig program to demonstrate a successful verification flow as explained above.



```
(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % python3 ./mydig_dnssec.py verisigninc.com A
The PubKSK digest matches the root anchor key digest. Hence, Root Zone '.' successfully verified
Found 3 DNSKey record(s) for zone '.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone '.', which has been verified with its corresponding RRSig by the PubZSK

The PubKSK digest matches the DS record from the parent zone. Hence, zone 'com.' successfully verified
Found 2 DNSKey record(s) for zone 'com.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone 'com.', which has been verified with its corresponding RRSig by the PubZSK

The PubKSK digest matches the DS record from the parent zone. Hence, zone 'verisigninc.com.' successfully verified
Found 2 DNSKey record(s) for zone 'verisigninc.com.', which has been verified with its corresponding RRSig by the PubKSK
Found 2 DS/A record(s) for zone 'verisigninc.com.', which has been verified with its corresponding RRSig by the PubZSK


; <<>> myDig 1.0.0 <<>> verisigninc.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18685
;; flags: QR AA RD; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; verisigninc.com. IN A

;; ANSWER SECTION:
verisigninc.com. 60 IN A 209.131.162.45
verisigninc.com. 60 IN A 69.58.187.40
verisigninc.com. 60 IN RRSIG A 8 2 60 20211023232003 20210923232003 20844 verisigninc.com. ThS7oOZSR4+8B2eCeNrBnJLjCk9/JkBl kp44tzVkOMGb2YzqZgMcMyOLTT
rJPKWt YQiJL6POxmdzGYAULzgqr7zQypp+5K+G R3VC3mn5oanEsbhiyMKSAQgTIDB/IHrX k+i8y9e0E6Rp6pQ67fnlTbxCjYLWHiww QAQBG0glcnI=

;; AUTHORITY SECTION:
verisigninc.com. 86400 IN NS av2.nstld.com.
verisigninc.com. 86400 IN NS av4.nstld.com.
verisigninc.com. 86400 IN NS av1.nstld.com.
verisigninc.com. 86400 IN NS av3.nstld.com.
verisigninc.com. 86400 IN RRSIG NS 8 2 86400 20211023232003 20210923232003 20844 verisigninc.com. rMcX3ynFogCVkAsgcivsNqcbagtv5Xpf Z8fhl9BbRnQvjiotabY
v1A4x/YKjKA8+ qrNbKsaAkGiNDun30yulzO2GEChLAWK2 l08JhoM56s3Bds04gLozy5HdSNuU7dM2 2DzXtUG6SGMUuHA37Cd2BpCu9ql9/C2v aysurbUmhGw=

;; Query time: 132 msec
;; SERVER: ASOMAYAJ-MBP-295.local
;; WHEN: Fri Sep 24 00:07:56 EDT 2021
;; MSG SIZE  rcvd: 991

(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % █
```

