CS 329E Quiz 3: April 15, 2015

Name: __________________________________________

Note that this quiz has two sides.

1. (True or False: 1 point each, 10 points total) Write T or F on each line.

(a) _____ AES allows keys of length 100, 200, or 300 bits.

(b) _____ A symmetric encryption algorithm with a key length of $k$ bits has $2^k$ possible keys.

(c) _____ A one-way function is easy to compute but difficult to invert (reverse).

(d) _____ A hash function is collision resistant if it is hard to find any two messages that hash to the same value.

(e) _____ Diffie-Hellman is a key-agreement protocol.

(f) _____ A digital certificate vouches for the agreement between a principal’s identity and IP address.

(g) _____ X.509 is an international standard for hash functions.

(h) _____ The Needham-Schroeder protocol involves three principals, one of which has a specialized role.

(i) _____ Nonce is another name for a timestamp.

(j) _____ Using DES twice with two 56-bit keys gives the security of a 112-bit key. (Don’t worry that DES keys are actually 64-bits.)
2. (10 points) The following is a protocol called the *Wide-Mouth Frog Protocol*. The goal is to transfer a secret message \( M \) from \( A \) to \( B \) using a trusted third party \( S \) as an intermediary. A timestamp just records the current time of the sender. \( T_a \) is a timestamp generated by \( A \) and \( T_s \) is a timestamp generated by \( S \). All encryption is symmetric.

1. \( A \rightarrow S : A, \{T_a, B, M\}_{K_{as}} \)
2. \( S \rightarrow B : \{T_s, A, M\}_{K_{bs}} \)

Each of the following is either an assumption about the environment in which protocol runs, a belief of \( B \) as a result of the protocol, or neither. For each line write one of: assumption, belief, neither.

(a) A and S share key \( K_{as} \)

(b) S sent M recently

(c) A originally sent M

(d) Timestamps are reliable

(e) A and B share key \( K_{ab} \)

3. **Extra credit:** (3 points) Given a cryptographic hash function that produces a 128-bit hash value, approximately how many inputs would you expect to try before finding two that hash to the same value?