**COMP435 9/8/25 Practice** Name: ____________________

**Question 1: Bruteforce Attack Time** Given a 56-bit key, how long will it take to exhaustively search through all possible keys to find one that will correctly decrypt a given message? Assume you have a machine that can perform $10^{10} - 10^{15}$ encryptions per second.

**Question 2: Mono-alphabetic Substitution** A message encrypted under a mono-alphabetic substitution produced this ciphertext: AOPP. Which of the following is NOT a possible decryption of this ciphertext?

○ DRSS
○ TREE
○ THAT
○ None

**Question 3: One-Time Pad Decryption** A message encrypted under a one-time pad produced this ciphertext: AOPP. Which of the following is a possible decryption of this ciphertext?

○ DRSS
○ TREE
○ THAT
○ All of the above

**Question 4: One-Time Pad Frequency Analysis** We saw that a ciphertext encrypted with the Caesar cipher is susceptible to letter-frequency analysis. Is the same true of a ciphertext encrypted with a OTP? Why or Why not?

**Question 5: One-Time Pad Eavesdropping** The attacker, Mallory, sees a ciphertext encrypted with a one time pad (OTP) sent over the wire. Using the structure of the ciphertext (e.g., it's length) what information can Mallory learn about the original plaintext?