1.1 Cipher identification strategy [6.5 marks]

a. As a warm-up: in 5 words or less, how to identify a ciphertext from cipher 1? (0.5 mark)

-Look for inconsistent pattern.

b. State a simple way to tell if a ciphertext is from one of the ciphers 2, 3, 4, 5, 6, 7, as opposed to 8, 9. (Hint: recall that the plaintexts only contain letters and possibly whitespaces.) (1 mark)

-Check if ciphertext contains only letters.

c. In a single sentence, how can frequency analysis help decide whether a given ciphertext was created using a cipher from list A, as opposed to one from B, assuming English plaintext: (1 mark)

A: 2: Cæsar; 3: Simple substitution; 4: Simple transposition.

B: 5: Vigenere; 6: Hill; 7: OTP-ish.

-Part A preserves their letter frequency pattens, while part B does not.

d. Say you have narrowed the cipher down to list A above, can you tell which one? Give a very simple test (hint: as a single frequency analysis with different outcomes) to decide between: (1 mark) 2: Cæsar; 3: Simple substitution; 4: Simple transposition.

1. Letters remain the same, but they are in a different order: (4);

2. Letters are mapped to different letters, but their frequencies remain the same: (3);

3. Letters are shifted by the same amount, but their frequencies remain the same: (2).

e. If instead the ciphertext has been narrowed down to one on list B, give a good way to test whether the cipher is 7 “OTP-ish”. (1 mark)

-There should be no clear frequency patterns in the ciphertext of OTP-ish.

f. If the cipher is on list B but is not 7, then it should be 5 (Vigenere) or 6 (Hill-2x2). How would you tell? (You may assume that the Vigenere period is d > 2, and d odd if that makes your life easier.) (1 mark)

-Look any kind of periodic structure in the ciphertext. Repeating patterns are more likely to be 5 while no repeating patterns are more likely to be 6.

g. Lastly, if earlier you found that the cipher is either 8 (binary OTP) or 9 (a strong modern cipher):

- Is it even feasible to tell them apart, in general (i.e., is there a method that always works)? (0.5 mark)
  -No, both 8 and 9 produce ciphertexts that appear random and have no recognizable patterns.
- Is it feasible in your given challenge, perhaps based on some special lucky circumstance? (0.5 mark)
  -Well... If the binary OTP key is reused, maybe I can somehow see the pattern.