Quiz/Attendance 5F

Total: [ ]

Firstname Lastname [ ] ID #

1. How many cats visited us for cat day?

2. Alice and Bob use a substitution cipher (as discussed in yesterday’s discussion section) with an alphabet $\Sigma = \{A, \ldots, Z, 0, 1, \ldots, 9, *\}$. Alice transmits a ciphertext of:

   Z3VR8JKVY39V

Her plaintext

   Could be ECS127*SUCKS
   Couldn’t be

   Could be ECS127*ROCKS
   Couldn’t be

3. Darken the correct answer.

   True False AES and DES are both PRPs (pseudorandom permutations).
   True False AES keys are so short that exhaustive key search is practical.
   True False AES is a Feistel network.