Cryptography: Part 2: One-time Pads

Physics II: Modern Physics

College of the Atlantic

Here is a bit of a message that was encoded using a running key¹:

IIXAQTEHBTHBNZOX

Subtract the word THE from each three-letter sequence in the ciphertext. That is,

$$IIX - THE = ? (1)$$

$$IXA - THE = ? (2)$$

$$XAQ - THE = ? (3)$$

and so on, up to

$$ZOX - THE = ?$$
 (4)

(5)

Which of the resulting three-letter sequences could possibly be a part of an English word?

¹This example was taken from Susan Loepp and William K. Wooters, *Protecting Information: From Classical Error Correction to Quantum Cryptography*, Cambridge University Press, 2006.