**SECTION I**

1. Symmetric key encryption
2. Frequency analysis
3. 256-bit encryption
4. Asymmetric encryption
5. You can determine if a website is using either SSL or TLS by looking for a padlock icon or the letters “https” in the address bar at the top of your website.
6. The military

**SECTION II**

1. Algorithms
2. Distribution of the key is a secure manner
3. A) A public key

B) The user’s private key

1. The second key
2. Authentication and nonrepudiation
3. Asymmetric-key encryption

**SECTION III**

1. 81a0dc754f1d53b16c0519bb0b4361bcc67e3947c1e7699326f339b53ad637bf9bf0db8467f257ae6872c730e8dd1a7a
2. 9aЈ`����6#eTans students can network

Compared to the original plain text changing the first hexadecimal character affected the first word in the message. No, the decrypted text should not be identical except for the first character because the flipped bit belonged to the encrypted hash of the first word. Without the correct hash, that part of the message was not decrypted properly.

1. On the text plain after I clicked decrypted with an incorrect key, this appeared “Given final block not properly padded. Such issues can arise if a bad key is used during decryption.”. I expected it not to work since I entered an incorrect key, but I didn’t expect it to tell me that. Since I feel that helps threat actors if they are trying to guess the key.