CS 798

Assignment 1

due 11:30 AM, October 8

1. Setting up an SSL session, as described in Section 1.1.2, incorporates server-to-client authentication but no client-to-server authentication. Briefly discuss any reasons you can think of why the protocol may only use one-way authentication.

2. Consider the Rabin cryptosystem with $n = 638160384373$. Suppose the ciphertext is 377838732432. Factor n, and use the Rabin decryption algorithm to determin the four possible plaintexts whose encryption is n. You can implement the Chinese remainder theorem with two moduli yourself.

   Hint: This is an easy exercise using Maple. The command `ifactor` can be used to factor n. A modular exponentiation $z^c \bmod m$ can be done using the command `z &^ c mod m`, and a modular inverse $z^{-1} \bmod m$ can be done using the command `1/z mod m`.

3. The integer $p = 90872345251$ is prime.

   (a) Factor $p - 1$, and then verify that 2 is a primitive element in $\mathbb{Z}_p{}^*$ using the efficient test described in class. Show that 3 is not a primitive element.

   (b) How many primitive elements are there in $\mathbb{Z}_p{}^*$ for the given value of p. (Use the formula given in class!)

   Hint: This is an easy exercise using Maple.

4. Prove that the Rabin cryptosystem is *insecure* in a chosen-ciphertext attack.

   Hint: Consider Algorithm 1.9.

5. Decribe attack models and adversarial goals for message authentication codes, by modifying the ones given for signature schemes in an appropriate manner.

6. This question concerns MAC security.

   Let $\ell \geq k \geq 1$ be integers. Suppose that a MAC is a keyed hash family $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$, where $\mathcal{X} = \{0,1\}^\ell$ and $\mathcal{Y} = \{0,1\}^k$ (thus a message is an ℓ-bit string and an authentication tag is a k-bit string). Suppose that the adversary has access to no previously authenticated messages and suppose that the message to be authenticated will be chosen at random. Finally, define

   $$\epsilon = \max\left\{\frac{1}{|\mathcal{K}|}, \frac{1}{2^k}\right\}.$$

   Give a complete proof that an adversary can compute the valid MAC for any message $x \in \mathcal{X}$ with probability at least ϵ.

   Hint: Do *not* assume that the key K is chosen uniformly at random, and do *not* assume that all possible authentication tags are equally likely, given that the key is K.