DNSSEC implementation details:

Parts B and A are generally the same. But the difference is that in part B, ZSK verifies the RRSET before contacting the server. ZSK is obtained from server name and server IP. RRSET is obtained from the server IP and the target domain, and the digital signature RRSIG is obtained. Validation is via dns.dnssec.validate(RRSET, RRSIG, {name:ZSK}). After the verification is passed, the server can be contacted normally, otherwise it will exit.

After contacting the server normally and obtaining the server IP of the next layer, verification of the hash code is also required. KSK verifies ZSK. ZSK is obtained by the next server name and current server IP, and KSK is obtained by the next server name and next server IP. Then use KSK to make a hash code and compare the hash code of ZSK. Incorrect comparison will exist.

After that, recursive analysis will be performed, and the same method as the previous two paragraphs will be implemented. Any incorrect verification will exit, all verifications are successful, and the result will be output.