CS 329E Quiz 2: April 6, 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 is a breakable algorithm

   (b) _____ A symmetric algorithm uses the same key for encryption and decryption.

   (c) _____ A Caesar Cipher is a transposition cipher

   (d) _____ A perfect cipher is possible

   (e) _____ To get pairwise secure communication in a system with many users, symmetric encryption requires fewer keys than asymmetric.

   (f) _____ Columnar transposition is a stream cipher.

   (g) _____ Electronic Code Book (ECB) XORs each successive plaintext block with the previous ciphertext block before encrypting.

   (h) _____ Asymmetric (public key) encryption largely solves the key distribution problem.

   (i) _____ In all public key encryption algorithms, either key (public or private) can be used for encryption, with the other used to decrypt.

   (j) _____ DES is no longer widely used because the key is too short to be secure.

Page total: _____

2. (5 points) Some padlocks have a three number combination. Numbers on the dial range from $[0 \ldots 39]$. *Assume that there are no shortcuts to finding the key other than trying combinations until one works and that all combinations are possible (numbers can be re-used).*

   (a) _____ What is the size of the "keyspace" for this algorithm? (A formula is fine; you don't need an integer answer.)

   (b) _____ *On average*, how many attempts will you need to discover the key?

   (c) _____ Is the algorithm breakable?

   (d) _____ Is the algorithm strong?

   (e) _____ Would this provide adequate protection if this were a digital encryption algorithm rather than a physical device?

3. (5 points) Suppose you have a BLP secure system with exactly the four subjects given below, with the confidentiality levels given.

Type	**Name**	**Level**
Subject	S_1	$(L, \{A, B\})$
Subject	S_2	$(H, \emptyset)$
Subject	S_3	$(L, \{A, B, C\})$
Subject	S_4	$(H, \{B, C\})$

   Give the corresponding non-interference policy, using the notation $S_i \mapsto S_j$ to indicate that subject S_i *may interfere with* subject S_j. List all interferences allowed in the system (except the reflexive interferences of the form $S_i \mapsto S_i$).

Page total: _____