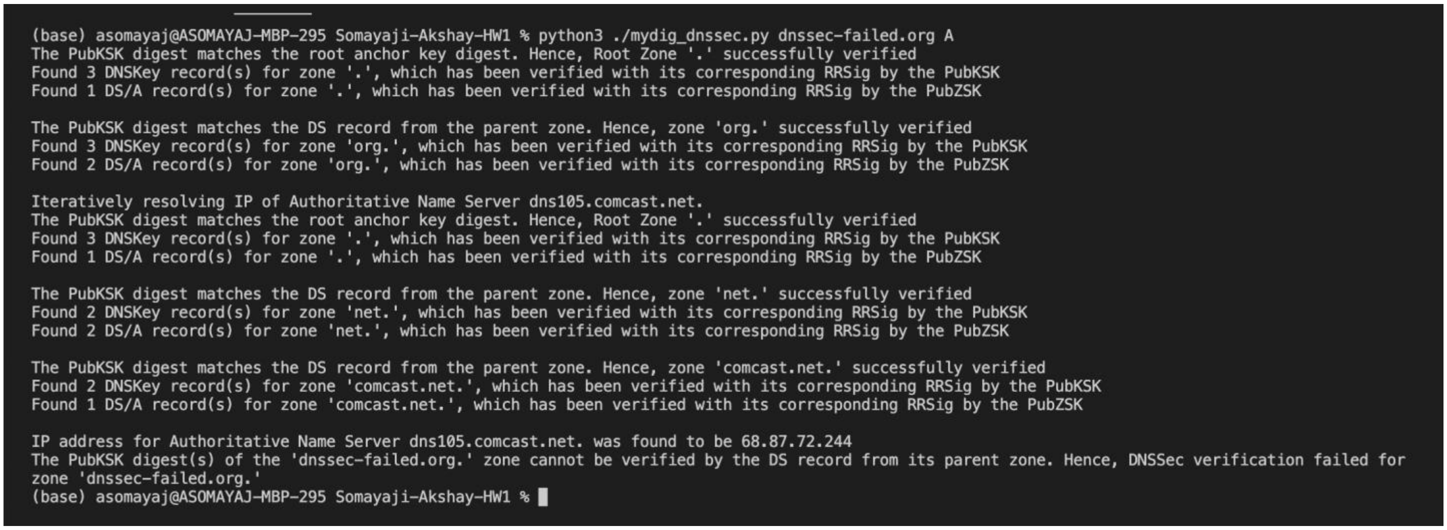
B. **DNSSEC verification failures**

- I will use this section to talk about how to identify when DNSSEC verification was not successful, which we need to implement as per questions 2 and 3 of Part B. The first kind is when the domain itself does not support DNSSEC as of yet. An example is **cnn.org**. We can verify the root zone, but when we are trying to verify the 'org.' zone, we cannot do so as it does not contain a DS record containing the hash of the PubKSK for the child ('cnn.org.') zone, as shown below from the program output.



```
(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % python3 ./mydig_dnssec.py cnn.org A
The PubKSK digest matches the root anchor key digest. Hence, Root Zone '.' successfully verified
Found 3 DNSKey record(s) for zone '.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone '.', which has been verified with its corresponding RRSig by the PubZSK

Could not find the DS record for the child zone from the parent 'org.' zone. Hence, DNSSEC not supported by this domain
(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % █
```

- The second kind of verification failure occurs when we are unable to match the RRSig with their corresponding RRSets, or when we cannot verify the zone by matching the zone's PubKSK hash with the one obtained from the DS record of the parent zone. An example is shown below for



```
(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % python3 ./mydig_dnssec.py dnssec-failed.org A
The PubKSK digest matches the root anchor key digest. Hence, Root Zone '.' successfully verified
Found 3 DNSKey record(s) for zone '.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone '.', which has been verified with its corresponding RRSig by the PubZSK

The PubKSK digest matches the DS record from the parent zone. Hence, zone 'org.' successfully verified
Found 3 DNSKey record(s) for zone 'org.', which has been verified with its corresponding RRSig by the PubKSK
Found 2 DS/A record(s) for zone 'org.', which has been verified with its corresponding RRSig by the PubZSK

Iteratively resolving IP of Authoritative Name Server dns105.comcast.net.
The PubKSK digest matches the root anchor key digest. Hence, Root Zone '.' successfully verified
Found 3 DNSKey record(s) for zone '.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone '.', which has been verified with its corresponding RRSig by the PubZSK

The PubKSK digest matches the DS record from the parent zone. Hence, zone 'net.' successfully verified
Found 2 DNSKey record(s) for zone 'net.', which has been verified with its corresponding RRSig by the PubKSK
Found 2 DS/A record(s) for zone 'net.', which has been verified with its corresponding RRSig by the PubZSK

The PubKSK digest matches the DS record from the parent zone. Hence, zone 'comcast.net.' successfully verified
Found 2 DNSKey record(s) for zone 'comcast.net.', which has been verified with its corresponding RRSig by the PubKSK
Found 1 DS/A record(s) for zone 'comcast.net.', which has been verified with its corresponding RRSig by the PubZSK

IP address for Authoritative Name Server dns105.comcast.net. was found to be 68.87.72.244
The PubKSK digest(s) of the 'dnssec-failed.org.' zone cannot be verified by the DS record from its parent zone. Hence, DNSSec verification failed for
zone 'dnssec-failed.org.'
(base) asomayaj@ASOMAYAJ-MBP-295 Somayaji-Akshay-HW1 % █
```