

## **Week 6 Wednesday**

Make sure you're sitting next to someone!

## Local Recommendations

Make sure you know your neighbor's name(s), and then take about 2 minutes to discuss:

What is your top recommendation for something to do, eat, or see on-campus or around San Diego?

## 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. Remember the alien language from Quiz 4? It had three letters in its alphabet ( $\oplus$ ,  $\ominus$ ,  $\otimes$ ), and their respective plaintext frequencies were 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

3. 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:

Gussed 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