DNSSEC IMPLEMENTATION METHOD

I build the DNSSEC verifications in a whole dig pass, to the designation name sever.

(1) In each zone, there are two kinds of verifications.
The first one is to verify the DNSKSK, which is together with DNSZSK in the dnskey set. But in doing this, the DNSKEY set needed to be fetched from this zone's name servers. After checking the answer of the response object, there are two types of keys, ksk with flag 256 and zsk with flag 257. When verifying the root zone's ksk, it is different from the descending zones.
The root zone' ksk is verified using the key I found from internet, it's a public information. This step just uses the validate function. It will give me confidence that the zsk is official. It will return "DNSksk Validation Success!" if verify successfully, otherwise returns "…failed".

The second verification is using the zsk, from the dns set mentioned above, to verify the DS. The DS set is in the response's authority section. I used a try and exception way to return "DS verification success" or "…failed".

(2) Store the DS at the end of the recursive function call. By doing this, I check the child zone's ksk in the dnskey set. Here the ksk need to be hashed by "SHA-256" and then compared with the DS of the parent zone. And then starts this child zone's new round of two validations.

(3) About the recursive function
There are two parameters, zone and DS are special other than the other three parameters in the "get_answer" function in the "mydig_dnssec.py". When called recursively, this two are passed into the new round.

At the beginning of this function, the response' answer section is checked first. If there is "A" type rrset in it, then print out the IP information and return. Otherwise do verifications of the ksk and subsequent DS validation, and then call recursively using the IP address from the additional section and DS.

(4) Performance
My mydig_dnssec sometimes returns failure even if I query the same domain. Although it is maybe the reason of unreliable of this dnssec system, I really need to improve my program's performance in further.