ECS 127: Cryptography
UC Davis — Phillip Rogaway

Handout 5F
2 May 2024

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 $\Sigma = \{\texttt{A}, \ldots, \texttt{Z}, \texttt{0}, \texttt{1}, \ldots, \texttt{9}, *\}$. Alice transmits a ciphertext of:

`Z3VR8JKVY39V`

Her plaintext

Could be **Couldn't be** `ECS127∗SUCKS`

Could be **Couldn't be** `ECS127∗ROCKS`

3. **Darken** the correct answer.

True **False** AES and DES are both PRPs (pseudorandom permuations).

True **False** AES keys are so short that exhaustive key search is practical.

True **False** AES is a Feistel network.