DNSSEC Implementation

We build a DNS Resolver with DNSSEC implementation to verify the DNSSEC support for websites.

validateRootServer(response):
Since root doesn't have a parent, we compare the public KSK to verify the keys for the root server against the given list.

validateDS(response, iterResponse):
This is used to verify the DS records and its corresponding RRSig which was signed using the private ZSK

getZones(hostname, passCounter):
It gives you the domain for the next DNS key response

resolve(hostname, response):

- Gets the DNS response and the DNS Key response
- If it is a rootServer, we use validateRootServer() function for validation
- After this, we validate the DS using validateDS() function
- Next, we fetch the public KSK from the DNS key record of the current website and we hash it using SHA256 and SHA1. This hashed value of the public KSK is compared to the previous DS record.
- If these values do not match, we return 'DNS Verification Failed'
- After validation, we store the current DS record for the next validation
- Next, we verify the DNSKeys and its corresponding RRSig. This is done to validate the public ZSK using the public KSK
- We continue iterating through the next query since everything is verified

For resolution:

- We first check the answer section. If it contains CNAME, we redo the entire resolution using the CNAME. If it contains the IP Address to the queried domain, we directly return the same and end the resolution.
- Next, we check the additional section for other IP Addresses. If it contains IPv4 addresses, we query the initial domain on these addresses.
- Finally, if both answer and additional are empty, we check the authority section.
- If this contains the nameserver, we redo the entire resolution using the nameserver

There might be cases where DNSSEC implementation might be unsuccessful. This happens in the following two cases:

a. DNSSEC Not Supported: This happens when DNSSEC is not supported by websites like 'google.com'

b. DNSSEC Verification Failed: If any of the 3 verifications fail, DNSSEC Verification is failed