Fall 2012 – CS 683 Computer Security and Privacy
Assignment 2
Make sure to include all the references in your submission

1. Cookies

Your replay attack in Step 4 is essentially what FireSheep (http://codebutler.com/firesheep/) has done, in the form of FireFox add-on. When you login to gmail.com and then go to youtube.com, you are still logged-in but it runs on HTTP, not on HTTPS.

(a) (2 points) Can you use this cookie to do a replay attack on http://youtube.com? Explain why.

(b) (3 points) Can you use this cookie to do a replay attack on http://gmail.com? Explain why.

2. RSA (5 points)

The public key of RSA consists of two numbers, \((e, n)\). The public key of USF Connect uses 65537 as \(e\), and the public key of google.com also uses 65537 as \(e\). In fact, many well-known websites uses 65537 as \(e\). Is it safe to use the same \(e\) in so many public keys?

3. Certificates

One of the benefits of using certificates is that the certificate authority does not have to be online to validate the public key in the certificate. In other words, when your web browser visits USF Connect, VeriSign does not have to be online for your web browser to check the validity of the public key of USF Connect. However, you may decide to check that the public key of USF Connect is not revoked using OCSP.

(a) (3 points) Explain how the OCSP works.

(b) (3 points) Could this OCSP server be a bottleneck? Explain your answer.

4. Symmetric Key Cryptography

\(K_{AB}\) is a shared (symmetric) key between Alice and Bob and \(K_{AB}(m)\) is the ciphertext of \(m\) encrypted with \(K_{AB}\). \(H\) is a secure hash function.

(a) (3 points) Imagine Alice sends \(m, K_{AB}(m)\) to Bob. Does this provide integrity and authentication of \(m\)? Explain your answer.

(b) (3 points) Imagine Alice sends \(m, K_{AB}(H(m))\) to Bob. Does this provide integrity and authentication of \(m\)? Explain your answer.

(c) (3 points) Imagine Alice sends \(K_{AB}(m), H(m)\) to Bob. Does this provide confidentiality, integrity and authentication of \(m\)? Explain your answer.

5. Stream Cipher (5 points)

Imagine that \(H\) is a secure hash function. Given the key \(k\), imagine that we use \(H(k), H(H(k)), H(H(H(k))), \ldots\) as key stream. Is this scheme one-time pad? In other words, is this scheme a good stream cipher?