Week 5 Tuesday

Favorite Season

Make sure you know your neighbors' names. Then discuss:

What's your favorite season? Why?

Index of Coincidence, Breaking Vignère

1. You have just intercepted some ciphertext that is the encryption of English plaintext, but you do not know which cipher was used to encrypt it. You find that the ciphertext has an index of coincidence of 1.1. Which of the following ciphers was most likely used to produce this ciphertext?

(A) Rectangular transposition

(B) Affine cipher

(C) Vignère cipher

(D) Caesar cipher

2. You have just intercepted a long piece of Vignère ciphertext. You make several guesses for the period, and find the following sequences of indices of coincidence for your guesses:

Guessed Period	Indices of Coincidence
3	1.75, 1.41, 1.32
4	1.15, 1.15, 1.15, 1.13
5	1.74, 1.74, 1.79, 1.71, 1.71
6	1.17, 1.12, 1.16, 1.16, 1.13, 1.15

Which of the following is the most likely period?

(A) 3

(B) 4

(C) 5

(D) 6

3. You have just intercepted a long piece of Vignère ciphertext. Based on an analysis of indices of coincidence, you think that the period is probably 5. When you rewrite the ciphertext into a rectangle of width 5, you find that the the most frequent letter in the third column is `F`. Which of the following *might* be the key word that was used to encrypt the text?

(A) `TOOTH`

(B) `LOFTY`

(C) `CUBES`

(D) `HAZEL`

4. An alien language has three letters in its alphabet: $\oplus$, $\ominus$, $\otimes$. Their respective plaintext frequencies are 20%, 20%, and 60%. Which of the following values is closest to the expected index of coincidence for plaintext in this alien language?

(A) 1

(B) 1.3

(C) 1.7

(D) 2

5. Consider again the same alien language, which has 3 letters in its alphabet: $\oplus$, $\ominus$, $\otimes$. What is the maximum possible index of coincidence for texts in this alphabet?

(A) 1

(B) 3

(C) 9

(D) None of the above

6. You have just intercepted some ciphertext that is the encryption of English plaintext, but you do not know which cipher was used to encrypt it. You find that the ciphertext has an index of coincidence of 1.75. Which of the following ciphers was most likely used to produce this ciphertext?

(A) Rectangular transposition

(B) Playfair cipher

(C) Vignère cipher

(D) Hill cipher