CS181S – Systems Security Fall 2020

Problem Session 4: Secure Channels

Monday September 21, 2020

1. An encryption scheme is malleable if an adversary with access to a ciphertext can modify that ciphertext to construct a valid ciphertext for a different message in a consistent, predictable way. That is, the adversary should know the relationship between the original plaintext and the message you get when you decrypt the modified ciphertext. For each of the following encryption schemes, give an example of a way in which an adversary could modify a ciphertext in this manner:

   (a) Textbook RSA

   (b) AES-CBC

   (c) AES-CTR

2. How could you use MACs and/or digital signatures to detect these sorts of attacks?

3. Get started on A3!