PIYUSH MITAL - 113219650

Implementation of DNSSEC

Following are the steps I followed to establish DNS SEC Alongside my DNS
I've taken .com as a sample website wherein DNSSEC is available.

1. First, I send request for DNSKEY to root server
2. I get 4 things,
    a. DNSKEY of root (.)
    b. RRSIG of DNSKEY
    c. DS record of TLD's zone (.com)
    d. RRSIG for the DS record signed with private ZSK of root
3. Decrypts RRSIG using Public KSK of root
4. I validate root server's public KSK with trust anchor
5. Decrypt DS record of next TLD using Public ZSK of the root

After this I proceed to the next iteration by checking the additional section of the response.

1. I send a request to TLD (.com) for its DNSKEY
2. I get 4 things:
    a. DNSKEY of TLD (.com)
    b. RRSIG Against DNSKEY
    c. DS record of apple.com's Authoritative Name Server
    d. RRSIG for the DS record signed with private ZSK of TLD (.com)
3. I do 3 things with this:
    a. Decrypts RRSIG using Public KSK of TLD
    b. Validate TLD server's public KSK with public KSK stored in the previous iteration
    c. Decrypt DS record of Authoritative Name server (apple.com) using Public ZSK of TLD (.com)

Finally, I reach the terminating iteration:

1. I send a request to Authoritative Name Server (apple.com) for its DNSKEY+
2. I get 4 things:
    a. DNSKEY of Authoritative Name Server (apple.com)
    b. RRSIG Against DNSKEY
    c. A record of apple.com's server
    d. RRSIG for the A record signed with private ZSK of Authoritative Name Server (apple.com)
3. I do 3 things with this:
    a. Decrypts RRSIG using Public KSK of Authoritative Name Server
    b. Validate Authoritative Name Server's public KSK with public KSK stored in the previous iteration
    c. Decrypt the A record using Public ZSK of apple.com's Authoritative Name Server.

Hence DNS records are verified for apple.com

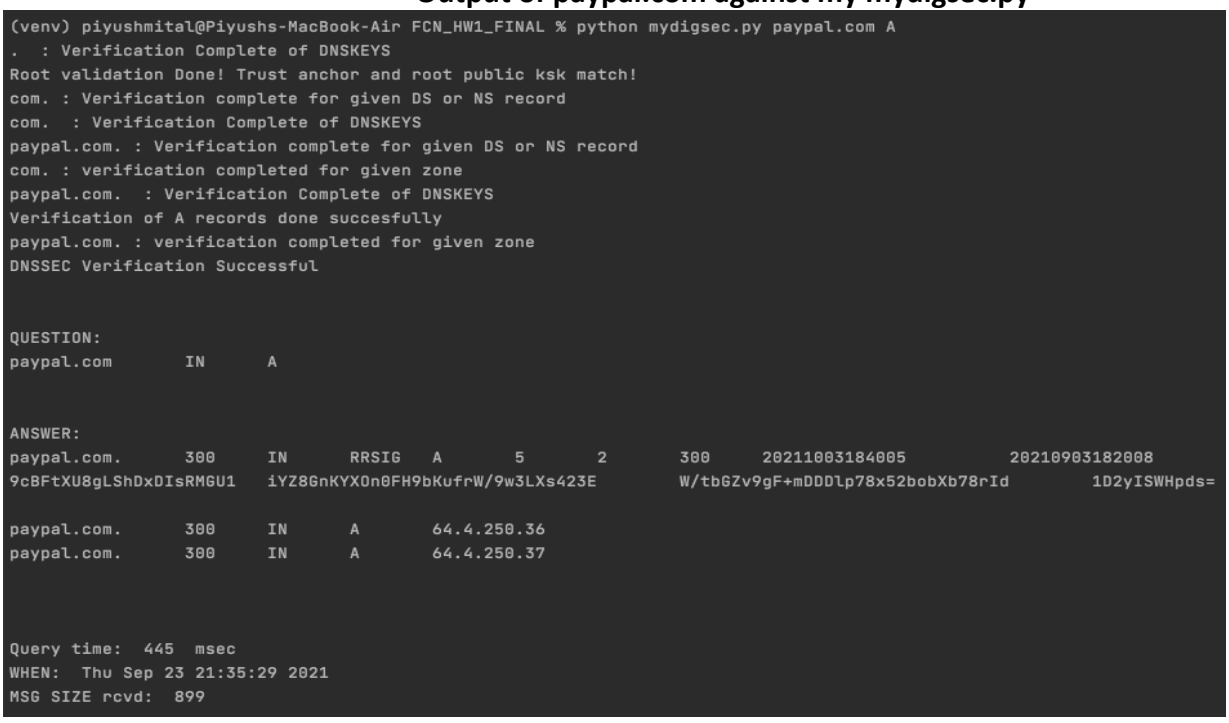
I've attached a screenshot-based version of the same below for further understanding

OUTPUT OF PART B

Output of running against dnssec-failed.org

".", "org." both were verified and validated. But the authoritative server of dnssec-failed.org. did not send the correct keys for conducting validation and hence DNS SEC verification failed

Output of paypal.com against my mydigsec.py



".", "com." and "paypal.com." servers could be verified. The final A record was also verified and hence it is proved that DNSSEC works for paypal.com

Output of cnn.com

```
(venv) piyushmital@Piyushs-MacBook-Air FCN_HW1_FINAL % python mydigsec.py cnn.com A
.  : Verification Complete of DNSKEYS
Root validation Done! Trust anchor and root public ksk match!
com. : Verification complete for given DS or NS record
 Server hasn't responded with a rdtype 43, so DNSSEC NOT SUPPORTED
 Server hasn't responded with a rdtype 43, so DNSSEC NOT SUPPORTED
 Server hasn't responded with a rdtype 43, so DNSSEC NOT SUPPORTED


DNSSEC not supported
```

“.”, “com.” both were verified and validated. But the authoritative server of cnn.com. doesn’t support DNS SEC.