Data Communication and Networks	**Quiz 9: HTTPS (Open book)**
CSCI-351 Fall 2018	**December 6, 2018**

You have 15 minutes to complete this quiz.

Name: Grading Key

RIT Username: _____

Problem	**Possible**	**Score**
1	10	
2	10	
3	20	
Total	40	

1. Assume that you fetched a certificate from google.com. Your browser will validate the certificate to create a session key to encrypt/decrypt your traffic. List (at least) 3 steps to confirm that the certificate is valid. (10 pts)

Expiration check, trust-of-chain validation, signature check, revocation check, server's domain name accordance with the common name, and etc.

2. Assume that an attacker successfully stole the private key of BankofAmerica.com. What/how should the administrator of BankofAmerica.com need to do once the administrator have noticed that their key has been stolen? (10 pts)

Notice to the issuer of the certificate to revoke the certificate.

3. There are two main certificate revocation methods that we discussed in the class. Name each of (1) the methods, (2) their limitation, and (3) other extensions (if any) to solve the limitation. (20 pts)

CRL and OCSP. CRL's limitation is that it is inefficient due to its big size. OCSP's limitation is that it introduces additional latency (clients need to wait until the OCSP response comes) and privacy issues (CA basically can track the websites that clients visit). To solve the limitation, OCSP-Stapling introduced where the websever prefetches the OCSP response from the CA and provides it along with the certificate. The limitation is soft-failure problem where clients just accept a certificate even though they fail to fetch revocation status from OCSP responders. To solve this limitation, OCSP Must-Staple was introduced to instruct clients that the OCSP response will and MUST be provided by the webserver; thus the clients MUST reject the certificates if the OCSP response is not provided by the webserver.