COMP435 9/8/25 Practice Name: _____

Question 1: Transposition Which of the following are true about transposition?

- ◯ It obscures the symbols of the original plaintext
- ◯ It obscures the patterns of the original plaintext
- ◯ It is a necessary part of any secure public key encryption algorithm
- ◯ It is a necessary part of any secure symmetric encryption algorithm

Question 2: Substitution without Transposition Substition without transposition is insufficient for a secure symmetric encryption algorithm.

- ◯ True
- ◯ False

Question 3: Substitution Which of the following is true about substitution?

- ◯ It obscures the symbols of the original plaintext
- ◯ It obscures the patterns of the original plaintext
- ◯ It is not used in any modern symmetric encryption algorithm

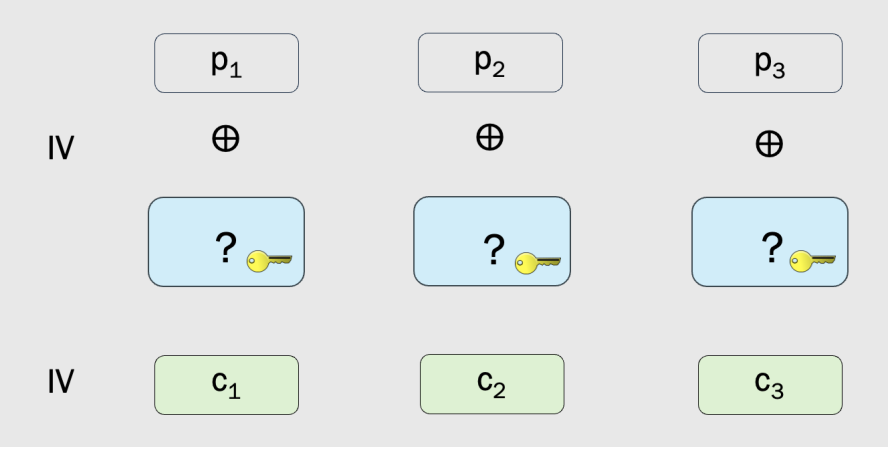
Question 4: One-Time Pad Review The one-time pad uses...

- ◯ neither transposition nor substitution
- ◯ transposition, but not substitution
- ◯ substitution, but not transposition
- ◯ both transposition and substitution

Question 5: Stream ciphers All stream ciphers, including the one-time pad, rely solely on:

- ◯ diffusion
- ◯ confusion

Question 6: CBC Mode Decryption Fill in the corresponding figure for CBC mode decryption. Must decryption be done sequentially?



Question 7: OFB Mode Decryption Fill in the corresponding figure for OFB mode decryption. Why is pre-processing not an option for the message receiver?