Data Communication and Networks	**Quiz 8: DNSSEC (Open book)**
CSCI-351 Fall 2019	**November 21, 2019**

You have 10 minutes to complete this quiz.

Name: Grading Key

RIT Username: ____________________

Problem	Possible	Score
1	10	
2	10	
3	20	
Total	40	

1. There are three principles in the information security model. Explain what they are and whether each of them is hold in DNSSEC or not. (10 pts)

Confidentiality: data must only be released to authorized principals; Not hold in DNSSEC. Integrity: data must not be modified; Hold in DNSSEC. Availability: data and resources must be accessible when required; Hold in DNSSEC (as long as the server is available)

2. There are two types of `DNSKEY` in DNSSEC. Discuss what they are and why DNSSEC uses two types of `DNSKEY` rather than a single one. (10 pts)

The `KSK` signs for `ZSK`, and `ZSK` signs for DNS records. Thus, `KSK` can be stored in more secure place such as HSM because it is less frequently used than `ZSK`. If `ZSK` were compromised, the domain owner can generate `ZSK` and `KSK` can simply signs the new `ZSK`

3. Assume that you are using a DNSSEC-supporting resolver to return the `A` record of `example.com`, of which nameserver supports DNSSEC. Using proper terminologies, explain all the required steps to verify the `A` record. (20 pts)

Verifying the signature (`RRSIG`) of `A` record using `DNSKEY (ZSK)`. `ZSK`'s signature can be verified using `KSK`. `KSK` can be verified using its signature and comparing the `DS` record fetched from the parent zone (.com zone). The `DS` record is also signed by the parent zone, of which signature can be verified similarly. This process is iteratively excuted until it verifies the root's `DNSKEY` using the prefetched root's `KSK`.