The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 20
April 12, 2018

Homework 10 – Due Tuesday, April 17

1. In the last homework, you was that if the "per message secret number" in DSA wasn't kept secret, that the signer's private key could be computed. The "per message" part of the phrase "per message secret number" is also vital. If an attacker could trick a signer into signing two different messages, say M_1 and M_2, using the same secret k, what can the attacker figure out from knowledge of those two signatures and the two messages.

   [*Hint: As last time, try playing around with the formulas and seeing what you can cancel out or otherwise compute. Also, feel free to use the results of last week's homework problem in solving this one!*]

2. What is a certificate and what role does it play in the distribution of public keys? Describe what a certificate does, what it protects against, and how it does this. Be clear on what basic security goal certificates address (confidentiality, integrity, or availability).

3. What is a certificate revocation list (CRL), and what is it used for? Describe two specific scenarios that would require a CRL.