

Question 1: 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 2: 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 3: 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 4: 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?

Question 5: 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 6: Substitution without Transposition Substitution without transposition is insufficient for a secure symmetric encryption algorithm.

- ☐ True
- ☐ False

Question 7: 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 8: 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 9: Stream ciphers All stream ciphers, including the one-time pad, rely solely on:

- ☐ diffusion
- ☐ confusion